

**Oracle® Communications
Policy Management**

CMP Wireline User's Guide

E68935 Revision 01

December 2015

Oracle® Communications Policy Management CMP Wireline User's Guide

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: Introduction.....	12
Introduction.....	13
How This Guide is Organized.....	13
Scope and Audience.....	13
Related Publications.....	14
Other Publications.....	15
Locate Product Documentation on the Oracle Help Center Site.....	15
Customer Training.....	15
My Oracle Support (MOS).....	16
Emergency Response.....	16
Chapter 2: The Oracle Communications Policy Management	
Solution.....	17
The Multimedia Policy Engine.....	18
Understanding Policy Rules.....	20
The Oracle Communications Policy Management Configuration Management Platform.....	20
Organizing Policy Rules.....	21
GUI Overview.....	21
Specifications for Using the GUI.....	22
Logging In.....	22
GUI Icons.....	23
Shortcut Selection Keys.....	23
Changing a Password.....	23
Overview of Main Tasks.....	24
Chapter 3: Configuring the Policy Management Topology.....	26
About the Policy Management Topology.....	27
High Availability.....	27
Server Status.....	28
Setting Up the Topology.....	29
Setting Up the CMP Cluster.....	29
Setting Up an MPE Cluster.....	30

Modifying the Topology.....	32
Modifying an MPE Cluster.....	32
Modifying a CMP Cluster.....	33
Removing a Cluster from the Topology.....	34
Forcing a Server into Standby Status.....	34
Configuring SNMP Settings.....	35
Defining Global Configuration Settings.....	37
Setting Stats Settings.....	37

Chapter 4: Managing Multimedia Policy Engine Devices.....39

Policy Server Profiles.....	40
Creating a Policy Server Profile.....	40
Configuring or Modifying a Policy Server Profile.....	41
Deleting a Policy Server Profile.....	41
Configuring Protocol Options on the Policy Server.....	42
Configuring MPE Advanced Settings.....	44
Policy Server Groups.....	45
Creating a Policy Server Group.....	45
Adding a Policy Server to a Policy Server Group.....	46
Creating a Policy Server Sub-group.....	46
Renaming a Policy Server Group.....	46
Removing a Policy Server Profile from a Policy Server Group.....	47
Deleting a Policy Server Group.....	47
Reapplying the Configuration to a Policy Server.....	48
Checking the Status of an MPE Server.....	48
Policy Server Reports.....	50
Cluster Information Report.....	50
Policy Statistics.....	51
Protocol Statistics.....	51
VoD Server Statistics.....	52
Viewing Policy Server Logs.....	53
Viewing the Trace Log.....	53
Syslog Support.....	55
The Session Synchronization Log.....	55
Configuring Log Settings.....	56
VoD Session Flow Scenarios.....	58
Synchronizing a TANDBERG VoD Server.....	59
Synchronization Operations and Failover.....	60
Synchronizing a B-RAS Server.....	60

Chapter 5: Managing Network Elements.....	61
About Network Elements.....	62
Defining a Network Element.....	62
Modifying a Network Element.....	63
Deleting Network Elements.....	63
Finding a Network Element.....	64
Configuring Options for Network Elements.....	65
B-RAS, Router, and Server.....	65
Creating Subnets.....	66
Associating a Network Element with an MPE Device.....	66
Working with Network Element Groups.....	67
Creating a Network Element Group.....	67
Adding a Network Element to a Network Element Group.....	68
Creating a Network Element Sub-group.....	69
Deleting a Network Element from a Network Element Group.....	70
Modifying a Network Element Group.....	70
Deleting a Network Element Group or Sub-group.....	70
Importing VoD Configuration Information.....	71
Provisioning Topology and Subscriber Data.....	71
Path Definitions.....	72
Importing a Large Number of Subscribers.....	73
Chapter 6: Managing Application Profiles.....	74
About Application Profiles.....	75
Creating an Application Profile for a TANDBERG Server.....	75
Modifying an Application Profile.....	76
Deleting an Application Profile.....	76
Chapter 7: Understanding and Creating Policy Rules.....	77
About Policy Rules.....	78
Structure and Evaluation of Policy Rules.....	78
Structure of Policy Rules.....	78
Evaluating Policy Rules.....	79
Creating a Policy.....	81
Modes and the Policy Wizard.....	84
Parameters Within Policy Rules.....	85
Conditions for Writing Policy Rules.....	85
Request Conditions.....	86

Application Conditions.....	89
Network Device Identity Conditions.....	95
Network Device Usage Conditions.....	98
User Conditions.....	104
Policy Context Property Conditions.....	115
Time-of-Day Conditions.....	117
Actions for Writing Policy Rules.....	119
Mandatory Policy-Processing Actions.....	120
Optional Policy-Processing Actions.....	121
Policy Rule Variables.....	123
Using Policy Rule Variables.....	123
Basic Policy Rule Variables.....	123
Policy Rule Examples.....	127

Chapter 8: Managing Policy Rules.....129

Displaying a Policy.....	130
Deploying Policy Rules.....	130
Modifying and Deleting a Policy.....	133
Modifying a Policy.....	133
Deleting a Policy.....	134
Policy Templates.....	134
Creating a Policy Template.....	135
Modifying a Policy Template.....	135
Deleting a Policy Template.....	136
Managing a Policy Group.....	136
Creating a Policy Group.....	137
Adding a Policy or a Policy Group to a Policy Group.....	137
Removing a Policy from a Policy Group.....	138
Changing the Sequence of Policies or Policy Groups Within a Policy Group.....	138
Displaying Policy Details Contained Within a Policy Group.....	139
Deploying a Policy or Policy Group to MPE Devices.....	139
Removing a Policy from a Policy Group on an MPE Device.....	140
Removing a Policy or Policy Group from an MPE Device.....	141
Changing the Sequence of Deployed Policies or Policy Groups.....	141
Importing and Exporting Policies, Policy Groups, and Templates.....	142
Importing Policies.....	142
Exporting Policies.....	142

Chapter 9: Managing Subscribers.....144

Creating a Tier.....	145
----------------------	-----

Displaying Subscriber Activity History.....	145
Displaying Real-time Subscriber Statistics.....	146
Deleting a Tier.....	147
Creating an Account.....	147
Modifying an Account.....	148
Updating Accounts.....	148
Deleting an Account.....	149
Static IP Addresses.....	149
Configuring a Static IP Address.....	150
Deleting a Static IP Address from a Subscriber Account.....	150
Provisioning Static IP Addresses Using XML.....	151
Chapter 10: System-Wide Report.....	152
Viewing Active Alarms.....	153
Viewing the Alarm History Report.....	154
Chapter 11: Upgrade Manager.....	156
About ISO Files on Servers.....	157
ISO Maintenance Elements.....	157
Viewing the ISO Status of Servers.....	158
Pushing a Script to a Server.....	158
Adding an ISO File to a Server.....	159
Deleting an ISO File from a Server.....	159
About Performing an Upgrade.....	160
About Preparing for an Upgrade.....	160
System Maintenance Elements.....	160
Viewing Upgrade Status of Servers.....	162
Changing maxMsgSize Configuration After Upgrading from 10.4 to 10.4.x.....	162
Chapter 12: System Administration.....	164
Configuring System Settings.....	165
Importing and Exporting Configurable Objects.....	167
Using the OSSI XML Interface.....	167
Importing an XML File to Input Objects.....	168
Exporting an XML File.....	169
The Manager Report.....	170
The Trace Log.....	170
Viewing the Trace Log.....	171
Modifying the Trace Log Configuration.....	171

Viewing the Audit Log.....	172
Searching for Audit Log Entries.....	173
Exporting Audit Log Data.....	174
Purging Audit Log Data.....	174
Managing Scheduled Tasks.....	175
Configuring a Task.....	175
About Managing Users.....	177
Configuring Roles.....	177
Creating a Role.....	177
Modifying a Role.....	179
Deleting a Role.....	180
Creating a New Scope.....	180
Modifying a Scope.....	181
Deleting a Scope.....	181
Creating a User Profile.....	181
Modifying a User Profile.....	182
Deleting a User Profile.....	183
About Locking and Unlocking User Accounts.....	183
Changing a Password.....	184
Appendix A: CMP Modes.....	186
The Mode Settings Page.....	187
Glossary.....	190

List of Figures

Figure 1: The Policy Management Solution and MPE Devices.....19

Figure 2: Structure of the CMP Wireline GUI.....21

Figure 3: Policy Management Topology.....27

Figure 4: High Availability.....28

Figure 5: Cluster Settings Page for MPE Cluster.....32

Figure 6: Group View49

Figure 7: Select Network Elements.....67

Figure 8: Add Network Element Page.....69

Figure 9: Selecting a condition.....82

Figure 10: Selecting an action.....83

Figure 11: Naming a policy.....84

Figure 12: Example of a Parameter Pop-up.....85

Figure 13: Sample Policy Description.....130

Figure 14: Policy Deployment.....131

Figure 15: Policy Group Deployment.....132

Figure 16: Policy Redeployment.....133

Figure 17: Modify Policy Template Window.....136

Figure 18: Policy server selection window.....140

Figure 19: Sample Active Alarms Report.....153

Figure 20: Alert Details.....155

Figure 21: Sample Password Strength Policy.....167

Figure 22: Audit Log.....172

Figure 23: Audit Log Details.....173

Figure 24: Schedule Task Administration - OM Statistics.....176

Figure 25: Scheduled Task Administration.....176

Figure 26: Mode Settings Page.....189

List of Tables

Table 1: SNMP Attributes.....	35
Table 2: Associations Configuration Options.....	42
Table 3: Diameter Configuration Options.....	43
Table 4: VoD Server Synchronization Configuration Options.....	43
Table 5: B-RAS Server Synchronization Configuration Options.....	43
Table 6: B-RAS Buffers Configuration Options.....	44
Table 7: Load Shedding Configuration Options.....	44
Table 8: Policy Condition Categories.....	85
Table 9: Basic Policy Rule Variables.....	124
Table 10: ISO Maintenance Elements.....	157
Table 11: System Maintenance Elements.....	160

Chapter 1

Introduction

Topics:

- *Introduction.....13*
- *How This Guide is Organized.....13*
- *Scope and Audience.....13*
- *Related Publications.....14*
- *Locate Product Documentation on the Oracle Help Center Site.....15*
- *Customer Training.....15*
- *My Oracle Support (MOS).....16*
- *Emergency Response.....16*

This chapter contains an overview of the manual, describes how to obtain help, where to find related documentation, and provides other general information.

Introduction

This guide describes how to use the Oracle Communications Policy Management Configuration Management Platform (CMP) system to configure and manage Policy Management devices in a wireline network.

How This Guide is Organized

The information in this guide is presented in the following order:

- *Introduction* provides general information about the organization of this guide, related documentation, and how to get technical assistance.
- *The Oracle Communications Policy Management Solution* provides an overview of the Multimedia Policy Engine (MPE) device, which manages:
 - Multiple network-based client sessions
 - The network in which the MPE device operates
 - Policies
 - The Oracle Communications Policy Management Configuration Management Platform (CMP) system, which controls MPE devices and associated applications.
- *Configuring the Policy Management Topology* describes how to set the topology configuration.
- *Managing Multimedia Policy Engine Devices* describes how to use the CMP system to configure and manage the MPE devices in a network.
- *Managing Network Elements* describes how to manage network elements.
- *Managing Application Profiles* describes how to manage application profiles.
- *Understanding and Creating Policy Rules* describes policy rules, which dynamically control how an MPE device processes protocol messages as they pass through it.
- *Managing Policy Rules* describes how to manage your library of policy rules and policy groups.
- *Managing Subscribers* describes how to manage subscriber tiers and accounts within the CMP system.
- *System-Wide Report* describes the reports available on the function of Policy Management systems in your network.
- *Upgrade Manager* describes the purpose of the Upgrade Manager GUI page and the elements found on that page.
- *System Administration* describes functions reserved for CMP system administrators.
- The appendix, *CMP Modes*, lists the functions available in the CMP system, as determined by the operating modes and sub-modes selected when the software is installed.

Scope and Audience

This guide is intended for the following trained and qualified service personnel who are responsible for operating Policy Management devices:

- Network operators, who configure, operate, monitor, and maintain Policy Management systems in a carrier network
- System administrators, who maintain the accounts of users of CMP systems

Related Publications

The Policy Management product set includes the following publications, which provide information for the configuration and use of Policy Management products in the following environments:

Cable

- *Feature Notice*
- *Cable Release Notes*
- *Roadmap to Hardware Documentation*
- *Policy Wizard*
- *CMP Cable User's Guide*
- *Troubleshooting Reference*
- *SNMP User's Guide*
- *OSSI XML Interface Definitions Reference*
- *Platform Configuration User's Guide*
- *Bandwidth on Demand Application Manager User's Guide*
- *PCMM specification PKT-SP-MM-I06* (third-party document, used as reference material for PCMM)

Wireless

- *Feature Notice*
- *Wireless Release Notes*
- *Roadmap to Hardware Documentation*
- *Policy Wizard*
- *CMP Wireless User's Guide*
- *Multi-Protocol Routing Agent User's Guide*
- *Troubleshooting Reference*
- *SNMP User's Guide*
- *OSSI XML Interface Definitions Reference*
- *Analytics Data Stream Reference*
- *Platform Configuration User's Guide*
- *Message Distribution Function Reference*

Wireline

- *Feature Notice*
- *Wireline Release Notes*
- *Roadmap to Hardware Documentation*
- *CMP Wireline User's Guide*
- *Troubleshooting Reference*
- *SNMP User's Guide*
- *OSSI XML Interface Definitions Reference*
- *Platform Configuration User's Guide*

Other Publications

The following documents are useful for reference:

- 3rd Generation Partnership Project (3GPP) technical specifications:
 - 3GPP TS 23.203: "Policy and charging control architecture (Release 8)"
 - 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows (Release 6)"
 - 3GPP TS 29.212: "Policy and Charging Control over Gx/Sd reference point (Release 11)"
 - 3GPP TS 29.214: "Policy and Charging Control over Rx reference point (Release 8)"
 - 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 8)"
 - 3GPP TS 32.240: "Charging architecture and principles (Release 8)"
 - 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications (Release 8)"
- RFC 3164: "The BSD syslog Protocol"

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

<http://education.oracle.com/communication>

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
 - For Technical issues such as creating a new Service Request (SR), Select **1**
 - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Chapter 2

The Oracle Communications Policy Management Solution

Topics:

- *The Multimedia Policy Engine.....18*
- *Understanding Policy Rules.....20*
- *The Oracle Communications Policy Management Configuration Management Platform.....20*
- *Overview of Main Tasks.....24*

This chapter provides an overview of the major elements of the Policy Management solution. The major elements include:

- The Oracle Communications Policy Management Configuration Management Platform (CMP) system controls MPE devices and associated applications.
- The Oracle Communications Policy Management Multimedia Policy Engine (MPE) device manages multiple network-based client sessions.

The Multimedia Policy Engine

The Multimedia Policy Engine (MPE) device provides a policy and charging rules function (PCRF) as defined in the 3rd Generation Partnership Project (3GPP) technical specification “Policy and charging control architecture” (TS 23.203). The MPE device includes a simple, powerful, and flexible policy rules engine. Through the use of policy rules, you can modify the behavior of an MPE device dynamically as it processes protocol messages.

A policy is a set of operator-created business rules. These business rules control how subscribers, applications, and network resources are used. Policies define the conditions and actions used by a carrier network to determine how network resources are allocated and used and how applications and subscribers are treated.

The MPE device provides Call Admission Control (CAC) to support video on demand (VoD). [Figure 1: The Policy Management Solution and MPE Devices](#) shows how the Oracle Policy Management solution fits into a wireline network containing VoD servers and bandwidth remote access server (B-RAS) routers.

The major elements of a Policy Management network are:

- MPE devices — Provide policy control decisions and flow-based charging control. When a request for a policy decision is received for a subscriber session, the MPE device obtains subscriber information, evaluates the applicable policies, and directs the enforcement device to handle the session based on policy rules.
- Oracle Communications Policy Management Configuration Management Platform (CMP) — Provides the policy console. The CMP system contains a centralized repository for configuration information that is used by MPE devices to make CAC decisions, including policy rules, policy objects, network elements, bandwidth allocation per interface, element links, and subscriber data. Carriers can exchange database information in eXtensible Markup Language (XML) format with an office support system (OSS). The Policy Management network can communicate with a network management station (NMS) using Simple Network Management Protocol (SNMP).

The Policy and Charging Enforcement Function (PCEF) receives requests to start new sessions for subscribers. An example of a PCEF is a B-RAS device. MPE devices communicate with PCEFs to receive requests for policy decisions and send those policy decisions to PCEFs for implementation.

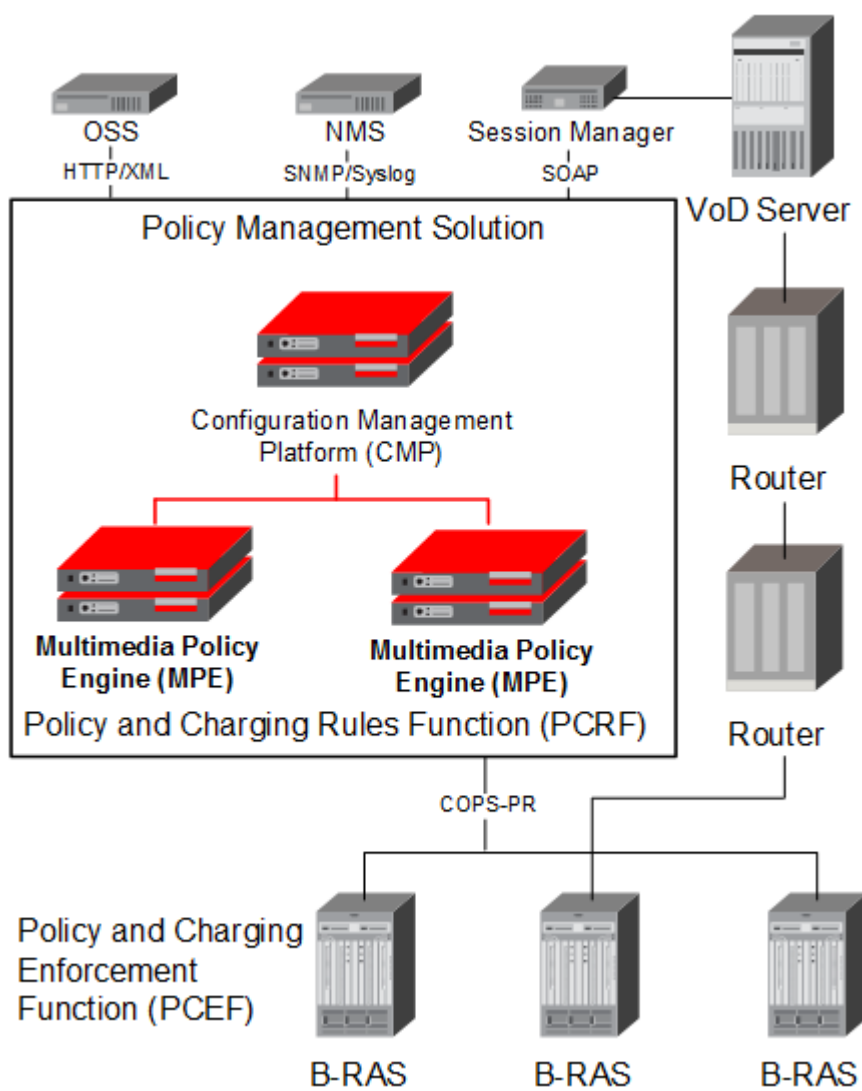


Figure 1: The Policy Management Solution and MPE Devices

Configuration information is pushed to the CMP database by an OSS system or manually configured using the CMP Graphical User Interface (GUI). The CMP device is responsible for pushing this data to MPE devices in the network.

A B-RAS router connects to the MPE device using the COPS-PR protocol, and once a connection is established, the MPE device synchronizes with the B-RAS router configuration information, providing the MPE device with the current list of subscribers connected to the B-RAS router.

As users connect to or disconnect from the network, the B-RAS router notifies the MPE device about the users' IP addresses. This information is later used by the MPE device in making CAC decisions.

When a user generates a VoD request, a Session Manager device requests a CAC decision from an MPE device. The MPE device, using the IP address of the subscriber and the VoD server in the request, determines a path between the source (the VoD server) and the destination (the B-RAS router) that would be used for the video data stream. This path could consist of multiple network segment hops; for example, the path could be from the VoD server to a video distribution router, to a video aggregation

router, to a gateway router (GWR). Once it has the path, the MPE device runs the path through configured policies that limit the usage on the segments in the path. If any one of the segments fails a policy test, the MPE device returns a CAC failure message to the Session Manager. If all the segments in the path pass the policy test, the MPE device returns a CAC success message to the Session Manager.

Understanding Policy Rules

A policy rule is an if-then statement that has a set of conditions and actions. If the conditions are met, the actions are performed. You create policy rules within the CMP database, using a policy wizard that organizes a large number of conditions and actions to assist you in the construction of policy rules. After you create policy rules, you manually deploy the rules to MPE devices.

You can combine policy rules to provide additional power and flexibility. When there are multiple policy rules, the order in which the policy rules are evaluated can also influence MPE device activity, so the order of evaluation is also configurable through the CMP system. You can also organize policy rules into groups to simplify the management of policy rules. You can cause groups of rules to be executed.

The following are sample scenarios for which you might use policy rules:

- You can modify the contents of protocol messages using policy rules. For example, you could use a policy rule to override the requested bandwidth parameters in a request.
- You can create policy rules that track the use of resources for devices in the network and implement limits on how those resources are used.
- Some protocols allow for the provisioning of default QoS parameters for subscribers. With these protocols, policy rules can implement subscriber tiers where different subscribers have different bandwidth available.
- You can configure policy rules to monitor the reservation of bandwidth on network elements and notify operators when an element exceeds certain threshold levels.

The Oracle Communications Policy Management Configuration Management Platform

The Oracle Communications Policy Management Configuration Management Platform (CMP) provides centralized management and administration of policy rules, Policy Management devices, associated applications, and manageable objects, all from a single management console. This management console is browser-based and supports the following features and functions:

- Definition of network elements
- Creation, modification, deletion, and deployment of policy rules
- Creation, modification, and deletion of objects that can be included in policy rules
- Monitoring of individual product subsystem status
- Administration and management of CMP users
- Upgrading the software on Policy Management devices

Organizing Policy Rules

The CMP system includes features to simplify the management of multiple policy rules.

The order in which rules are evaluated is important. The CMP system lets you configure the evaluation order of policies. See [Structure and Evaluation of Policy Rules](#).

The CMP system provides a policy template feature to simplify the creation of multiple policy rules that have similar conditions and actions. After you create a policy template, you can use it to create additional rules. See [Creating a Policy Template](#).

The CMP system also provides a policy rule grouping feature. Policy rules can be organized into groups and the groups can be used to simplify the process of deploying policies to MPE devices. See [Creating a Policy Group](#).

GUI Overview

You interact with the Configuration Management Platform (CMP) system through an intuitive and highly portable graphical user interface (GUI) supporting industry-standard web technologies (SSL, HTTP, HTTPS, IPv4, and XML). [Figure 2: Structure of the CMP Wireline GUI](#) shows the layout of the CMP GUI.

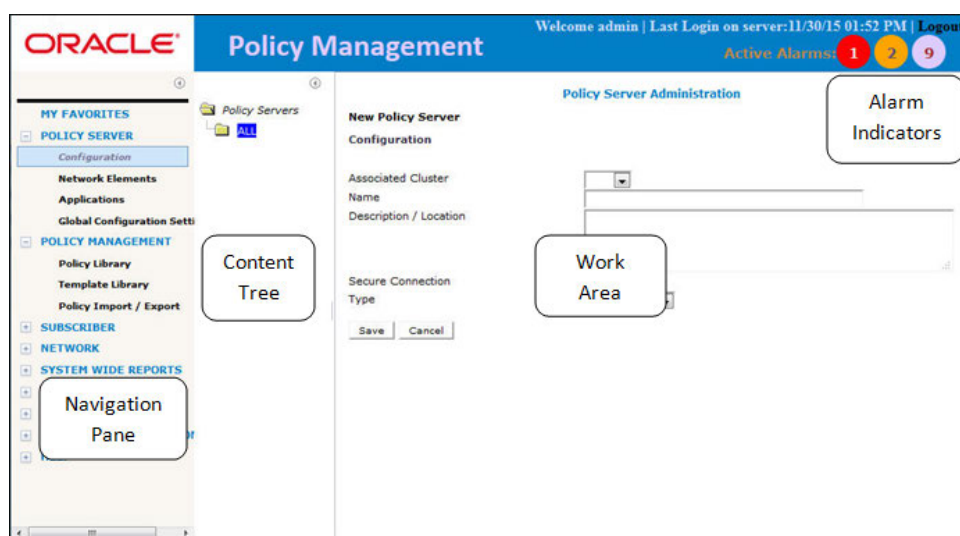


Figure 2: Structure of the CMP Wireline GUI

Navigation Pane

Provides access to the various available options configured within the CMP system.

You can bookmark options in the navigation pane by right-clicking the option and selecting **Add to Favorite**. Access the bookmarks by clicking the **My Favorites** folder at the top of the navigation pane. Within the **My Favorites** folder, you can arrange or delete options by right-clicking the option and selecting **Move Up**, **Move Down**, or **Delete from Favorite**.

You can collapse the navigation pane to make more room by clicking the button in the top right corner of the pane (⊞). Click the button again to expand the pane.

Content Tree	<p>Contains an expandable/collapsible listing of all the defined items for a given selection. For content trees that contain a group labeled ALL, you can create customized groups that display in the tree.</p> <p>The content tree section is not visible with all navigation selections.</p> <p>You can collapse the content tree to make more room by clicking the button in the top right corner of the pane (⊞). Click the button again to expand the tree. You can also resize the content tree relative to the work area.</p>
Work Area	<p>Contains information that relates to choices in both the navigation pane and the content tree. This is the area where you perform all work.</p>
Alarm Indicators	<p>Provides visual indicators that show the number of active alarms.</p>

Specifications for Using the GUI

You interact with the CMP system through a web browser graphical user interface (GUI). To take best advantage of the GUI, Oracle recommends the following:

- | | |
|---------------------|--|
| Web Browsers | <ul style="list-style-type: none">• Mozilla Firefox release 23.0.1 or higher• Microsoft Internet Explorer 9.0 or higher |
|---------------------|--|

Monitor	Use a resolution of 1024 x 768 or higher
----------------	--

Note: When using the CMP system for the first time, Oracle recommends that you change the default user name and password to a self-assigned value. See [Changing a Password](#) for details.

Logging In

The CMP system supports either HTTP or HTTPS access. Access is controlled by a standard username and password login scheme.

Note: The CMP system also supports carrier-specific network authentication and authorization environments. For information on setting up an alternate login process, see [System Administration](#).

Before logging in, you need to know the following:

- The IP address of the CMP system
- Your assigned username
- The account password

Note: As delivered, the profile **admin** provides full access privileges, and is the assumed profile used in all procedures described in this document. The default username of this profile is **admin** and the default password is **policies**. You cannot delete this user profile, but you should immediately change the password. See [Changing a Password](#).

To log in:


1. Open a web browser and enter the IP address of the CMP system.
The login page opens.
2. Enter the following information in the appropriate fields:


- a) **Username**
 - b) **Password**
3. Click **Login**.
The main page opens.


You are logged in.

GUI Icons


The CMP GUI provides the following icons to perform actions or indicate status:

 **Add** The CMP GUI provides icons for removing, deleting, or changing the sequential order of items displayed in a list:

 **Remove icon** — When visible in the work area, selecting the Remove icon removes an item from the group it is associated with. The item is still listed in the ALL group and any other group that it is currently associated with. For example, if you remove MPE device PS_1 from policy server group PS_Group2, PS_1 still displays in the ALL group.

 **Delete icon** — When visible in the work area, selecting the Delete icon deletes an item, removing it from the MPE device.

Note: Deleting an item from the **ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.

 **Move icon** — The up/down arrow icons are displayed when it is possible to change the sequential order of items in a list.

Use this icon to add an item to a list.

Shortcut Selection Keys

The CMP GUI supports the following standard browser techniques for selecting multiple items from a list:

Shift + click Selects two or more consecutive items. To select consecutive items, select the first item, then press Shift and click the last item to select both items and all items in between.

Control + click Selects two or more non-consecutive items. To select multiple non-consecutive items, hold down the Ctrl key as you click each item.

Changing a Password

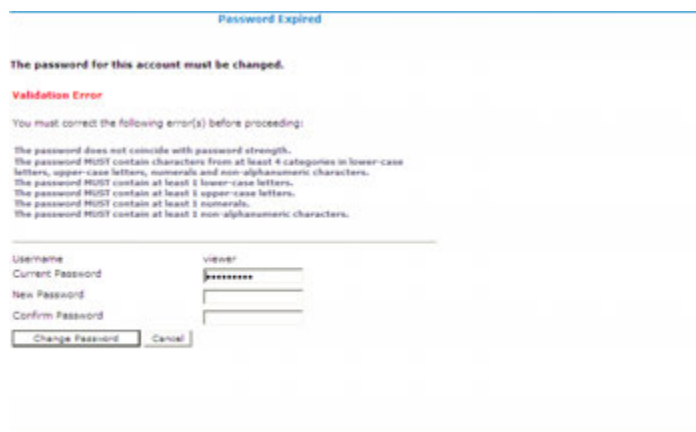
The Change Password option lets users change their password. This system administration function is available to all users.

Note: The **admin** user can change the password for any user.

Note: To reset the administrator password, contact My Oracle Support.

To change your password:

1. From the **System Administration** section of the navigation pane, select **Change Password**.
The **Change Password** page opens. If your account is set up with a password expiration period, the expiration date is displayed.
2. Enter the following information:
 - a) **Current Password** — The present value of the password.
 - b) **New Password** — The value of the new password.
This value is case sensitive and must conform to the password strength rules. The password cannot contain the user name.
 - c) **Confirm Password** — Enter the new password value again.
If your new password does not conform to the password strength rules, a validation error message appears; for example:



The screenshot shows a web page titled "Password Expired". The main message is "The password for this account must be changed." Below this is a red "Validation Error" section stating "You must correct the following error(s) before proceeding:". The error details are: "The password does not coincide with password strength. The password MUST contain characters from at least 4 categories in lower-case letters, upper-case letters, numerals and non-alphanumeric characters. The password MUST contain at least 3 lower-case letters. The password MUST contain at least 3 upper-case letters. The password MUST contain at least 3 numerals. The password MUST contain at least 3 non-alphanumeric characters." Below the error message is a form with fields for "Username" (value: viewer), "Current Password" (masked with asterisks), "New Password", and "Confirm Password". At the bottom of the form are "Change Password" and "Cancel" buttons.

3. When you finish, click **Change Password**.
Your password is changed.

Overview of Main Tasks

The major tasks involved in using MPE devices are configuration, defining manageable elements and profiles, creating and deploying policy rules, and administering the authorized CMP users.

The configuration tasks are a series of required steps that must be completed in the following order:

1. Configure the Policy Management topology, which defines the addresses of Policy Management clusters in your network. These steps are described in [Configuring the Policy Management Topology](#).

The element and profile definition tasks you need to perform depend on what exists on your network. They can be defined in any order at any time as needed. Once elements and profiles are defined, you can refer to them in policy rules. The complete set of tasks follows:

- Create network element profiles, including protocol options, for each network element with which the MPE devices interact. This task is described in [Managing Network Elements](#).
- Specify which MPE device will interact with which network elements. This task is described in [Managing Network Elements](#).
- Create application profiles, which specify protocol information to associate each request with an application. This task is described in [Managing Application Profiles](#).

The steps to create and deploy policy rules must be done in the following order:

1. Create policy rules in the CMP database. This step is described in [Understanding and Creating Policy Rules](#).
2. Deploy the policy rules from the CMP database to MPE devices. This step is described in [Managing Policy Rules](#).

The management and administrative tasks, which are optional and performed only as needed, are as follows:

- Manage subscriber tiers and accounts. This task is described in [Managing Subscribers](#).
- View reports the function of the Policy Management systems in your network. This task is described in [System-Wide Report](#).
- Manage CMP users, accounts, access, authorization, and operation. This task is described in [System Administration](#).
- Upgrade software using the Upgrade Manager GUI page. This page is described in [Upgrade Manager](#).

Chapter 3

Configuring the Policy Management Topology

Topics:

- *About the Policy Management Topology.....27*
- *Setting Up the Topology.....29*
- *Modifying the Topology.....32*
- *Configuring SNMP Settings.....35*
- *Defining Global Configuration Settings.....37*

This chapter describes how to configure the Policy Management devices into a network and how to configure the CMP system to manage them.

About the Policy Management Topology

You need to configure a network topology for the Policy Management products (CMP and MPE devices). The topology determines the following:

- How clusters are set up
- How configuration data is replicated
- How incidents (events and alarms) get reported to the CMP system that controls the Policy Management network.

Figure 3: Policy Management Topology illustrates a Policy Management topology consisting of a CMP cluster and two MPE clusters.

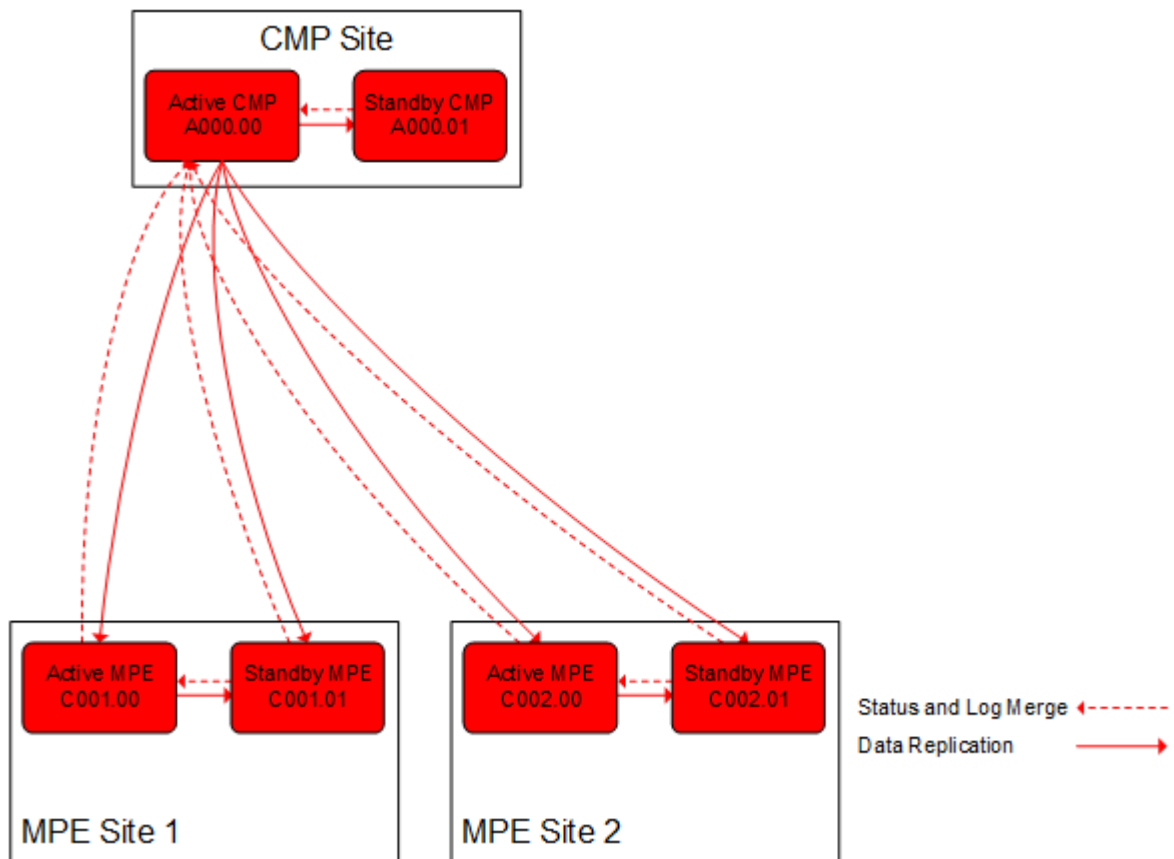


Figure 3: Policy Management Topology

High Availability

High Availability (HA) is provided for all Policy Management cluster configurations. HA is accomplished by using two servers per cluster, an active server and a standby server. As shown in *Figure 4: High Availability*, the active server processes network traffic and is accessible and connected to external devices, clients, gateways, and so forth. Only one server in a cluster can be the active server.

Configuring the Policy Management Topology

Within the cluster, the servers are connected together and work collaboratively, as follows:

1. The active and standby servers communicate using a TCP connection over the backplane network (direct-link High Availability) to replicate current state data, monitor server heartbeats, and merge alarms. Separating OAM and signaling traffic allows the ability to shut down one network without affecting the other, and also the opportunity to include separate and redundant signaling (SIG-A and SIG-B) networks.
2. The servers share a virtual IP (VIP) cluster address to support automatic failover. The active server controls the VIP address.
3. The standby server does not receive any live traffic load, but holds an up-to-date copy of the active session state data at all times, replicated by High Availability. (This is sometimes called a warm standby.)
4. The COMCOL database runtime process constantly monitors the status of both servers in the cluster.
5. If the active server fails, it instructs the standby server to take over and become the active server.

The terms active and standby denote roles, or states, that the servers assume, and these roles, or states, can change based on decisions made by the underlying COMCOL database, automatically and at any time. If necessary, the standby server assumes control and becomes the active server. (For example, this would occur if the active server became unresponsive as determined by lack of a heartbeat signal.) When this happens, the server that was previously the active server assumes the role, or state, of the standby server.

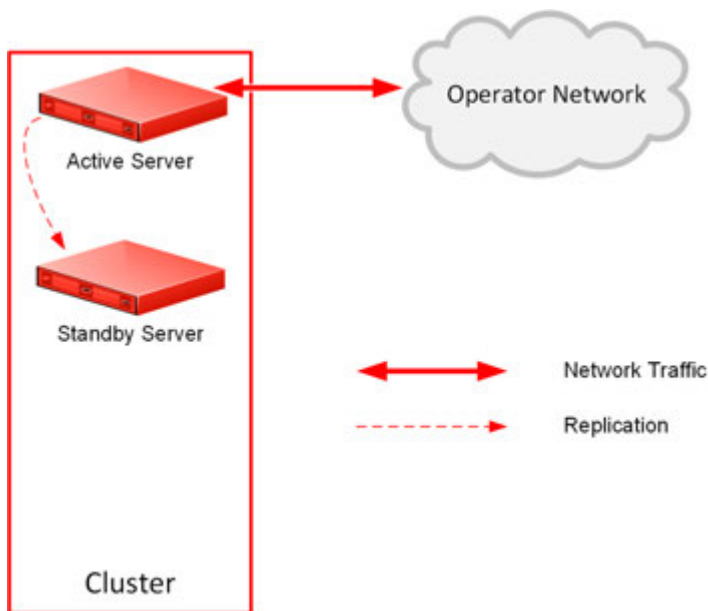


Figure 4: High Availability

Server Status

You can display the status of a server in the Cluster Information Report (see [Cluster Information Report](#)). The display refreshes every 10 seconds.

The status of a server can be thought of as its current role. The status describes what function the server is currently performing in the cluster. Statuses can change from server to server within a cluster,

but no two servers in the same cluster should ever have the same status. (Two servers in the same cluster with the same status is an error condition.)

The status values are as follows:

- **Active:** The active server in a cluster is the server that is the externally connected. The active server is the only server that is handling connections and servicing messages and requests. Only the active server writes to the database.
- **Standby:** The standby server in a cluster is the server that is prepared to immediately take over in the event that the current active server is no longer able to provide service. If the standby server takes over, it becomes the active server. Once the previously active server has recovered, it reverts to its former status of standby server.
- **Out of Service (OOS):** If a server has failed and is unavailable to assume any of the other roles, then its status is out of service. A server is reported as out of service in two scenarios:
 - The CMP system can reach the server, but the software service on the server is down
 - The CMP system cannot reach the server

Setting Up the Topology

Topology configuration defines the Policy Management sites and clusters, including their addresses and hierarchy. The CMP system uses this information to establish communications with the servers and clusters it manages. You can add MPE clusters to the topology before configuring the individual servers themselves. You can define all the servers in a cluster in the same operation.

The recommended sequence of creating the Policy Management topology is as follows:

1. Configure the primary CMP cluster — You start to build a topology by logging in to the active CMP server. Configure the CMP cluster settings. The settings are replicated (pushed) to the standby CMP server. Together, the two servers form the primary CMP site for the whole topology network. The primary site cannot be deleted from the topology.
2. Configure MPE clusters — Enter MPE cluster settings on the active CMP server on the primary site. You can define the topology before defining the servers themselves. Once defined, the configuration information is replicated as follows:
 - a. The topology configuration, including the cluster settings, is replicated to the active and standby servers. These servers form an MPE cluster based on the topology configuration.
 - b. The servers share a virtual IP (VIP) cluster address to support automatic failover.
 - c. A monitoring process constantly monitors the status of the servers in each cluster. If an active server fails, it instructs the standby server to take over and become the active server.

Once you define the topology, use the System tab of each policy server profile to determine if there are any topology mismatches. See [Reapplying the Configuration to a Policy Server](#) for more information.

Setting Up the CMP Cluster

You must define a CMP cluster before continuing with the topology. The site you define will be the primary (Site 1) cluster.

Before defining the cluster, ensure the following:

Configuring the Policy Management Topology

- The CMP software is installed on all servers in the cluster
- The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses
- The CMP server IP connection is active
- The CMP application is running on at least one server

To set up the CMP cluster:

1. Log in to the CMP server.
2. From the **Platform Setting** section of the navigation pane, select **Topology Setting**. The Topology Configuration page opens.
3. From the content tree, select the **All Clusters** group. The Cluster Configuration page opens.
4. Click **Add CMP Site1 Cluster**. The Cluster Settings Page opens. The cluster name and application type are fixed.
5. Enter the following information:
 - a) **HW Type** — Select **RMS** (for a rack-mounted server).
 - b) **OAM VIP** (required) — Enter the IPv4 address and mask of the OAM VIP. The OAM VIP is the IP address the CMP uses to communicate with a Policy Management cluster. Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.
Note: This address corresponds to the cluster address in Policy Management systems before V7.5.
 - c) **Signaling VIP 1** through **Signaling VIP 4** (optional) — Enter up to four IPv4 addresses and masks of the signaling virtual IP (VIP) addresses; for each, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. You must enter a Signaling VIP value if you specify either SIG-A or SIG-B. If you enter an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32.
6. Select **Server-A** and enter the following information for the first server of the cluster (which will be the initial active server):
 - a) **IP** (required) — The IP address of the server. Enter the standard dot-formatted IP address string.
 - b) **HostName** (required) — The name of the server. This must exactly match the host name provisioned for this server (that is, the output of the Linux command `uname -n`).
 - c) **Forced Standby** — Select to force this server into standby mode. The flag is set automatically when a new server is added to a cluster, or if a server setting is modified and another server already exists in the cluster.
7. Once you define a Server A, you can select **Server-B** to enter the appropriate information for the second server of the cluster.
8. When you finish, click **Save**.
A confirmation message appears and the active server restarts.

The CMP cluster topology is defined.

Once you define the topology, use the **System** tab of each policy server profile to determine if there are any topology mismatches. See [Reapplying the Configuration to a Policy Server](#) for more information.

Setting Up an MPE Cluster

Before defining an MPE cluster, ensure the following:

Configuring the Policy Management Topology

- The MPE software is installed on all servers in the cluster
- The servers have been configured with network time protocol (NTP), domain name server (DNS), IP Routing, and OAM IP addresses
- The MPE server IP connection is active
- The MPE application is running on at least one server

To define an MPE cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
The Cluster Configuration page opens.
2. Click **Add MPE/MRA Cluster**.
The Topology Configuration Page opens.
3. Enter the following information ([Figure 5: Cluster Settings Page for MPE Cluster](#) shows an example):
 - a) **Name** (required) — Name of the cluster. Enter up to 255 characters, excluding quotation marks (") and commas (,).
 - b) **Appl Type** — Select **MPE** (the default).
 - c) **HW Type** — Select **RMS** (for a rack-mounted server).
 - d) **OAM VIP** (optional) — Enter the IPv4 address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the IP address the CMP cluster uses to communicate with the MPE cluster. Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.
Note: This address corresponds to the cluster address in Policy Management systems before V7.5.
 - e) **Signaling VIP 1** through **Signaling VIP 4** — Enter up to four IPv4 addresses and masks of the signaling virtual IP (VIP) addresses; for each, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. The Signaling VIP is the IP address a PCEF device uses to communicate with an MPE cluster. (To support redundant communication channels, an MPE cluster uses both **SIG-A** and **SIG-B**.) You must enter a Signaling VIP value if you specify either SIG-A or SIG-B. If you enter an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For a CMP cluster, the Signaling VIP is optional, but for an MPE cluster, at least one signaling VIP, either SIG-A or SIG-B, is required.
4. Select **Server-A** and enter the following information for the first server of the cluster:
 - a) **IP** (required) — The IPv4 address of the server. Enter the standard dot-formatted IPv4 address string.
 - b) **HostName** (required) — The name of the server. This must exactly match the host name provisioned for this server (that is, the output of the Linux command `uname -n`).
5. Once you define Server A, you can optionally click **Add Server-B** and enter the appropriate information for the second server of the cluster.
6. Click **Save**.
7. If you are setting up multiple clusters, repeat the above steps as often as necessary.

The MPE cluster is defined.

Once you define the topology, use the System tab of each policy server profile to determine if there are any topology mismatches. See [Reapplying the Configuration to a Policy Server](#) for more information.

Topology Configuration

Cluster Settings

Name:

Appl Type:

HW Type:

OAM VIP: /

Signaling VIP 1: /

Signaling VIP 2: /

Signaling VIP 3: /

Signaling VIP 4: /

	None	SIG-A	SIG-B
	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Server-A	Server-B
IP: 10.60.30.202	
HostName: mpe202	
Forced Standby: No	
Status: active	

Figure 5: Cluster Settings Page for MPE Cluster

Modifying the Topology

Once the topology is configured, you can change it as necessary—to correct errors, add a server to a cluster, define new clusters, or put an active server into standby status.

You can modify a cluster even if the standby server is off line. However, you cannot modify or delete the active server of a cluster.

Modifying the topology is described in the following topics:

- [Modifying an MPE Cluster](#)
- [Modifying a CMP Cluster](#)
- [Removing a Cluster from the Topology](#)
- [Forcing a Server into Standby Status](#)

Modifying an MPE Cluster

To modify an MPE cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**. The Topology Configuration page opens.
2. From the content tree, select the cluster you want to modify. The Topology Configuration page opens, displaying information about the cluster.

3. On the Topology Configuration page, click the appropriate button for the changes you want to make:
 - To modify cluster settings, click **Modify Cluster Settings**.
 - To modify the primary server, click **Modify Server-A**.
 - To modify the secondary server, click **Modify Server-B**.

The appropriate fields on the Topology Configuration page become editable.

4. Make changes as required.

You must make changes to each section individually. You can remove either server from a cluster, but not both. You can select **Forced Standby** on one or more servers of an MPE cluster.



Caution: If you force all servers in a cluster into the Standby state, then no server can be active, which effectively removes the cluster from service.

Note: If you add, remove, or modify a server, the active server restarts.

5. When you finish, click **Save** (or **Cancel** to discard your changes).
You are prompted, "Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect."
6. Click **OK** (or **Cancel** to discard your changes).

The cluster is modified. You can determine if there is a topology mismatch by using the System tab of each policy server profile.

Modifying a CMP Cluster

To modify a CMP cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
The **Cluster Configuration** page opens.
2. From the content tree, select the cluster.
The **Topology Configuration** page opens, displaying information about the cluster.
3. Click the button for the changes you want to make:
 - To modify cluster settings, click **Modify Cluster Settings**.
 - To modify the configuration of the first server defined in the cluster, click **Modify Server-A**.
 - To modify the configuration of the second server defined in the cluster, click **Modify Server-B**.

The fields on the **Topology Configuration** page become editable. For information on configurable fields, see [Setting Up the CMP Cluster](#).

4. Make changes.

You must make changes to each section individually. You can remove either server from the cluster, but not both. You can select **Forced Standby** on either server of the cluster, but not both, and not at all if the cluster has only one server.

Note: If you add, remove, or modify a server, the active server restarts.

5. Click **Save**.
A restart message displays.
6. Click **OK**.

The cluster is modified. You can determine if there is a topology mismatch by viewing the **System** tab for each policy server profile.

Removing a Cluster from the Topology

You can remove an MPE cluster from the topology. (You cannot remove the Site 1 (primary) CMP cluster from the topology.)



Caution: Contact Oracle Technical Support before restoring a cluster deleted from the topology.

Before removing an MPE cluster, remove the profiles of its servers; see [Deleting a Policy Server Profile](#).

To remove a cluster from the topology:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**. The Topology Configuration page opens.
2. From the content tree, select the **All Clusters** folder. The Cluster Configuration page opens, displaying a cluster settings table listing information about the clusters defined in the topology.
3. In the topology configuration table, in the row listing the cluster you want to remove, click **Delete**. You are prompted, "Are you sure you want to delete this Cluster?"
4. Click **Delete** (or **Cancel** to abandon your request). The page closes.

The cluster is removed from the topology.

Forcing a Server into Standby Status

You can change the status of an active or spare server in a cluster to Standby. You would do this, for example, to the active server prior to performing maintenance on it.

When you place a server into forced standby status, the following happens:

- If the server is active, it demotes itself.
- The server will not assume the active role, regardless of the status or roles of the other servers in the cluster.
- The server continues as part of its cluster, and reports its status as "Forced-Standby."



Caution: If you force all servers in a cluster into Standby status, you can trigger a site outage.

To force a server into standby status:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**. The Topology Configuration page opens, displaying a cluster settings table listing information about the clusters defined in the topology.
2. In the cluster settings table, in the row listing the cluster containing the server you want to force into standby status, click **View**. The Topology Configuration page displays information about the cluster.

3. Click either **Modify Server-A** or **Modify Server-B**, as appropriate.
4. Select **Forced Standby**.
5. Click **Save** (or **Cancel** to abandon your request).
The page closes.

The server is placed in standby status.

Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network.

Note: SNMP settings configuration must be done on the active server.

To configure SNMP settings:

1. Log in to the CMP system from its server address as a user with administrator privileges.
The navigation pane opens.
2. From the **Platform Setting** section of the navigation pane, select **SNMP Setting**.
The **SNMP Settings** page opens.
3. Click **Modify**.
The **Edit SNMP Settings** page opens.
4. Edit the settings.
5. Click **Save**.

Table 1: SNMP Attributes describes the SNMP attributes that can be edited.

Table 1: SNMP Attributes

Field Name	Description
Manager 1-5	SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IPv4 address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. The field is required to allow the Manager to receive traps. By default, these fields are empty. Note: The IPv6 address is not supported.
Enabled Versions	Supported SNMP versions: <ul style="list-style-type: none"> • SNMPv2c • SNMPv3 • SNMPv2c and SNMPv3 (default)

Configuring the Policy Management Topology

Field Name	Description
Traps Enabled	<p>Enable sending SNMPv2 traps (default is box check marked)</p> <p>Disable sending SNMPv2 traps (box not check marked)</p>
Traps from individual Servers	<p>Enable sending traps from an individual server (box check marked).</p> <p>Send traps only from the activeCMP system (default is box not check marked)</p>
SNMPv2c Community Name	<p>The SNMP read-write community string.</p> <p>The field is required if SNMPv2c is enabled.</p> <p>The name can contain alphanumeric characters and cannot exceed 31 characters in length.</p> <p>The name cannot be either private or public.</p> <p>The default value is snmppublic.</p>
SNMPv3 Engine ID	<p>Configured Engine ID for SNMPv3.</p> <p>The field is required If SNMPv3 is enabled.</p> <p>The Engine ID includes only hexadecimal digits (0-9 and a-f).</p> <p>The length can be from 10 to 64 digits.</p> <p>The default is no value (empty).</p>
SNMPv3 Security Level	<p>SNMPv3 Authentication and Privacy options.</p> <ul style="list-style-type: none"> • No Auth No Priv - Authenticate using the Username. No Privacy. • Auth No Priv - Authentication using MD5 or SHA1 protocol. • Auth Priv - Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol. <p>The default value is Auth Priv.</p>
SNMPv3 Authentication Type	<p>Authentication protocol for SNMPv3. Options are:</p> <ul style="list-style-type: none"> • SHA-1 - Use Secure Hash Algorithm authentication. • MD5 - Use Message Digest authentication. <p>The default value is SHA-1.</p>

Field Name	Description
SNMPv3 Privacy Type	<p>Privacy Protocol for SNMPv3. Options are:</p> <ul style="list-style-type: none"> • AES - Use Advanced Encryption Standard privacy. • DES - Use Data Encryption Standard privacy. <p>The default value is AES.</p>
SNMPv3 Username	<p>The SNMPv3 User Name.</p> <p>The field is required if SNMPv3 is enabled.</p> <p>The name must contain alphanumeric characters and cannot not exceed 32 characters in length.</p> <p>The default value is TekSNMPUser.</p>
SNMPv3 Password	<p>Authentication password for SNMPv3. This value is also used for msgPrivacyParameters.</p> <p>The field is required If SNMPv3 is enabled.</p> <p>The length of the password must be between 8 and 64 characters; it can include any character.</p> <p>The default value is snmpv3password.</p>

Defining Global Configuration Settings

This section describes how to configure global CMP settings.

Setting Stats Settings

You can define when and how measurement statistic values are reset.



Caution: Saving changes to the statistics settings causes the historical stats data to be lost.

To change stats settings:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
The content tree displays a list of global configuration settings.
2. From the content tree, select the **Stats Settings** folder.
The **Stats Settings** page opens in the work group area.
3. Click **Modify**.
The fields become editable.
4. Configure the **Stats Reset Configuration**.
 - **Manual** (default)

Configuring the Policy Management Topology

When in Manual mode, numeric values can only reset when the system restarts (for example, on failover or initial startup) or when you issue a reset command. Manual mode disables the resetting of numeric fields at regular intervals but does not alter historical data collection.

- **Interval**

When in Interval mode, numeric values are reset at regular intervals, controlled by the Stats Collection Period variable. During Interval mode, a reset occurs on the hour and then every 5, 10, 15, 20, 30 or 60 minutes afterwards, depending on the value selected in **Stats Collection Period**, providing a better idea of the performance of the Policy Management system at specific times of day. The default value is Manual.

5. Set the **Stats Collection Period**. When **Stats Reset Configuration** is set to Interval, specify the time interval from the list. Options are minutes.

- 5
- 10
- 15 (default)
- 20
- 30
- 60

6. Click **Save**.

The Stats Settings attributes are configured.

Managing Multimedia Policy Engine Devices

Topics:

- *Policy Server Profiles.....40*
- *Configuring Protocol Options on the Policy Server.....42*
- *Configuring MPE Advanced Settings.....44*
- *Policy Server Groups.....45*
- *Reapplying the Configuration to a Policy Server.....48*
- *Checking the Status of an MPE Server.....48*
- *Policy Server Reports.....50*
- *Viewing Policy Server Logs.....53*
- *VoD Session Flow Scenarios.....58*
- *Synchronizing a TANDBERG VoD Server.....59*
- *Synchronizing a B-RAS Server.....60*

This chapter describes how to use the CMP system to configure and manage the Multimedia Policy Engine (MPE) devices in a network.

Note: The MPE device is the Policy Management policy server. The terms policy server and MPE device are synonymous.

Policy Server Profiles

A policy server profile contains the configuration information for an MPE device. The CMP system stores policy server profiles in a configuration database. After you define profiles, you deploy them to MPE devices across the network.

The following subsections describe how to manage policy server profiles. For information on deploying defined policies to an MPE device, see [Deploying a Policy or Policy Group to MPE Devices](#).

Creating a Policy Server Profile

You must establish the Policy Management network topology before you can create policy server profiles.

To create a policy server profile:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Server Administration** page opens in the work area.
3. Click **Create Policy Server**.
The **New Policy Server** page opens.
4. Enter values for the configuration attributes:
 - a) **Associated Cluster** (required) — Select the cluster with which to associate this MPE device.
 - b) **Name** — Name of this MPE device. The default is the associated cluster name. A name is subject to the following rules:
 - Case insensitive (uppercase and lowercase are treated as the same)
 - Must be no longer than 255 characters
 - Must not contain quotation marks (") or commas (,)
 - c) **Description / Location** (optional) — Information that defines the function or location of this MPE device.
 - d) **Secure Connection** — Designates whether or not to use the HTTPS protocol for communication between Policy Management devices.
 - e) **Type** — Defines the policy server type:
 - **Oracle** (default) — The policy server is an MPE device and can be fully managed by the CMP.
 - **Unmanaged** — The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non-Oracle policy server.
5. Click **Save**.

The profile appears in the list of policy servers. You have defined the policy server profile.

For most protocols to function correctly, once a policy server profile is created, you must configure attribute information on the **Policy Server** tab (see [Configuring Protocol Options on the Policy Server](#)).

Once you have defined policy server profiles for the MPE devices in your Policy Management network, you can associate network elements with them (see [Managing Network Elements](#)).

Configuring or Modifying a Policy Server Profile

To configure or modify a policy server profile:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.

2. From the content tree, select the policy server.

The **Policy Server Administration** page opens in the work area.

The page contains the following tabs:

- **System** — Defines the system information associated with this policy server, including the name, host name or IP address in IPv4 format, information about the policy server, and whether or not the policy server uses a secure connection to any management system (such as the CMP).
- **Reports** (read only)— Displays various statistics and counters related to the physical hardware of the cluster, policy execution, and network protocol operation. Reports cannot be modified.
- **Logs** — Displays the Trace Log, Policy Log, Syslog, and session synchronization log configurations.
- **Policy Server** — Lets you associate applications and network elements with the MPE device and configure protocol information.
- **Policies** — Lets you manage policies that are deployed on the policy server.

3. Select the tab that contains the information you want to modify and click **Modify**.
4. Edit the configuration.
5. When you finish your modifications, click **Save**.

Deleting a Policy Server Profile

Deleting a policy server profile for an MPE device from the ALL group also deletes it from any associated group.


To delete an MPE device profile:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of server groups; the initial group is **ALL**.

2. From the content tree, select the **ALL** group.

The **Policy Server Administration** page opens in the work area.

3. Use one of the following methods to select the MPE device profile to delete:

- From the work area, click  (trash can) located next to the MPE device profile you want to delete.
- From the policy server group tree, select the MPE device. The **Policy Server Administration** page opens. Click the **System** tab, and then click **Delete**.

A confirmation message displays.

4. Click **OK** to delete the MPE device profile.
The profile is removed from the list.

The policy server profile is deleted.

Configuring Protocol Options on the Policy Server

To configure protocol options on an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the desired MPE device.
The **Policy Server Administration** page opens.
3. Select the **Policy Server** tab.
The current configuration options are displayed.
4. Click **Modify** and define options as necessary.
The following tables define the available options. (The options you see vary depending on the mode configuration of your system.)
 - [Table 2: Associations Configuration Options](#)
 - [Table 3: Diameter Configuration Options](#)
 - [Table 4: VoD Server Synchronization Configuration Options](#)
 - [Table 5: B-RAS Server Synchronization Configuration Options](#)
 - [Table 6: B-RAS Buffers Configuration Options](#)
5. Click **Save**.

You have defined the protocol options for this MPE device.

Table 2: Associations Configuration Options

Attribute	Description
Applications	The application profiles associated with this MPE device. To modify this list, click Manage .
Network Elements	The network elements associated with this MPE device. To modify this list, click Manage .
Network Element Groups	The network element groups associated with this MPE device. To modify this list, select or deselect groups.
Default Local Time Mode	Select the time used within a user's session from the drop list: <ul style="list-style-type: none"> • System Local Time to use the local time of the MPE device (default) • User Local Time to use the local time of the user <p>Note: If the time zone was never provided for the user equipment, system local time is applied.</p>

Table 3: Diameter Configuration Options

Attribute	Description
Diameter Realm	The domain of responsibility (for example, galactel.com) for the MPE device.
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, mpe3.galactel.com).
Validate wireline user	If enabled, sessions for unknown users are rejected.

Table 4: VoD Server Synchronization Configuration Options

Attribute	Description
Tandberg Interval (minutes)	The interval of time specified for synchronization between a TANDBERG VoD server and the MPE device. When a gateway establishes a new connection to the MPE device, the MPE device initiates either a full or incremental synchronization. This field accepts a numeric value of 1–99999. Note: If your attributes are defined and you want to synchronize the VoD server, click Sync Tandberg VoD Server Now . Synchronization is initiated with all known TANDBERG VoD servers within ten seconds. When the synchronization is completed, the gateway sends Address Management messages to the MPE device whenever a new user connects to or disconnects from the network.
Tandberg Application Name	Set to match the name that the TANDBERG VoD server sends. The default is OpenStream.
Tandberg Keep Alive (seconds; 0 is disabled)	The interval of time, in seconds, before the MPE device issues a KEEPALIVE status request to the TANDBERG server in the absence of any other traffic. The default value is 0 (no keepalive messages are sent). Note: The MPE device logs, but does not take any other action, if the TANDBERG server does not respond to a keepalive request.

Table 5: B-RAS Server Synchronization Configuration Options

Attribute	Description
Concurrent Bras synchronizations	When a Juniper B-RAS server connects to an MPE device, the MPE device issues a synchronization request to it. This causes the B-RAS server to send a COPS-PR request for each attached subscriber that it knows about. This can potentially result in thousands of messages being returned to the MPE device. This option limits the number of outstanding synchronization requests that the MPE device will have active at any given time. The default is 8.
Fast Sync Enabled	When enabled, when an ERX device connects to the MPE device, if the IP address it reports of the last policy server to which it connected matches the MPE device address, the MPE device sends an unsolicited Decision (DEC) message to the ERX device, which replies with just Request (REQ) and Delete (DRQ) messages instead of full state information. The default is disabled.

Table 6: B-RAS Buffers Configuration Options

Attribute	Description
TCP Send Buffer (bytes)	The default is 0 bytes.
Max Size of TCP Send Buffer (bytes)	The default is 4,194,304 bytes (4 MB).
Shrink Wait Time (milliseconds)	The default is 3,000,000 ms (50 minutes).

Table 7: Load Shedding Configuration Options

Attribute	Description
Enabled	Select to enable load shedding. You can enable or disable load shedding on individual MPE devices.

Configuring MPE Advanced Settings

The **Advanced** page provides access to factory-default attribute settings that are not normally changed.



Caution: Do not attempt to change a service override without first consulting with My Oracle Support.

To configure an advanced setting on an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select an MPE device.
The **Policy Server Administration** page opens.
3. Select the **Policy Server** tab.
The Policy Server configuration settings are displayed.
4. Click **Advanced**. Advanced configuration settings are displayed and can be edited.
 - Setting Other Advanced Configuration Settings
 - Adding a key to the table.
 1. Click **Add**. The **Add Configuration Key Value** window opens.
 2. Enter the following values:
 - **Configuration Key** — The attribute to set
 - **Value** — The attribute value

When you finish, click **Save**.



Caution: There is no input validation on values. Also, if you overwrite a setting that is configurable using the CMP GUI, the value adopted by the device is undetermined.

- Cloning a key.
 1. Select an existing key in the table.
 2. Click **Clone**. The **Clone Configuration Key Value** window opens with the information for the key.
 3. Make changes.
 4. When you finish, click **Save**.
 - Editing a key in the table.
 1. Select an existing key in the table.
 2. Click **Edit**. The **Edit Configuration Key Value** window opens with the information for the key.
 3. Make changes.
 4. When you finish, click **Save**.
 - Deleting a key from the table.
 - Select an existing key in the table.
 - Click **Delete**. A confirmation prompt displays.
 - Click **Delete** to remove the key.
5. Click **Save**.

The settings are applied to the selected MPE device.

Policy Server Groups

For organizational purposes, you can aggregate the MPE devices in your network into groups. For example, you can use groups to define authorization scopes. The following subsections describe how to manage policy server (MPE) groups.

Creating a Policy Server Group

To create a policy server group:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Server Administration** page opens in the work area.
3. Click **Create Group**.
The **Create Group** page opens.
4. Enter the name of the new policy server group.
The name cannot contain quotation marks (") or commas (,).

5. Click **Save**.

You have created a policy server group.

Adding a Policy Server to a Policy Server Group

To add a policy server to a policy server group:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server group.
The **Policy Server Administration** page opens in the work area displaying the contents of the selected policy server group.
3. Click **Add Policy Server**.
The **Add Policy Server** page opens, displaying the policy servers not already part of the group.
4. Click the policy server you want to add; press Ctrl or Shift-Ctrl to select multiple policy servers.
5. Click **Save**.

The policy server is added to the selected group.

Creating a Policy Server Sub-group

You can create sub-groups to further organize your policy server network. To add a policy server sub-group to an existing policy server group:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server group.
The **Policy Server Administration** page opens in the work area, displaying the contents of the selected policy server group.
3. Click **Create Sub-Group**.
The **Create Group** page opens.
4. Enter the name of the new sub-group.
The name cannot contain quotation marks (") or commas (,).
5. Click **Save**.

The sub-group is added to the selected group.

Renaming a Policy Server Group

To modify the name assigned to a policy server group or sub-group:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server group or sub-group.
The **Policy Server Administration** page opens in the work area.
3. Click **Modify**.

The **Modify Group** page opens.

4. Enter the new name in the **Name** field.

The name cannot contain quotation marks (") or commas (,).

5. Click **Save**.

The group is renamed.

Removing a Policy Server Profile from a Policy Server Group

Removing a policy server profile from a policy server group or sub-group does not delete the profile. To delete a policy server profile, see [Deleting a Policy Server Profile](#).

To remove a policy server profile from a policy server group or sub-group:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server group or sub-group.
The **Policy Server Administration** page opens in the work area, displaying the contents of the selected policy server group or sub-group.
3. Remove the policy server profile using one of the following methods:

Note: The policy server is removed immediately; there is no confirmation message.

- Click the **Remove** (🗑️) icon located next to the policy server you want to remove.
- From the content tree, select the policy server. The **Policy Server Administration** page opens. Select the **System** tab and click **Remove**.

The policy server is removed from the group or sub-group.

Deleting a Policy Server Group

Deleting a policy server group also deletes any associated sub-groups. However, any policy server profiles associated with the deleted group or sub-groups remain in the ALL group. You cannot delete the ALL group.

To delete a policy server group or subgroup:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server group or sub-group.
The **Policy Server Administration** page opens in the work area, displaying the contents of the selected policy server group or sub-group.
3. On the **Policy Server Administration** page, click **Delete**.
A confirmation message displays.
4. Click **OK** to delete the group.

The policy group is deleted.

Reapplying the Configuration to a Policy Server

The CMP system lets you reapply the configuration to each MPE device. When you reapply the configuration, the CMP system completely reconfigures the MPE device with topology information (such as network elements and links), ensuring that the MPE device configuration matches the data in the CMP database. This action is not needed during normal operation but is useful in the following situations:

- When the servers of a cluster are replaced, the new servers come up initially with default values. Reapplying the configuration lets you redeploy the entire configuration rather than reconfiguring the MPE device field by field. You should also apply the Rediscover Cluster operation to the CMP system to re-initialize the Cluster Information Report for the device, thereby clearing out the status of the failed servers.
- After upgrading the software on an MPE device, Oracle recommends that you reapply the configuration from the CMP system to ensure that the upgraded MPE device and the CMP database are synchronized.
- There are situations in which it is possible for an MPE device configuration to go out of synchronization with the CMP system; for example, when a break in the network causes communication to fail between the CMP system and the MPE device. If such a condition occurs, the CMP system displays the MPE device status on the **System** tab with the notation "Config Mismatch". You can click the notice to display a report comparing the MPE device configuration with the CMP database information. Reapplying the configuration synchronizes the MPE device back with the CMP database.

To reapply the configuration associated with an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Server Administration** page opens in the work area.
3. From the group **ALL**, select the MPE device.
The **Policy Server Administration** page opens to the **System** tab, displaying information for that device.
4. Click **Reapply Configuration**.
The profile information is saved to the MPE device.
5. Click **Reapply Subscriber Configuration**.
Subscriber information is saved to the MPE device.

The MPE device is synchronized with the CMP database.

Checking the Status of an MPE Server

The CMP lets you view the status of MPE servers, either collectively (all servers within the topology) or individually.

- | | |
|--------------|---|
| Group | Select ALL from the policy server content tree to view all the defined MPE servers, or |
| View | select a specific policy server group or sub-group to view just the servers associated with |

that group. The display in the work area includes a status column that indicates the following states:

- **On-line**

The servers in the cluster have completed startup, and their database services are synchronized.

- **Degraded**

At least one server is not functioning properly (its database services are not synchronized or it has not completed startup) or has failed, but the cluster continues to function with the active server. This state sets alarm ID 70005 with severity Major.

Note: If a cluster status is **Degraded**, but the server details do not show any failures or disconnections, then the cluster is performing a database synchronization operation. Until the synchronization process has completed, the server cannot perform as the active server.

- **Out of Service**

Communication to the cluster has been lost.

- **No Data**

Communication to the cluster has been lost. This status value provides backward compatibility with previous Policy Management releases. It can be observed during the upgrade process.

- **Config Mismatch**

The MPE device configuration does not match the CMP database.

Policy Server Profile View

Select a server from the content tree, then click the **System** tab to view the current operating status of the device (**On-line** or **Off-line**) and profile configuration.

Figure 6: Group View shows an example of a Group View in which one of the servers is degraded.

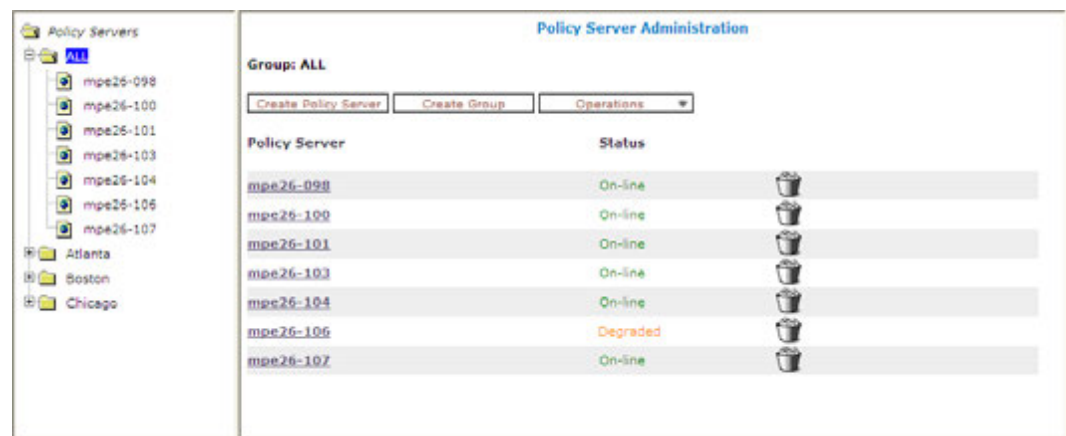



Figure 6: Group View

Trash can icon

Click  (trash can icon) to delete an MPE server.

Policy Server Reports

The **Reports** tab lets you view a hierarchical set of reports that you can use to monitor both the status and the activity of a specific policy server.

Report pages provide the following information:

Mode	Shows whether data collection is currently Active or Paused, Absolute (displaying statistics since the last reset) or Delta (displaying changes in the statistics during the last 10-second refresh period).
Buttons	The buttons let you navigate between reports, or control the information displayed within the report. The following list describes the buttons; which buttons are available depends on your configuration and differ from one report page to the next:
Show Absolute/Show Deltas	Switches between absolute mode (statistics since last reset) and delta mode (statistics since last display).
Reset Counters/Reset All Counters	Resets counters on the current page, or all counters under Policy Statistics and Protocol Statistics, back to initial values (except for Session count and Downstream Bandwidth in the Network Elements) section.
Rediscover Cluster	Rediscoveres the cluster, deleting any failed servers that have been removed from service.
Pause/Resume	Stops or restarts automatic refreshing of displayed information. The refresh period is 10 seconds.
Cancel	Returns to previous page.

The CMP system also displays various statistics and counters related to the following:


Cluster Information Report	Information about the cluster.
Policy Statistics	Information about the execution of policy rules.
Protocol Statistics	Information about the active network protocols.

Note: The Cluster Information Report is also available as a selection on the navigation pane.

Cluster Information Report

The fields that are displayed in the Cluster Information Report section include the **Cluster Status**:

- **On-line:** If one server, it is active; if two servers, one is active and one is standby. No server is in forced-standby mode or out of service.
- **Degraded** (two servers only): One server is active, but the other server is not available due to an ongoing database synchronization, being in forced-standby mode, being out of service, or loss of both bond interfaces.
- **Offline:** No server is active.
- **Inconsistent** (two servers only): Both servers are in the active role. This is a “split brain” error condition, and can only happen when the backplane link fails.

Also within the Cluster Information Report is a listing of all the servers (blades) contained within the cluster. A symbol () indicates which server currently has the external connection (that is, which blade is the active server). The report also lists the following server-specific information:

- **Overall** — Displays the current topology state (Active, Standby, or Out-Of-Service), number of server (blade) failures, and total uptime (time providing active or standby policy or GUI service). For the definitions of these states, see [Server Status](#).
- **Utilization** — Displays the percentage utilization of disk (of the /var/camiant filesystem), average value for the CPU utilization, and memory.
- **Actions** — Buttons in this section let you restart the Policy Management software on the server (**Restart**) or restart the server itself (**Reboot**).

Policy Statistics

The Policy Statistics section summarizes policy rule activity within the MPE device. This is presented as a table of statistics for each policy rule that is configured for the MPE device.

The following statistics are included:

Name	Name of the policy being polled.
Evaluated	Number of times the conditions in the policy were evaluated.
Executed	Number of times policy actions were executed. This implies that the conditions in the policy evaluated to be true.
Ignored	Number of times the policy was ignored. This can happen because the policy conditions refer to data which was not applicable given the context in which it was evaluated.

Protocol Statistics

The Protocol Statistics section summarizes the protocol activity within the MPE device. This information is presented as a table of summary statistics for each protocol. Some protocols are broken down into sub-entries to distinguish between the different types of protocol activity.

The summary protocol statistics are the following:

Connections	If the protocol is connection oriented, this value represents the current number of established connections using each protocol.
Total client messages in / out	The total number of incoming and outgoing messages received and sent using each protocol.
Total messages timeout	The total number of incoming and outgoing messages that timed out using each protocol.

You can click the name of each entry in the Protocol Statistics table to display a detailed report page. For most protocols, this report page displays a set of counters that break down the protocol activity by message type, message response type, errors, and so on.

Many of the protocol report pages also include a table that summarizes the activity for each client or server with which the MPE device is communicating through that protocol. These tables let you select a specific entry to further examine detailed protocol statistics that are specific to that client or server.

Since many of these statistics contain detailed protocol-specific summaries of information, the specific definitions of the information that is displayed are not included here. For more specific information, see the appropriate technical specification that describes the protocol in which you are interested (see [Other Publications](#)).

Note:

1. Statistical information is returned from the MPE device as a series of running peg counts. To arrive at interval rate information, such as session success and failure counts, two intervals are needed to perform the difference calculation. Also, statistical information, such as session activation counts, is kept in memory and is therefore not persisted across the cluster. After a failover, non-persistent metrics must be repopulated based on a sampling from the newly active primary server. Therefore, when an MPE device is brought on line, or after a failover, one or more sample periods will display no statistical information.
2. Historical network element statistical data is inaccurate if configuration values (such as capacity) were changed in the interim. If the network element was renamed in the interim, no historical data is returned.

VoD Server Statistics

The VoD Statistics section summarizes VoD server activity within the MPE device. This information is presented as a table of summary statistics plus statistics for any selected network elements.

The summary represents the aggregated statistics for every VoD server associated with this MPE device, and includes the following:

- **Total messages in / out** — The total number of incoming and outgoing messages sent and received by this MPE device.
- **Total VOD sessions** — The total number of VoD session requests received by this MPE device, whether successful or not, since the last time the counters were reset. A session teardown does not decrement this value.
- **Success VOD sessions** — The total number of successful reserve requests (defined as a single reserve request followed by an ACK from this MPE device) since the last time the counters were reset.
- **Failure VOD sessions** — The total number of failed session requests (defined as a single reserve request from a VoD server followed by a NAK from this MPE device) since the last time the counters were reset.
- **Active VOD sessions** — The number of currently active session requests.

The Reports tab also includes a table that summarizes activity through network elements with which this MPE device is communicating. This table lets you select specific network elements to further examine detailed statistics that are specific to that network element.

You can search for specific network elements of one or more types. Select **B-RAS**, **Subscriber Group**, **Router**, **Server**, or **Wireline Gateway**, enter the name of the network element (up to 250 characters; use "*" or "?" as wildcard characters, or leave the field blank to search for all elements of that type), and click **Search**. Information for the selected network element(s) is displayed.

Tip: To display information for all network elements, select the element class and click **Search**.

The resulting table displays the following information:

- **Network Element** — Unique identifier for this device.
- **Session count** — Number of active sessions handled by this device.

- **Session success count** — Number of successful reserve requests (defined as a single reserve request followed by an ACK from the MPE device) by this device since the MPE device was last started or the counters reset.
- **Session count HS/SD** — Number of sessions in high definition (HD) and standard definition (SD).
- **Upstream bandwidth** — Current reserved upstream bandwidth allocated for this network element.
- **Downstream bandwidth** — Current reserved downstream bandwidth allocated for this network element.

For statistics on an individual VoD server, click on its network element name.

Note:

1. Statistical information is returned from the MPE device as a series of running peg counts. To arrive at interval rate information, such as session success and failure counts, two intervals are needed to perform the difference calculation. Also, statistical information, such as session activation counts, is kept in memory and is therefore not persisted across the cluster. After a failover, non-persistent metrics must be repopulated based on a sampling from the newly active primary server. Therefore, when an MPE device is brought on line, or after a failover, one or more sample periods will display no statistical information.
2. Historical network element statistical data is inaccurate if configuration values (such as capacity) were changed in the interim. If the network element was renamed in the interim, no historical data is returned.

Viewing Policy Server Logs

The log files trace the activity of a Policy Management device. The system handles log file writing, compression, forwarding, and rotation automatically. You can view and configure the logs for an individual cluster.

To view the log:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups.
2. From the content tree, select the Policy Management device.
The **Policy Server Administration** page opens in the work area.
3. Select the **Logs** tab.

Depending on your mode and release, you can configure the following logs:

- **Trace log** — Records application-level notifications.
- **Policy Syslog Forwarding** — Records policy-processing activity. Supports the standard UNIX logging system, in conformance with RFC 3164.
- **Session Synchronization log** — Contains information on Video on Demand (VoD) session synchronization.

Viewing the Trace Log

The trace log records Policy Management application notifications, such as protocol messages and custom messages generated by policy actions, for individual servers. Trace logs are not replicated

between servers in a cluster, but they persist after failovers. You can use the trace log to debug problems by tracing through application-level messages.

You can configure the severity level of messages that are recorded in the trace log.

To view log information using the Trace Log Viewer:



1. Select the device to view:
 - To view an MPE device, from the **Policy Server** section of the navigation pane, select **Configuration**.

The content tree displays a list of groups; the initial group is **ALL**.

2. From the content tree, select the device.
The appropriate **Administration** page opens in the work area.
3. On the **Administration** page, select the **Logs** tab.
Log information for the selected device is displayed.
4. Click **View Trace Log**.

While data is being retrieved, the in-progress message *Scanning Trace Logs* appears.

When the **Trace Log Viewer** window opens in a new browser window, all events contain the following information:

- **Date/Time** — Event timestamp. This time is relative to the server time.
 - **Code** — The event code or ID number. For information about event codes and messages, see the *Troubleshooting Reference*.
 - **Severity** — Severity level of the event. Application-level trace log entries are not logged at a higher level than **Error**.
 - **Message** — The message associated with the event. If additional information is available, the event entry shows as a link. Click the link to see additional detail in the frame below.
5. Filter the events displayed using the following:
 - **Trace Log Viewer for Server** — Select the individual server within the cluster.
 - **Start Date/Time** — Click  (calendar icon), select the starting date and time, then click **Enter**.
 - **End Date/Time** — Click  (calendar icon), select the ending date and time, then click **Enter**.
 - **Trace Codes** — Enter one or a comma-separated list of trace code IDs. Trace code IDs are integer strings up to 10 digits long.
 - **Use timezone of remote server for Start Date/Time** — Select to use the time of a remote server (if it is in a different time zone) instead of the time of the CMP server.
 - **Severity** — Filter by severity level. Events with the selected severity and higher are displayed. For example, if the severity selected is **Warning**, the trace log displays events with the severity level **Warning** and higher.
 - **Contains** — Enter a text string to search for. For example, if you enter **connection**, all events containing the word **connection** appear.

Note: The **Start Date/Time** setting overrides the **Contains** setting. For example, if you search for events happening this month, and search for a string that appeared in events last month and this month, only results from this month appear.
 6. After entering the filtering information, click **Search**.
The selected events are displayed. By default, the window displays 25 events per page.
 7. To change the number of events per page, select a value from the **Display results per page** list.

You can change this to 50, 75, or 100 events per page.

Note: Events that occur after the Trace Log Viewer starts are not visible until you refresh the display.

8. To refresh the display, click any of the following:
 - **Show Most Recent** — Applies filter settings and refreshes the display. This displays the most recent log entries that fit the filtering criteria.
 - **Next/Prev** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.
 - **First/Last** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.
9. When you are finished viewing the trace log, click **Close**.
The trace log window closes.

Syslog Support

Notifications generated by policy actions are sent to the standard UNIX syslog. No other notifications are forwarded to the syslog. .

Note: This feature is separate from the TPD syslog support.

The Session Synchronization Log

The session synchronization log records VoD synchronization operations performed by the MPE device. Log files are stored in compressed format.

When the logging function is enabled, the following information is logged during every VoD synchronization operation by the MPE device:

- VoD session count list
- VoD session server ID list
- MPE device session count
- MPE device session ID list
- Sessions missing on MPE device
- Sessions missing on VoD server (with associated subscriber information as available)
- Any delete or recreate actions taken for session mismatches
- Session count and IDs included in synch response sent by MPE device
- Session count and IDs included in synch response received by MPE device

The format of a log file record is as follows:

```
timestamp | servertype | IP_addr | operation | (Count: nnnnn) session_list |
```

where:

timestamp

A date/time stamp

servoertype

Tandberg

IP_addr

The IP address of the server

operation

One of the following:

- LS — local sessions
- RS — remote sessions (VoD server sessions)
- LD — local deleted sessions
- RD — remote deleted sessions
- LR — local recreated sessions
- SR — status response to VoD server

Configuring Log Settings

To configure the log settings for the servers in a cluster:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Server Administration** page opens in the work area.
3. Select an MPE device from the list.
The **Policy Server Administration** page opens in the work area and details the configuration settings of the selected device.
4. Select the **Logs** tab.
The **Policy Server Administration** page opens and details the logs configuration settings for the specified device.
5. To edit the logs configuration settings, click **Modify**.
The editable fields open in the work area.
6. In the **Modify Trace Log Settings** section of the page, select the **Trace Log Level** from the list.
This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164 *The BSD syslog Protocol*. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:
 - **Emergency** — Provides the least amount of logging, recording only notification of events causing the system to be unusable.
 - **Alert** — Action must be taken immediately in order to prevent an unusable system.
 - **Critical** — Events causing service impact to operations.
 - **Error** — Designates error events which may or may not be fatal to the application.
 - **Warning** — Designates potentially harmful situations.
 - **Notice** — Provides messages that may be of significant interest that occur during normal operation.
 - **Info** — Designates informational messages highlighting overall progress of the application.
 - **Debug** — Designates information events of lower importance.



Caution: Before changing the default logging level, consider the implications. Lowering the **Trace Log Level** setting from its default value (for example, from **Warning** to **Info**) causes more notifications to be recorded in the trace log and can adversely affect performance. Similarly, raising the log level setting (for example, from **Warning** to **Alert**) causes fewer notifications to be recorded in the trace log, and may cause you to miss important notifications.

7. Configure the **Maximum Trace Log File Size** (in KB).

The system will maintain up to this number of trace log files, removing old files when it reaches this limit. The choices are 512, 1,024, 2,048, 4,096, 8,192, 16,384, or 32,678 KB. The default is 2,048 KB.

8. Configure the **Maximum Trace Log File Count**. The system manages rotation of log files automatically.

The range is 2–8 files. The default is 8 files.

9. To configure the trace log forwarding settings, for each system, enter the following:

a) **Hostname/IP Addresses** — Remote system host name or IPv4 address.



Caution: Forwarding addresses are not checked for loops. If you forward events on System A to System B, and then forward events on System B back to System A, a message flood can result, causing dropped packets.

b) **Severity** — Filters the severity of notifications that are written to the log:

- **Emergency** — Provides the least amount of logging, recording only notification of events causing the system to be unusable.
- **Alert** — Action must be taken immediately in order to prevent an unusable system.
- **Critical** — Events causing service impact to operations.
- **Error** — Designates error events which may or may not be fatal to the application.
- **Warning** — Designates potentially harmful situations.
- **Notice** — Provides messages that may be of significant interest that occur during normal operation.
- **Info** (default) — Designates informational messages highlighting overall progress of the application.
- **Debug** — Designates information events of lower importance.

10. In the **Modify Log Forwarding Configuration** section of the page, select **Enable Policy Log Forwarding** to forward the policy log to remote locations.

11. To configure session synchronization log settings:

a) In the **Modify Session Synchronization Log Settings** section of the page, select **Enable Session Synchronization Log** to enable the session synchronization log. The **Number of Session Synchronization Log Files** field appears.

b) Enter the **Number of Session Synchronization Log Files**.

The system manages rotation of log files automatically. The range is 2–10 files. The default is 10 files.

12. Click **Save**.

The log settings are configured.

VoD Session Flow Scenarios

The following is a general list of session flow scenarios and the action(s) of the MPE device for each.

Scenario 1

The MPE device has knowledge of a user's account, but the user's IP address was not received by the MPE device from the B-RAS server.

MPE Action: An internal switch, set by Oracle Technical Support personnel only, is available to allow the MPE device to accept this request. Otherwise, if the Session Manager sends a request for a video session to the MPE device, the request is **rejected** as the MPE device has no knowledge of the IP address of the user.

Scenario 2

The MPE device has no knowledge of a user's account, but does know the IP address of the user from messaging with the B-RAS server.

MPE Action: The request is **processed normally**.

Scenario 3

A VoD request destination IP address does not match configured subnets on the B-RAS, and an entry does not exist in the COPS-PR database.

MPE Action: The request is **rejected**. A 6203 message is written into the trace log.

Scenario 4

A VoD request destination IP address does not match configured subnets on the B-RAS, but an entry exists in the COPS-PR database.

MPE Action: The request is **rejected**. A 6203 message is written into the trace log.

Scenario 5

A VoD request destination IP address matches configured subnets on the B-RAS server, but the entry does not exist in the COPS-PR database.

MPE Action: An internal switch, set by Oracle Technical Support only, is available to allow the MPE device to accept this request. Otherwise, the request is **rejected**. A 6203 message is written into the trace log.

Scenario 6

A VoD request destination IP address matches configured subnets on the B-RAS server, but the entry exists in the COPS-PR database under a different gateway router (GWR).

MPE Action: The request is **rejected**. A 6203 message is written into the trace log.

If a request is not rejected by any of the scenarios above, it is presented to the customer-defined policy rules.

Note: During installation and transition of MPE devices, rejections due to scenarios 1 and 2 must be disabled. This is to allow for the staged startup of B-RAS devices. During the transition only a subset of B-RAS servers will be sending the MPE device COPS-PR information, but session requests will be received from all B-RAS devices within a given video hub office (VHO). Rejection mode is disabled and enabled using an internal switch set by Oracle Technical Support personnel only.

Synchronizing a TANDBERG VoD Server

The MPE device communicates with multiple VoD servers, but will not synchronize with a TANDBERG server until it first receives an allocate resource or status request from it. The MPE device uses SSL when synchronizing with a TANDBERG server if the last allocate request was received over an HTTPS connection. The synchronization interval is expressed in minutes.

To force a synchronization with all connected TANDBERG VoD servers, select the Policy Server tab and click **Sync Tandberg VoD Server Now**. The page displays the message “The VoD Server synchronization initiated by user.”

TANDBERG synchronization proceeds as follows:

1. The MPE device builds a local list of sessions that it knows about.
2. The MPE device sends a SESSIONLIST status request to the TANDBERG server to obtain its list of sessions.
3. The MPE device compares the two lists and creates three new lists:
 - a) VoD server only
 - b) MPE device only
 - c) Common to both
4. Ideally, all sessions are in the “common to both” list and the other two lists are empty, in which case no further action is required.
5. For each session in the VoD server only list:
 - a) The MPE device checks to see whether the session was created while waiting for the session list response from the VoD server.

If the session now exists locally, no further action is required for this session.
 - b) If the session still does not exist locally, the MPE device sends a SESSIONID status request to the VoD server to request session details for the missing session.
 - c) If the VoD server responds with “session not found,” then no further action is required for this session.
 - d) If the VoD server responds with details for the missing session, then the MPE device attempts to recreate the session by allocating resources for it.
 - e) If recreating the session succeeds, no further action is required.
 - f) If recreating the session fails, then the MPE device sends a “release resources” request to the TANDBERG server to tear the session down.

6. For each session in the MPE only list:
 - a) The MPE device sends a SESSIONID status request to the VoD server to request session details for the missing session.
 - b) If the VoD server responds with details for the session, then no further action is required.
 - c) If the VoD server responds with "session not found," then the session is removed locally from the MPE device.

Synchronization Operations and Failover

After a blade failover, the MPE device loads the list of VoD servers that the previously active blade knew about and starts a synchronizer for each of them. The new active blade bases its next synchronization time on the last successful synchronization that the previously active blade completed. The synchronization failure counts are intentionally not transferred between blades; thus the newly active blade tries for another 150 minutes to communicate with a dead VoD server before removing it from the synchronization list.

Synchronizing a B-RAS Server

An ERX device needs to be synchronized with MPE devices. MPE devices support both full synchronization and the fast synch feature over the COPS-PR interface.

Fast Synch: When an ERX device connects to the MPE device, it includes information on the last policy server to which it connected as part of an OPN message. When fast synch is enabled, and the IP address sent matches the MPE device address, the MPE device sends an unsolicited Decision (DEC) message to the ERX device, which replies with just Request (REQ) and Delete (DRQ) messages instead of full state information. This makes it easier to recover from a temporary connection loss or a warm restart. (For information on configuring fast synch, see [Configuring Protocol Options on the Policy Server](#).)

Full Synch: If an MPE device detects that the last policy server IP address reported by the ERX device is different from its own, it sends a Synchronization (SSQ) message, which triggers a full state synchronization. If the ERX device determines that a full state synchronization is required (for example, after a cold restart or if the threshold hold time for fast synch recovery has expired), it reports the last policy server IP address as 0.0.0.0. In this case, the MPE device sends an SSQ message.

Force Synch: To force a full synchronization with a B-RAS server:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the desired B-RAS server.
The Network Element Administration page opens in the work area.
3. On the B-RAS tab, click **Force Full Synch Now**.

B-RAS synchronization proceeds as follows:

1. The MPE device closes the connection to the ERX device and waits for it to reconnect.
2. The MPE device determines whether a forced synchronization was requested, as since it was, sends an SSQ message to the server and ignores the policy server IP address reported back.
3. Once the full synchronization is complete, the forced synchronization override is reset, and fast synchronizations can resume (if the feature is enabled).

Chapter 5

Managing Network Elements

Topics:

- *About Network Elements.....62*
- *Defining a Network Element.....62*
- *Configuring Options for Network Elements.....65*
- *Associating a Network Element with an MPE Device.....66*
- *Working with Network Element Groups.....67*
- *Importing VoD Configuration Information.....71*

This chapter describes how to define network elements within the CMP system.

Network elements are the devices, servers, or functions within your network with which Policy Management systems interact.

About Network Elements

A network element is a high-level device, server, or other entity within your network for which you would use an MPE device to manage Quality of Service (QoS). Examples include the following:

- Broadband remote access server (B-RAS)
- Router
- Server

After you have defined a network element in the CMP database, you associate it with the MPE device that you will use to manage that element.

There are also lower-level entities within the network that the MPE device manages that are not considered network elements. These are sub-elements, such as an interface on a router, or devices that are connected directly to network elements. Typically, there is no need to define these lower-level entities, because after a network element is associated with an MPE device, the lower-level devices related to that network element are discovered and associated automatically.

Create a network element profile for each device you are associating with an MPE device. After defining a network element in the CMP database, configure its protocol options. The options available depend on the network element type.

For ease of management, you can define network elements and then you can combine them into network element groups.

Defining a Network Element

You must define a network element for each device associated with any of the MPE devices within the network. To define a network element:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** network element group.
(See [Creating a Network Element Group](#) for information on creating network element groups.)
The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, click **Create Network Element**.
The New Network Element page opens.
4. Enter information as appropriate for the network element:
 - a) **Name** (required) — The name you assign to the network element.
Enter up to 255 alphanumeric characters. The name can include underscores (_), hyphens (-), colons (:), and periods (.).
 - b) **Host Name/IP Address** (required) — Registered domain name, or IP address in IPv4 format, assigned to the network element.
 - c) **Backup Host Name** — Alternate address that is used if communication between the MPE device and the network element's primary address fails.
 - d) **Element ID** — Alternate unique ID for a network element.

- Enter up to 250 characters.
- e) **Description/Location** — Free-form text.
Enter up to 250 characters.
- f) **Type** (required) — Select the type of network element.
The supported types are:
- **B-RAS** (the default) — Broadband Remote Access Server (with the subtypes **ERX** or **E320**)
 - **Subscriber Group** — a subscriber group (for more information, see [Creating an Account](#))
 - **Router**
 - **Server**
 - **Wireline Gateway** — a gateway router (with the subtype **MX Series**)
- g) **Capacity** — The bandwidth allocated to this network element.
5. Select one or more policy servers (MPE devices) to associate with this network element.
 6. To add a network element to a network element group, select the desired group (see [Adding a Network Element to a Network Element Group](#)).
 7. When you finish, click **Save** (or **Cancel** to discard your changes).
The network element is displayed in the Network Element Administration page.
- You have created the definition for a network element.

Modifying a Network Element

To modify a network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**. If there are more than 50 network elements, only the number of network elements is displayed, not the elements themselves.
2. Select the network element.
If there are more than 50 network elements, the display is paginated. Select the page number or search for the network element by name (see [Finding a Network Element](#)).
3. On the System tab, click **Modify**.
The **Modify Network Element** page opens.
4. Modify network element information as required.
For a description of the fields contained on this page, see [Defining a Network Element](#).
5. Click **Save**.

The network element definition is modified.

Deleting Network Elements

Deleting a network element definition removes it from the list of items that a Policy Management device can support. To delete a network element definition, delete it from the ALL group. Deleting a network element from the ALL group also deletes it from every group with which it is associated.

To delete a network element:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.

The content tree displays a list of network element groups; the initial group is **ALL**. If there are more than 50 network elements, only the number of network elements is displayed, not the elements themselves.

2. Select the network element.

If there are more than 50 network elements, the display is paginated; select the page number or search for the network element by name (see [Finding a Network Element](#)).

3. From the work area, click the **Delete** icon, located to the right of the network element you want to delete.

A confirmation message appears.

4. Click **OK** to delete the network element.

The network element is removed from the list.

You have deleted the definition of the network element.

Bulk Delete

A large network can contain a great many network elements. To perform a bulk delete of network element definitions:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.

The content tree displays a list of network element groups; the initial group is **ALL**.

2. From the content tree, select **ALL**.

The **Network Element Administration** page opens in the work area.

3. On the **Network Element Administration** page, click **Bulk Delete**.

The **Bulk Delete Network Elements** page opens.

4. Select the network elements or network element groups to delete.

By default, the **Search Pattern** entry box contains an asterisk (*) to match all network elements. To search for a subset of network elements, enter a search pattern (for example, **star***, ***pGw**, or ***-***), click **Filter**, and select from the filtered results.

5. Click **Bulk Delete**.

A confirmation message displays.

6. Click **OK** to delete the network elements.

The selected network elements or groups are deleted from the CMP database and all associated MPE devices.

Finding a Network Element

The Search function lets you find a specific network element within a large configuration. To search the CMP database for a specific network element:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.

The content tree displays a list of network element groups; the initial group is **ALL**. If there are more than 50 network elements in a group, only the number of network elements is displayed, not the elements themselves.

2. From the content tree, select **ALL**.

The **Network Element Administration** page opens in the work area. If there are more than 50 network elements, the display is paginated.

3. On the **Network Element Administration** page, click **Search**.
The **Network Element Search Criteria** window opens.
4. Enter the search criteria. Searches are not case sensitive. You can use the asterisk (*) and question mark (?) wildcard characters.
 - **Name** — The name assigned to the network element.
 - **Host Name/IP Address** — The domain name or IP address, in IPv4 format, of the network element.
 - **ID** — The network element ID (an alternate unique ID for a network element). Enter up to 250 characters.
 - **Description** — The information pertaining to the network element that helps identify it within the network. Enter up to 250 characters.
5. After entering search criteria, click **Search**.

The **Search Results** page opens in the work area, displaying the results of the search. The last search results are held in a `Search Results` folder in the content tree until you close the **Search Results** page.

Configuring Options for Network Elements

The following sections describe how to configure options for a given network element type. The available network element types depend on the operating mode in which your CMP system is configured, and may differ from the list given here.

B-RAS, Router, and Server

To configure interface information for a B-RAS, Router, or Server network element:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**. If there are more than 50 network elements, only the number of network elements is displayed, not the elements themselves.
2. Select a network element from the content tree.
The **Network Element Administration** page opens in the work area.
3. Select the **Interfaces** tab and click **Create Interface**.
The **Create Network Element Interface** page opens.
4. Configure the following information:
 - a) **Name** — The name assigned to the network element.
The name can be up to 32 characters in length. The name cannot contain the :: (doubled colons) character string. Synchronization requests are processed based on the network element name.
 - b) **Capacity** — The bandwidth capacity of this interface.
 - c) **Description / Location** — The information pertaining to the network element that helps identify it within the network.
 - d) **Links** — Specifies the links to other network elements.
5. Click **Save**.

The interface information is configured.

Creating Subnets

A B-RAS server can contain subnets, which can be provisioned from an operations support system (OSS) or configured manually.

To create subnets associated with a device:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**. If there are more than 50 network elements only the number of network elements is displayed, not the elements themselves.
2. On the Network Element Administration page, select the desired network element. If there are more than 50 network elements, the display is paginated; select the page number or search for the network element by name (see [Finding a Network Element](#)).
3. Select the B-RAS tab.
Subnets are displayed in two categories:
 - a) **Subnets Configured Manually** — You can add to or delete from this list.
 - b) **Subnets Obtained from the OSS** — This read-only field displays subnets that were imported via the OSS interface to the CMP database(not supported).
4. Click **Modify**.
The **Modify Network Element** page opens.
5. Modify the subnet list as required:
 - To add a subnet, type the address block in CIDR (Classless Inter-Domain Routing) format and click **Add**. The subnet is added to the list.
 - To delete a subnet, select it from the list and click **Delete**. The subnet is removed from the list.
6. Click **Save**.

The subnets are configured.

To synchronize subnet changes throughout the Policy Management network, click **Force Full Sync Now**.

Associating a Network Element with an MPE Device

To associate a network element with an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the MPE device.
The **Policy Server Administration** page opens in the work area.
3. Select the **Policy Server** tab.
The **Associations** section lists the network elements associated with the MPE device.
4. Click **Modify**.
The **Modify Policy Server** page opens.

- To the right of the list of network elements in the **Associations** section, click **Manage**. The **Select Network Elements** window opens.

For example:

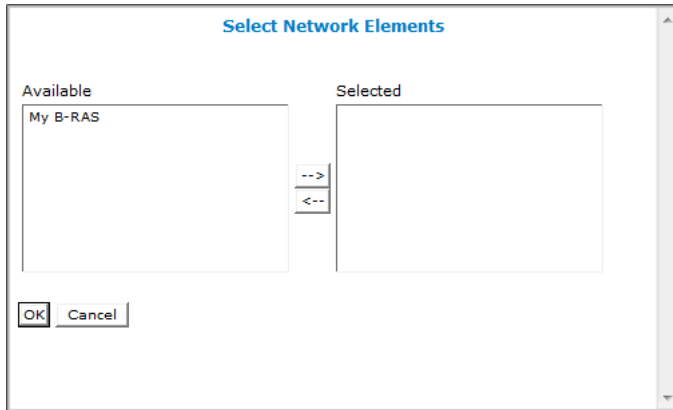


Figure 7: Select Network Elements

- Select the network elements in the **Available** list and click -->. To disassociate a network element from the MPE device, select the network element from the **Selected** list and click <--. To select entries, press the Ctrl or Shift key and select the entries.
- When you finish, click **OK**. The selected network elements are added to the list of network elements managed by this MPE device.
- To associate a network element group with the MPE device, select the group from the list of network element groups located under **Associations**.
- Click **Save**.

The network element is associated with this MPE device.

Working with Network Element Groups

For organizational purposes, you can aggregate the network elements in your network into groups. For example, you can use groups to define authorization scopes or geographic areas. You can then perform operations on all the network elements in a group with a single action.

Creating a Network Element Group

To create a network element group:

- From the **Policy Server** section of the navigation pane, select **Network Elements**. The content tree displays a list of network element groups; the initial group is **ALL**.
- From the content tree, select the **ALL** group. The **Network Element Administration** page opens in the work area.
- On the **Network Element Administration** page, click **Create Group**. The **Create Group** page opens.

4. Enter the name of the new network element group.
The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. Enter a text description of the network group.
6. Click **Save**.

The new group appears in the content tree. You have created a network element group.

Adding a Network Element to a Network Element Group

Once a network element group is created, you can add individual network elements to it. To add a network element to a network element group:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group.
The **Network Element Administration** page opens in the work area, displaying the contents of the selected network element group.

3. Click **Add Network Element**.

The **Add Network Elements** page opens. The page supports both small and large networks, as follows:

- If there are 25 or fewer network elements defined, the page displays the network elements not already part of the group. (*Figure 8: Add Network Element Page* shows an example.)
- If there are more than 25 network elements defined, the page does not display any of them. Instead, use the **Search Pattern** field to filter the list. Enter an asterisk (*) to generate a global search, or a search pattern to locate only those network elements whose name matches the pattern. When you have defined a search string, click **Filter**; the page displays the filtered list.

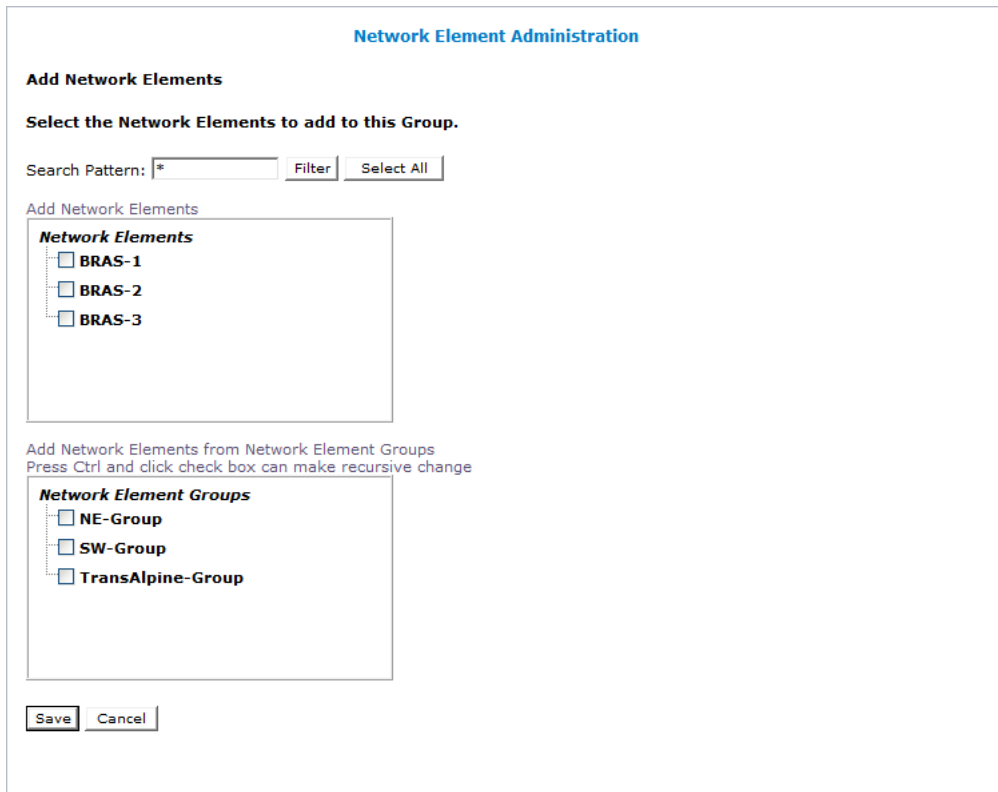


Figure 8: Add Network Element Page

4. Select the network element you want to add. Press the Ctrl or Shift key to select multiple network elements.

You can also add previously defined groups of network elements by selecting those groups.

5. Click **Save**.

The network element is added to the selected group and a message indicates the change. For example, 2 Network Elements were added to this group.

Creating a Network Element Sub-group

You can create sub-groups to further organize your network element network. To add a network element sub-group to an existing network element group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group.
The **Network Element Administration** page opens in the work area, displaying the contents of the selected network element group.
3. Click **Create Sub-Group**.
The **Create Group** page opens.
4. Enter the **Name** of the new sub-group.
The name cannot contain quotation marks (") or commas (,).

5. Enter a text **Description/Location** of the sub-group.
6. Click **Save**.

The sub-group is added to the selected group and appears in the listing.

Deleting a Network Element from a Network Element Group

Removing a network element from a network element group or sub-group does not delete the network element from the **ALL** group, so it can be used again if needed. Removing a network element from the **ALL** group removes it from all other groups and sub-groups.

To remove a network element from a network element group or sub-group:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group or sub-group.
The **Network Element Administration** page opens in the work area, displaying the contents of the selected network element group or sub-group.
3. Delete a network element using one of the following methods:
 - On the **Network Element Administration** page, click **Remove** (🗑️), located to the right to the network element you want to remove.
 - From the content tree, select the network element. The **Network Element Administration** page opens. Click the **System** tab and then click **Delete**.

A confirmation message displays.

4. Click **OK**.

The network element is removed from the group or sub-group.

Modifying a Network Element Group

To modify a network element group or sub-group:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group or sub-group.
The **Network Element Administration** page opens in the work area.
3. Click **Modify**.
The **Modify Group** page opens.
4. Modify the **Name** or **Description/Location**.
5. Click **Save**.

The group is modified.

Deleting a Network Element Group or Sub-group

Deleting a network element group also deletes any associated sub-groups. However, any network elements associated with the deleted groups or sub-groups remain in the **ALL** group, from which they can be used again if needed.

Note: You cannot delete the **ALL** group.

To delete a network element group or sub-group:

1. From the **Policy Server** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups.
2. From the content tree, select the network element group or sub-group.
The **Network Element Administration** page opens in the work area, displaying the contents of the selected network element group or sub-group.
3. Click **Delete**.
A confirmation message displays.
4. Click **OK** to delete the group.

The network element group or sub-group is deleted.

Importing VoD Configuration Information

The following procedure describes how to import VoD configuration information. It assumes that you have all components installed and operational, and that all subscriber information is available.

For additional information, see the *OSSI XML Interface Definitions Reference Guide*. This document describes the CMP OSSI XML interface, which lets you programmatically provision the system and retrieve operational statistics from the policy managers.

Provisioning Topology and Subscriber Data

The following subsections describe how to provision the topology and subscriber data. See [Managing Subscribers](#) for additional information about subscribers.

Manually within the CMP

To provision the topology and subscriber data manually:

1. Define the VoD server, including manually configured subnets and all legitimate VoD *pump* addresses.
2. Define a set of policy rules and deploy them to the policy server.
3. Define a network element group, add the VoD server into the group, and associate the group with the policy server (all of which is sent automatically to the policy server).

Using the OSSI XML Interface

To provision the topology and subscriber data using the OSSI XML interface:

1. Add network elements, network element interfaces, and network element links to represent the routers, B-RASs, and links in the network; then associate them with the same network element groups defined earlier so they are sent to the policy server automatically.
Over time, these network resources are updated via the OSSI XML interface to add new subnets and/or delete existing subnets.

2. Add paths that refer to the server, routers, B-RASs, links, and network element Interfaces defined earlier so they are sent to the MPE device automatically.
3. Add tiers.

Each tier should include a <TierRef> tag that refers to an associated tier so it is sent to the MPE device automatically.
4. Add accounts.

Each account should include a <NetworkElementName> tag that refers to its associated network element, as well as a <SubscriberData> tag that defines interface information, so they are sent to the MPE device automatically.

Path Definitions

Path definitions define the sequence the data transmission elements used by video sessions originating on VoD servers and terminating on gateway routers.

At a minimum, these path definitions consist of a series of interface definitions connecting the VoD server with a specific gateway router.

The following example shows a sample base path definition:

```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
<AddPath>
  <Path>
    <Name>VOD1-GWR</Name>
    <Description/>
    <Hops>
      <Hop>
        <NeName>VoD1</NeName>
      </Hop>
      <Hop>
        <NeName>VDR1</NeName>
        <IfName>if1</IfName>
      </Hop>
      <Hop>
        <NeName>VAR1</NeName>
        <IfName>if2</IfName>
      </Hop>
      <Hop>
        <NeName>GWR</NeName>
      </Hop>
    </Hops>
  </Path>
</AddPath>
</XmlInterfaceRequest>
```

If resource tracking and policy rule execution is desired against the router device (rather the interface on a router), you can use the router definition itself in the path definition. In the following example, the entries are added to track resources at the VDR1 and VAR1 routers:

```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
<AddPath>
  <Path>
```



```

<Name>VOD1-GWR</Name>
<Description/>
<Hops>
  <Hop>
    <NeName>VoD1</NeName>
  </Hop>
  <Hop>
    <NeName>VDR1</NeName>
  </Hop>
  <Hop>
    <NeName>VDR1</NeName>
    <IfName>if1</IfName>
  </Hop>
  <Hop>
    <NeName>VAR1</NeName>
  </Hop>
  <Hop>
    <NeName>VAR1</NeName>
    <IfName>if2</IfName>
  </Hop>
  <Hop>
    <NeName>GWR</NeName>
  </Hop>
</Hops>
</Path>
</AddPath>
</XmlInterfaceRequest>

```

Operational statistics are available for the routers defined in the path.

Importing a Large Number of Subscribers

The following procedure is recommended when using the OSSI XML interface to import a large number of subscribers:

1. Break up the entire collection of subscribers into subsets of 10,000.
2. Within the XML, include all 10,000 accounts in a single <AddAccount> tag (as opposed to using 10,000 separate <AddAccount> tags).
3. Use a separate HTTP POST command to push each subset to the CMP database.

Note: Do not specify a *DistributeImmediately* attribute of **no** in these commands. Either specify **yes** or do not include the attribute at all (the default value is **yes**). The subscriber data is distributed immediately from the CMP database to the MPE devices. In addition, the CMP system is configured to allow only post file sizes of up to 20MB.

Chapter 6

Managing Application Profiles

Topics:

- *About Application Profiles.....75*
- *Creating an Application Profile for a TANDBERG Server.....75*
- *Modifying an Application Profile.....76*
- *Deleting an Application Profile.....76*

This chapter describes how to create and manage application profiles within the CMP system.

An application is a service provided to network subscribers for which you want to manage Quality of Service (QoS).

About Application Profiles

An application is a service provided to users of your network for which you want to manage quality of service (QoS). Examples include voice over IP (VoIP) telephony, video on demand (VoD), and gaming. After you have defined an application profile in the CMP database, you can associate it with the MPE devices that will manage that application.

When you offer application services in your network, there are typically many servers in your network that provide that service. These servers are referred to as Application Managers or Application Servers. When these servers are establishing a session that requires quality of service they issue a request to a policy charging and rules function (PCRF). The MPE device provides PCRF for the CMP server.

When defining an application profile in the CMP database, you specify protocol information that is used by MPE devices to identify Application Managers and thus associate each request with its associated application. This lets the MPE device apply policy rules to the request that you have defined for the associated application.

Creating an Application Profile for a TANDBERG Server

An application profile is associated with a request received from a TANDBERG server based on the application name in the request. (If the application name is absent, the server IP address in the request is used.) This application profile can be used in policy conditions.

To create an application profile:

1. From the **Policy Server** section of the navigation pane, select **Applications**.
The content tree displays the **Applications** group.
2. Select the **Applications** group.
The **Application Administration** page opens in the work area.
3. Click **Create Application**.
The **New Application** page opens.
4. Enter the following application profile information:
 - a) **General Configuration:**
 - **Name** — Name assigned to the application (for example, **OpenStream**). Most TANDBERG allocation requests have ApplicationName = "OpenStream" and include MediaType = "VIDEO," and the MPE device concatenates the fields with a period (.), so the application name is usually "OpenStream.VIDEO." You must define an application with this name, or else all allocation requests from TANDBERG servers will generate "416 Invalid Application Name" errors.
 - **Description/Location** (optional) — Any information that helps identify the application.
 - **Connection IP Address(es)** (optional) — Enter the Connection Manager IP address(es) that are used by Application Managers for this application. To include an address in the connection list, type it and click **Add**; to remove an address from the list, select it and click **Delete**. It is not necessary to include an IP address if the allocation request includes the application name.
 - **SD/HD Threshold** — Enter the bitrate threshold between standard definition (SD) and high definition (HD). Bitrate requests below the threshold are assigned the service type "SD,"

and bitrate requests above the threshold are assigned the service type “HD.” Type a numeric value in the range 0–2147483647 ($2^{31}-1$).

The traffic classes “SD” and HD” are available as conditions in the policy wizard (see [Conditions for Writing Policy Rules](#)).

- b) **Policy Servers associated with this Application:** Select a policy server (MPE device) to associate it with this network element.

5. Click **Save**.

The TANDBERG application profile is created and stored in the **Applications** group. The application profile is created.

Modifying an Application Profile


To modify an application profile:

1. From the **Policy Server** section of the navigation pane, select **Applications**.
The content tree displays the **Applications** group.
2. Select the **Applications** group.
The Application Administration page opens in the work area, listing the application profiles.
3. On the Application Administration page, select the application profile you want to modify.
The profile is displayed.
4. Click **Modify**.
The Modify Application page opens.
5. Modify the application profile information as necessary.
See [Creating an Application Profile for a TANDBERG Server](#) for a description of the fields on this page.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The application profile is modified.

Deleting an Application Profile

To delete an application profile:

1. From the **Policy Server** section of the navigation pane, select **Applications**.
The content tree displays the **Applications** group.
2. Select the **Applications** group.
The **Application Administration** page opens in the work area.
3. Delete the application profile using one of the following methods:
 - From the work area, click the  (trash can icon), located to the right of the profile.
 - From the content tree, select the application and click **Delete**. A confirmation message displays.
4. Click **OK**.

The application profile is deleted from the CMP database and all MPE devices.

Understanding and Creating Policy Rules

Topics:

- *About Policy Rules.....78*
- *Structure and Evaluation of Policy Rules.....78*
- *Creating a Policy.....81*
- *Modes and the Policy Wizard.....84*
- *Parameters Within Policy Rules.....85*
- *Conditions for Writing Policy Rules.....85*
- *Actions for Writing Policy Rules.....119*
- *Policy Rule Variables.....123*
- *Policy Rule Examples.....127*

This chapter describes policy rules and how to create them, and provides reference information on the policy rule conditions and actions available for carrier networks.

About Policy Rules

Policy rules dynamically control how an MPE device processes protocol messages as they pass through it. Using these rules, you can define how and when network resources are utilized by subscribers. For example, when the MPE device receives a request to establish a session with a certain Quality of Service (QoS) level, you can use a policy rule to approve the request as is, to reject the request, or to make changes in the request before it is forwarded to the intended destination network element.

Structure and Evaluation of Policy Rules

The following topics provide an overview of how policy rules are structured and evaluated.

Note: The conditions, actions, and parameters available for your use in creating policy rules depend on the mode in which the CMP system is operating.

Structure of Policy Rules

Understanding how a policy rule is structured is helpful in understanding other Policy Management concepts. A policy rule is defined in an if-then structure, consisting of a set of conditions that the MPE device compares to information extracted from protocol messages and a set of actions that are executed (or not executed) when the conditions match. Many conditions can be tested for existence or non-existence (by optionally selecting the operator **is** or **is not**).

Policy Parameters

When you define a policy rule, you select from a list of available conditions and actions. Most of the conditions and actions are parameterized (that is, they contain placeholders that can be replaced with specific values to allow you to customize them as needed).

For example, consider the following policy rule, which has one condition and two actions:

```
where the device will be handling greater than 100 downstream sessions
set policy context property SessionClass to large
continue processing message
```

The condition, **where the device will be handling...**, allows the following parameters to be specified:

- An operator (*greater than*)
- A value (*100*)
- The flow direction (*downstream*)

The first action, **set policy context property ...**, specifies two parameters that represent the name and value of a policy context property to be applied to the request. The second action, **continue processing message**, instructs the MPE device to evaluate the remaining rules within the policy rules list (as opposed to immediately accepting or rejecting the request). The conditions and actions that are available for writing policies are discussed later in this section.

Policy Logical Operators

The policy wizard supports creation of rules using an explicit **AND** logical operator that contains a set of conditions. An AND operator must include at least two conditions. The actions are taken if all conditions are evaluated as true. For example, you can use an AND operator to define two conditions as follows:

```
And
  where the request is for downstream bandwidth
  where the requested guaranteed downstream bandwidth is greater than 2M bps
.
.
.
```

The policy wizard supports creation of rules using an **OR** logical operator that contains a set of conditions. An OR operator must include at least two conditions. The actions are taken if any condition is evaluated as true. For example, you can define the following set of conditions using an OR operator:

```
Or
  where the current time is between 18:00 and 23:59 using USER LOCAL TIME
  where today is a weekend day using USER LOCAL TIME
.
.
.
```

Finally, the policy wizard supports creation of rules using combinations of logical operators. You can nest operators. For example, you can define the following rule:

```
Or
  And
    where the request is for downstream bandwidth
    where the requested guaranteed downstream bandwidth is greater than
    2M bps
  where the session is an application session
  continue processing message
```

The policy wizard validates condition trees.

Evaluating Policy Rules

To write policy rules, it is important to understand how they are evaluated by the Policy Rules Engine contained within the MPE device, and how the engine fits into the protocol message processing within the MPE device.

If you look at the policy conditions that are available, you will see that many are not protocol specific. Although you can write protocol-specific policy rules, the Policy Rules Engine does not have any protocol knowledge. Instead, it deals with a set of abstractions that are mapped to the underlying protocol messages that are being processed. This allows the same policy rules to be used across multiple protocols.

When the MPE device receives a protocol message, it performs the initial processing of that message and then determines whether or not the message should be processed by the Policy Rules Engine. Generally, protocol messages that are either requesting bandwidth or modifying previous requests for bandwidth are processed by the Policy Rules Engine. Most other protocol messages are not. For example, a protocol message that releases bandwidth is typically not processed by the Policy Rules Engine because there is no reason to prevent or modify that action.

After a message is identified as a candidate for the policy rules, the MPE device attempts to associate as much information with the request as possible. For example:

- Which network elements will be impacted if the request is allowed to proceed?
- Which subscriber is associated with the request? What services is that subscriber entitled to?
- Which application is associated with the message?
- What time zone is the user equipment located in?

The reason for collecting this information is to make it available to the policy rules. The information that can be associated varies and depends on a number of factors, including:

- The protocol in question and how much information is provided in the protocol message
- The amount of network topology information that has been provisioned into the MPE device
- Whether there are other protocol sessions that can be associated with this message
- Whether there are external data sources configured that the MPE device can use to associate information with the message

When the process of associating information with the request is complete, the MPE device analyzes the information and maps it into several important abstractions that are central to the functioning of the Policy Rules Engine:

1. A list of network devices that the request affects. A network device is any network element, any logical or physical sub-component of a network element, or any other network equipment.
2. A list of flows associated with the request. A flow is a logical grouping of one or more packet filters and associated information such as QoS, charging, or service information. A flow can be in a single direction (either upstream or downstream). A flow can be a collection of bandwidth parameters. Different protocols can have a different number of flows associated with a message.

After constructing these lists, the Policy Rules Engine applies the policy rules according to the following algorithm:

```
For each network device:
  For each flow that is being created or modified:
    For each policy that is being evaluated:
      Evaluate all policy rules
    End
  End
End
```

It should be clear from this algorithm that a single message can result in multiple policies being evaluated, and a policy rule being evaluated multiple times. This is important to understand to ensure that the policy rules you write operate in the way you intended.

Note: Policies created using a more recent version of the CMP software may not evaluate and execute as intended on an MPE device running an older version of the MPE software. To ensure that policies are evaluated and executed as intended, update all systems to the same version of the software.

Creating a Policy

Policy rules are created and modified using the policy wizard in the CMP system. Once created or modified, the rule is stored in the policy library. The policy wizard guides you step by step to creating a new policy rule. The wizard displays only the options available at each step.

The following procedure describes how to create a new policy rule, using this policy as an example:

```
where the device type is B-RAS
  and where the device will be handling greater than 95 percent of downstream
  capacity

  reject message
```

To create a new policy rule:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the default is **ALL**.
2. From the content tree, select the **ALL** group.
The Policy Administration page opens in the work area.
3. On the Policy Administration page, click **Create Policy**.
The Create Policy page opens.
4. Select a starting point for the new policy:
 - **Blank** — The policy rule is created from the beginning, without any attributes being pre-defined.
 - **Use Template** — The policy rule is created based on a user-defined template that may have policy parameters pre-defined. This template can be modified as needed.
 - **Copy Existing Policy** — The policy rule is created based on an existing policy rule, which you modify as needed.
5. Click **Next**.
The Conditions page opens.
6. Select the desired policy conditions.
As a condition is selected, it appears in the Description area at the bottom of the page.
You can select multiple conditions, enter multiple instances of each condition, change the order of conditions, group conditions logically, or remove conditions:
 - To enter multiple instances of a condition, click the selection icon (•) in the Conditions window multiple times.
 - To combine a logical group of conditions, click **And**, located in the upper right corner of the Description window, and drag the conditions into the container that appears (represented by a folder icon). You can toggle a container between **And** and **Or** by double-clicking on the folder.
 - To change a condition's order of evaluation or include it within a logical container, drag and drop the condition within the Description window. You cannot drop a container onto itself or one of its sub-containers.
 - To negate a condition, change the **is** parameter if present.
 - To delete a condition or container from the rule, select it and click **Delete**. You are prompted, "The focused item and all its children will be deleted, Continue?" Click **OK**.

Tip: To add conditions directly to an existing container, select the container first.

For example:

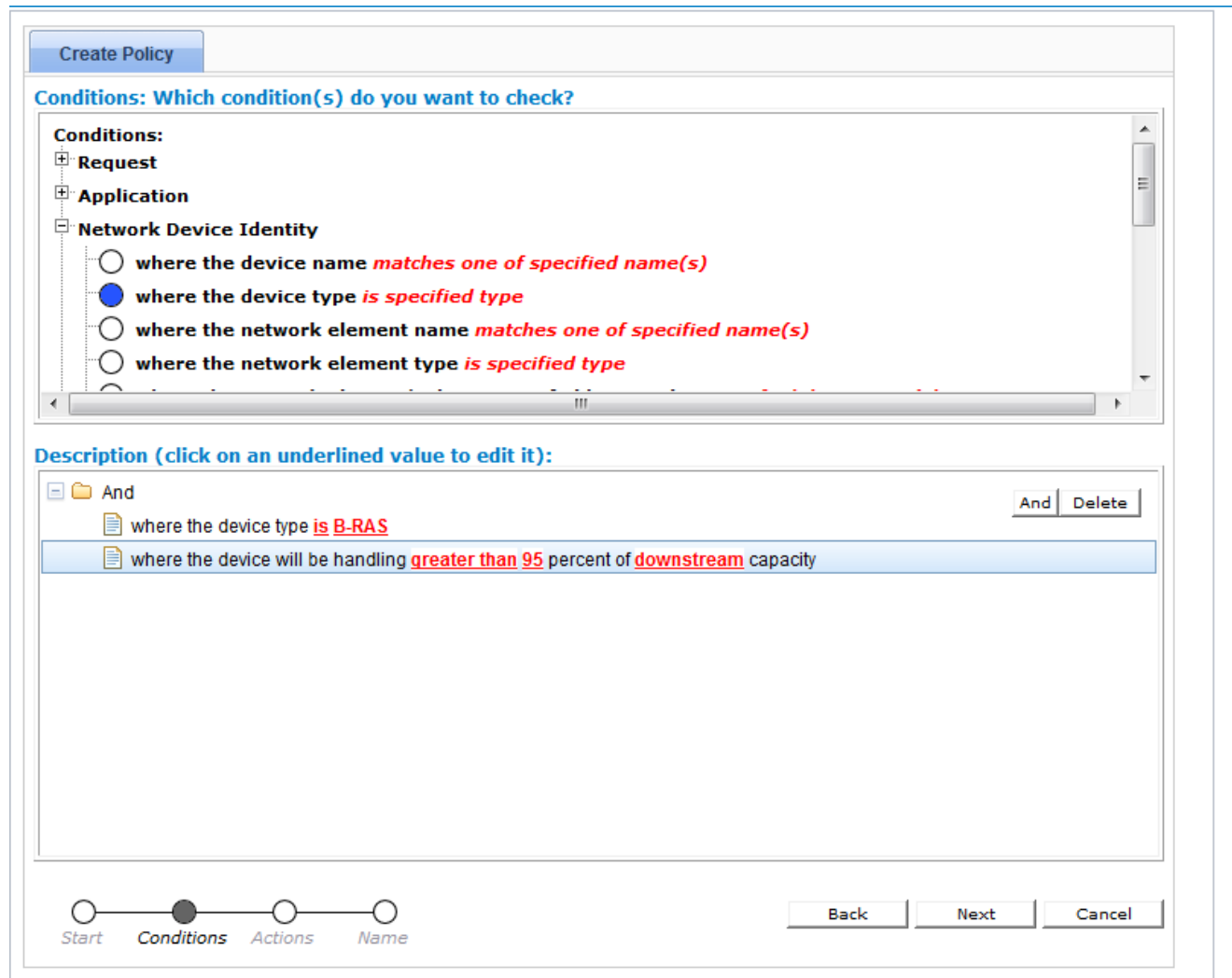


Figure 9: Selecting a condition

7. If a policy condition includes a parameter that requires further input, it displays red underlined text in the Description area. To provide the input, click the red underlined text; a popup window opens, from which you can do one of the following:
 - Select one or more options.
 - Enter a value (such as a traffic bit rate or percentage).

When you finish, click **OK**. The popup window closes and the input is added to the policy condition.

8. When you finish defining policy conditions, click **Next**. The Actions page opens.
9. Select the required action and any optional actions that the MPE device should execute if the policy request matches the defined conditions of the policy rule.

For example:

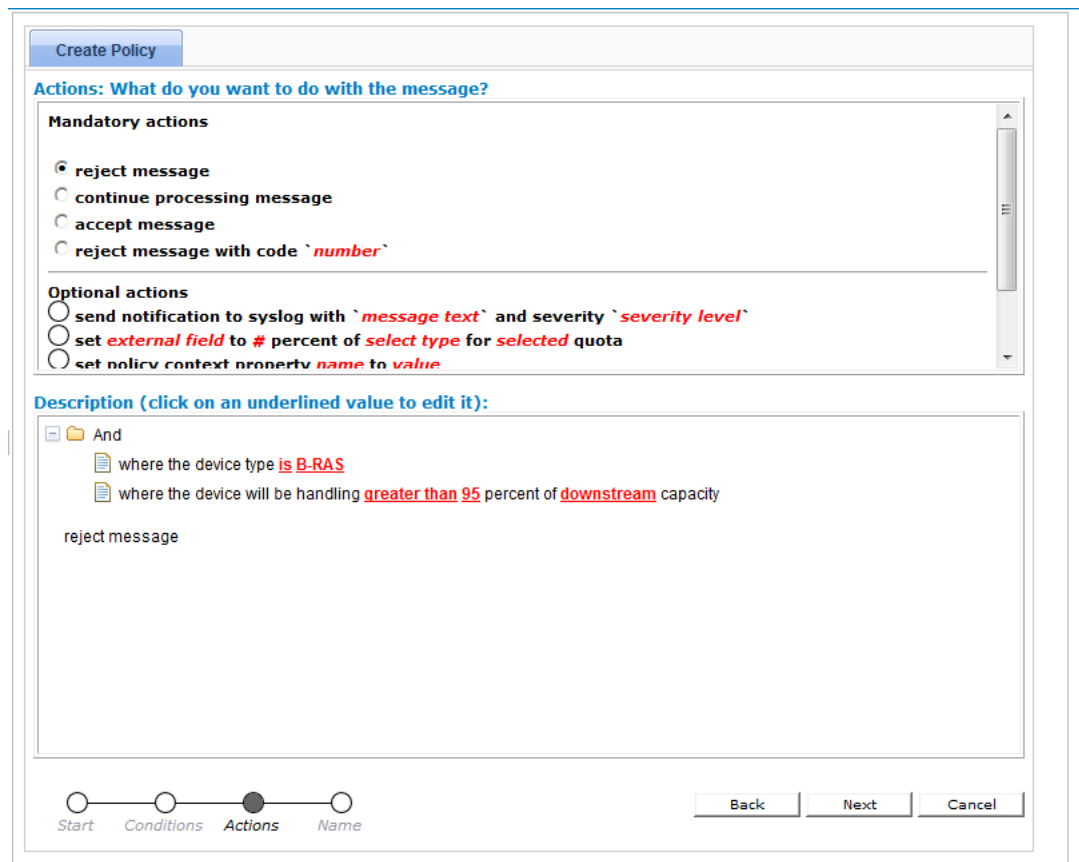


Figure 10: Selecting an action

- To enter multiple instances of an action, click the selection icon (■) multiple times
 - To move an action so that it is evaluated earlier in the rule, click the up icon (▲)
 - To move an action so that it is evaluated later in the rule, click the down icon (▼)
 - To delete an action from the rule, click the delete icon (✕)
10. When you finish, click **Next**.
The Name page opens.
 11. Assign a unique name (where uniqueness is not case sensitive) to the new policy rule (the name cannot contain the characters < > & ' " = % \ ;). For example:

Figure 11: Naming a policy

Note: The name can be up to 255 characters long and cannot contain the following characters: < > \ ; & ' " =

12. Click Finish.

The **Create Policy** page closes.

The policy rule is saved to the policy library in the CMP database.

Once a policy rule is created, you must deploy it to MPE devices so it can take effect. See [Managing Policy Rules](#).

Modes and the Policy Wizard

The policy wizard varies depending on the mode in which your CMP system is running. The mode configuration affects the following:

- Entire categories of conditions are made available or unavailable.
- Specific conditions and/or actions are made available or unavailable.
- Some conditions have a slightly different phrasing.
- The available values for some parameters vary.

If your policy wizard does not include a category, condition, action, or value documented here, it means that those categories, conditions, or actions are not available in your present CMP mode.

Parameters Within Policy Rules

When you are defining policy rules, both the conditions and actions may contain parameters. Parameters let you customize the specific situation in which a policy rule will be applied. Some conditions and actions may contain multiple parameters. For example, one possible condition is as follows:

where the device will be handling *greater than 100 upstream reserved* flows

This condition contains four different parameters. The policy wizard displays the parameters using a red font. In this example, *greater than* is a single parameter, as is *100*, *upstream*, and *reserved*.

You can click any parameter to open a pop-up window that lets you specify the value of that parameter. Each parameter has a data type associated with it that determines the values that can be specified: some may be numbers, some may be free-form text, and some may be limited to specific sets of values. For example, the following parameter is limited to a set of text values:

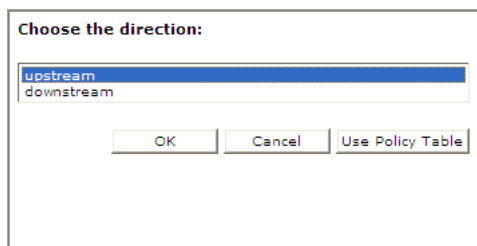


Figure 12: Example of a Parameter Pop-up

Conditions for Writing Policy Rules

The policy wizard supports a large number of conditions that can be used for constructing policy rules. To help you find the conditions you want, the conditions are organized into different categories, which are summarized in [Table 8: Policy Condition Categories](#).

Table 8: Policy Condition Categories

Category	Mode	Description
Request	All Modes	Conditions that are based on information that is explicitly contained within or related to the protocol message (request) that triggered the policy rule execution.
Application	All Modes	Conditions related to the application associated with the request. See Application Conditions .

Category	Mode	Description
Network Device Identity	All Modes	Conditions related to the specific network device for which the policy rule is being evaluated. This includes conditions based on the network device type, as well as those that refer to specific unique identifiers for network devices. See Network Device Identity Conditions .
Network Device Usage	All Modes	Conditions related to the calculated usage for the network device for which the policy rule is being evaluated. This usage includes device-level tracking of both bandwidth and flow/session counts. See Network Device Usage Conditions .
User	All Modes	Conditions related to the subscriber, or subscriber account, that is associated with the protocol message that triggered the policy rule execution. This includes subscriber-level and account-level tracking of usage. See User Conditions .
Policy Context Properties	All Modes	Conditions related to the context in which a policy is evaluated. See Policy Context Property Conditions .
Time of Day	All Modes	Conditions related to the time at which the policy rules are being executed. See Time-of-Day Conditions .

The conditions that are included within each of these categories are described in the sections that follow. Within each category, conditions are listed in alphabetical order. The parameters that can be modified within each condition are also detailed.

Request Conditions

Request conditions are based on information that is explicitly contained within, or related to, the protocol message (request) that triggered the policy rule execution.

where the request is for **downstream** bandwidth

Syntax

where the request is for *qos-direction* bandwidth

Parameters

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Distinguishes between protocol messages based on the direction of bandwidth that is being updated.

where the request *is* for *specified class of* traffic

Syntax

where the request *operator-binary* for *class-of-service* traffic

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

class-of-service

Select one or more from the list.

- **Best Effort**
- **Non Real-Time Polling**
- **Real-Time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

For Wireline mode:

- **Standard Definition**
- **High Definition**

Click OK.

Description

Distinguishes between protocol messages based on the class of service for the network traffic that is being updated.

where the requested *downstream* bandwidth is *greater than #* and *less than #* bps

Syntax

where the requested *qos-direction* bandwidth is *operator-greater bandwidth* and *operator-less bandwidth* bps

Parameters

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

Description

Selects protocol messages based on the direction and amount of bandwidth being requested, relative to a numeric value range.

where the requested guaranteed *downstream* bandwidth is *greater than # bps*

Syntax

where the requested guaranteed *qos-direction bandwidth is operator bandwidth bps*

Parameters

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second

g	gigabits per second
G	gigabits per second

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

Description

Selects protocol messages based on the amount of bandwidth being requested in a specific direction relative to a numeric value.

Application Conditions

Application conditions are related to the application associated with the request. See [Managing Application Profiles](#) for information on creating and managing application profiles.

where the application *is one of specified name*

Syntax

where the application *operator-binary* one of *app-name*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**.

Description

Triggers a policy based on the associated application.

where the application will be using *greater than #* and *less than # bps specified class of bandwidth*

Syntax

where the application will be using *operator-greater bandwidth* and *operator-less bandwidth bps class-of-service bandwidth*

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the associated application as it relates to a defined range. This can be further qualified by the allocation class of service of the bandwidth. The total represents the amount of bandwidth that is allocated if the current request is approved.

where the application will be using *greater than #* and *less than # downstream sessions*

Syntax

where the application will be using *operator-greater number* and *operator-less number qos-direction* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined range and direction. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using *greater than #* and *less than # specified class of sessions*

Syntax

where the application will be using *operator-greater number* and *operator-less number class-of-service* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined range. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using *greater than # specified class of* sessions

Syntax

where the application will be using *operator-greater number class-of-service* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined threshold. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using **greater than # bps upstream reserved** bandwidth

Syntax

where the application will be using *operator-greater bandwidth bps qos-direction qos-status bandwidth*

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

qos-status

One of the following:

- **reserved** (default)
- **committed**

Description

Triggers a policy based on the total amount of bandwidth used by the associated application as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the amount of bandwidth that is allocated if the current request is approved.

where the application will be using *greater than # bps of specified class of bandwidth*

Syntax

where the application will be using *operator-greater bandwidth bps of class-of-service bandwidth*

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the associated application as it relates to a defined threshold. This can be further qualified by the allocation class of service of the bandwidth. The total represents the amount of bandwidth that is allocated if the current request is approved.

where the application will be using *greater than # sessions*

Syntax

where the application will be using *operator-greater number sessions*

Parameters

operator-greater

One of the following:

- **greater than or equal to**

- **greater than** (default)

number

A numeric value.

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined threshold. The total represents the number of sessions that are allocated if the current request is approved.

where there is no application associated with the request

Syntax

where there is no application associated with the request

Parameters

None

Description

Triggers a policy when there is no associated application.

Network Device Identity Conditions

Network Device Identity conditions are related to the specific network device for which the policy rule is being evaluated. This includes conditions based on the network device type, as well as those that refer to specific unique identifiers for network devices. See the *CMP User's Guide* for information on defining the network elements available in your network.

where the device name *matches one of specified name(s)*

Syntax

where the device name *matches-op match-list*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**.

Description

Triggers a policy based on whether the device name matches one or more wildcard match patterns.

where the device type *is specified type*

Syntax

where the device type *operator-binary device-type*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

device-type

One or more of the following:

- **B-RAS**
- **Router**
- **VOD Server**
- **Interface**
- **Subscriber Group**
- **Wireline Gateway**

Click OK.

Description

Triggers a policy based on the device type for which it is evaluated.

where the network element name *matches one of specified name(s)*

Syntax

where the network element name *matches-op value-list*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click OK.

Description

Triggers a policy based on the name of the network element for which it is being evaluated.

where the network element type *is specified type*

Syntax

where the network element type *operator-binary element-type*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

element-type

One or more of the following:

- **B-RAS**
- **Router**
- **VOD Server**
- **Subscriber Group**
- **Wireline Gateway**

Click **OK**.

Description

Triggers a policy based on the type of network element for which it is being evaluated. If the policy is being evaluated for a device that is not a network element but is contained within a network element (such as an interface within a router) then the network element container is used as the basis of comparison.

where the network element's description field is equal to *specified description(s)*

Syntax

where the network element's description field is equal to *value*

Parameters

value

String.

Click **OK**.

Description

Triggers a policy that is only evaluated if the Description field of the network element matches the specified string.

Network Device Usage Conditions

Network Device Usage conditions are related to the calculated usage for the network device for which the policy rule is being evaluated. This usage includes device-level tracking of both bandwidth and flow/session counts.

where the device will be handling *greater than #* and *less than #* bps of *specified class of* sessions

Syntax

where the device will be handling *operator-greater number* and *operator-less number* bps of *class-of-service* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined range. This can be further qualified by the class of service of the sessions. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than #* and *less than #* bps of *specified class of* bandwidth

Syntax

where the device will be handling *operator-greater bandwidth* and *operator-less bandwidth* bps of *class-of-service* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined range. This can be further qualified by the class of service of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling **greater than #** and **less than #** percent of **downstream** capacity

Syntax

where the device will be handling *operator-greater bandwidth* and *operator-less bandwidth* percent of *qos-direction* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the percentage of capacity used by the current device as it relates to a defined range. This can be further qualified by the direction of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling **greater than #** and **less than # specified class of sessions**

Syntax

where the device will be handling *operator-greater number* and *operator-less number class-of-service* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**

- **less than** (default)

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined range. This can be further qualified by the class of service of the sessions. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than # bps downstream* bandwidth

Syntax

where the device will be handling *operator-greater bandwidth* bps
qos-direction bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined threshold and direction. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling **greater than #** bps of **specified class of** bandwidth

Syntax

where the device will be handling *operator-greater bandwidth* bps of *class-of-service* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined threshold. This is further qualified by the class of service of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling **greater than #** **downstream** sessions

Syntax

where the device will be handling *operator-greater number qos_direction* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

See common parameters.

qos-direction

See common parameters.

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined direction and threshold. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than # percent of downstream* capacity

Syntax

where the device will be handling *operator percent percent of qos-direction* capacity

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

percent

A numeric value.

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the percent of bandwidth capacity used by the current device as it relates to a defined threshold. This can be further qualified by the direction of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than # specified class of* sessions

Syntax

where the device will be handling *operator-greater number class-of-service* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined threshold. The total represents the number of sessions that are allocated if the current request is approved.

User Conditions

User conditions are related to the subscriber or subscriber account that is associated with the protocol message that triggered the policy rule execution. This includes subscriber-level and account-level tracking of usage. The following conditions are available.

where the account id *matches one of specified id(s)*

Syntax

where the account id *matches-op match-list*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific user ID values (based on matching wildcard patterns). See [Managing Subscribers](#) for information on accounts.

where the account will be handling *greater than #* and *less than #* percent of *downstream* limit

Syntax

where the account will be handling *operator-greater percent* and *operator-less percent* percent of *qos-direction* limit

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

percent

A numeric value.

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the percent of the bandwidth limit used by the account related to a defined range. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See [Managing Subscribers](#) for information on accounts.

where the account will be handling *greater than #* percent of *downstream* limit

Syntax

where the account will be handling *operator percent* percent of *qos-direction* limit

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**

- **not equal to**

The default for this condition is **greater than**.

percent

A numeric value.

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the percent of the bandwidth limit used by the account as it relates to a defined threshold. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See [Managing Subscribers](#) for information on accounts.

where the account will be using **greater than #** and **less than #** bps **downstream** bandwidth

Syntax

where the account will be using *operator-greater bandwidth* and *operator-less bandwidth* bps *qos-direction* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined range. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See [Managing Subscribers](#) for information on accounts.

where the account will be using **greater than #** and **less than # downstream** sessions

Syntax

where the account will be handling *operator-greater number* and *operator-less number qos-direction* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the number of sessions for a specific direction of service used by the account as it relates to a defined range. The total is the number of sessions allocated if the request is approved. See [Managing Subscribers](#) for information on accounts.

where the account will be using **greater than # bps downstream** bandwidth

Syntax

where the account will be using *operator bandwidth bps qos-direction* bandwidth

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined threshold. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See [Managing Subscribers](#) for information on accounts.

where the account will be using *greater than # bps of specified class of* bandwidth

Syntax

where the account will be using *operator-greater number* bps of *class-of-service* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined threshold. This can be further qualified by the class of service of the bandwidth. The total is the amount of bandwidth allocated if the request is approved.

where the account will be using *greater than # downstream* sessions

Syntax

where the account will be using *operator number qos-direction* sessions

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

qos-direction

One of the following:

- **upstream** (default)
- **downstream**

Description

Triggers a policy based on the total number of sessions used by the associated account as it relates to a defined threshold. This can be further qualified by the direction of the sessions. The total represents the number of sessions that are allocated if the current request is approved. See [Managing Subscribers](#) for information on accounts.

where the account will be using *greater than # specified class of* sessions

Syntax

where the account will be using *operator-greater number class-of-service* sessions

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions for specific classes of service used by the account as it relates to a defined threshold. This can be further qualified by the class of the sessions. The total is the number of sessions allocated if the request is approved. See [Managing Subscribers](#) for information on accounts.

where the tier *is one of specified tier(s)*

Syntax

where the tier *operator-binary* one of *tiers*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

tiers

A comma-separated list of names of one more tiers defined in the CMP database.

Click OK.

Description

Triggers a policy that is or is not evaluated for one or more specific tiers. See [Managing Subscribers](#) for information on tiers.

where the tier will be handling *greater than #* and *less than # specified class of sessions*

Syntax

where the tier will be handling *operator-greater number* and *operator-less number class-of-service session*

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions for a specific class of service used by the tier as it relates to a defined range. The total is the number of sessions allocated if the request is approved. See [Managing Subscribers](#) for information on tiers.

where the tier will be handling *greater than # specified class of sessions*

Syntax

where the tier will be handling *operator-greater number class-of-service sessions*

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions for a specific class of service used by the tier as it relates to a defined threshold. The total is the number of sessions allocated if the request is approved. See [Managing Subscribers](#) for information on tiers.

where the tier will be using **greater than # bps of specified class of bandwidth**

Syntax

where the tier will be using *operator-greater number* and *operator-less number* bps of *class-of-service* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the tier as it relates to a defined threshold. This is further qualified by the class of service of the bandwidth. The total is the amount of bandwidth allocated if the request is approved. See [Managing Subscribers](#) for information on tiers.

where the tier will be using *greater than #* and *less than #* bps of *specified class of bandwidth*

Syntax

where the tier will be using *operator-greater number* and *operator-less number* bps of *class-of-service* bandwidth

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the tier as it relates to a defined range. This can be further qualified by the class of service of the bandwidth. The total is the amount of bandwidth allocated if the request is approved. See [Managing Subscribers](#) for information on tiers.

where the User's Tier *downstream* bandwidth limit is between # bps and # bps

Syntax

where the User's Tier *qos-direction* bandwidth limit is between *bandwidth* bps and *bandwidth* bps

Parameters

qos-direction

One of the following:

- **upstream**
- **downstream** (default)

Click OK.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**.

Description

Triggers a policy that is evaluated for a user tier based on the bandwidth limit. This can be further qualified by the direction of the bandwidth.

Example

```
where the User's Tier downstream bandwidth limit is between 2M bps and 25M bps
```

where the User's Tier *downstream* bandwidth limit is *greater than #* bps

Syntax

```
where the User's Tier qos-direction bandwidth limit is operator bandwidth bps
```

Parameters

qos-direction

One of the following:

- **upstream**
- **downstream** (default)

Click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**.

Description

Triggers a policy that is evaluated for a user tier based on the comparison between the bandwidth limit and a numerical value. This can be further qualified by the direction of the bandwidth.

Example

```
where the User's Tier downstream bandwidth limit is less than or equal to 25M bps
```

Policy Context Property Conditions

Policy Context Properties are user-defined name/value string pairs that can be created from policy actions and evaluated from policy conditions. By using policy context properties, one policy can influence the execution of other policies. Policy context properties exist across multiple policy executions on the same request, but are not persistent across requests.

where the policy context property *name exists*

Syntax

where the policy context property *property-name accessibility*

Parameters

property-name

String.

Click **OK**.

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Triggers a policy based on whether or not the specified policy context property exists.

where the policy context property *name* is numerically *equal to value*

Syntax

where the policy context property *property-name* is numerically *operator value*

Parameters

property-name

String.

Click OK.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

For this condition the default is **equal to**.

value

String.

Integer value in the inclusive range of $-9,223,372,036,854,775,808$ to $9,223,372,036,854,775,807$ (that is, -2^{63} to $2^{63} - 1$).

Description

Triggers a policy based on a numerical comparison between the specified policy context property value and a specified value.

where the policy context property *name matches one of `value(s)`*

Syntax

where the policy context property *property-name matches-op `match-list`*

Parameters

property-name

String.

Click OK.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**.

Description

Triggers a policy based on whether the specified policy context property value matches a list of specified values (based on matching wildcard patterns).

Time-of-Day Conditions

Time-of-Day conditions are related to the time at which the policy rules are being executed.

where the current time *is* between *start time* and *end time* using *configured local time*

Syntax

where the current time *operator-binary* between *time-of-day* and *time-of-day* using *time-zone*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

time-of-day

A time, in the format of *hh:mm*, where *hh* is a number in the range from 0 to 23.

Click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location configured for the user equipment's location

Click **OK**.

Description

Triggers a policy based on time. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

where today is a week day using *configured local time*

Syntax

where today is a week day using *time-zone*

Parameters

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location configured for the user equipment's location

Click **OK**.

Description

Triggers a policy based on the day of the week. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

where today is a weekend day using *configured local time*

Syntax

where today is a weekend day using *time-zone*

Parameters

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location configured for the user equipment's location

Click **OK**.

Description

Triggers a policy based on the day of the week. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

where today *is day* using *configured local time*

Syntax

where today *operator-binary day-of-week* using *time-zone*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

day-of-week

One of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

Click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location configured for the user equipment's location

Click **OK**.

Description

Triggers a policy based on the day of the week. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Actions for Writing Policy Rules

The policy wizard supports a large number of actions that can be used for constructing policy rules. There are two types of policy-processing actions:

- | | |
|--------------------------|--|
| Mandatory actions | This action defines what happens when the current policy is through executing. When you are creating a policy rule in the policy wizard, these actions are displayed at the top of the list of available actions with a radio button that forces you to select only one of these actions. |
| Optional actions | These are actions executed when the conditions in the policy rule have been met. When you are creating a policy rule in the policy wizard, this is a list of actions that you can add to your policy rule. You can select none, one, several, or up to 40 of these optional actions per rule. However, each action is limited, so that it can be executed only once per policy rule. |

In the same way that you can customize conditions by editing parameter values, many of these actions can be customized by specifying parameter values as well.

Actions are listed in alphabetical order. Actions also are affected by the current mode. Therefore, some of the actions documented may not be available in your policy wizard.

Mandatory Policy-Processing Actions

Policy-processing actions define what the Policy Engine should do when the current policy is through executing. The following are the mandatory policy-processing actions; one of these actions must be selected in each policy.

accept message

Syntax

`accept message`

Parameters

None

Description

After executing the current policy rule, the Policy Engine continues with the normal processing of the protocol message but no further policy rules are evaluated.

continue processing message

Syntax

`continue processing message`

Parameters

None

Description

After executing the current policy rule, the Policy Engine continues with the next policy rule.

reject message

Syntax

`reject message`

Parameters

None

Description

After executing the current policy rule, the Policy Engine terminates all policy-rule processing and rejects the current protocol message. The specific interpretation of rejecting the message varies depending on the associated protocol. For most application-level requests this translates into some type of error being sent back to the application.

reject message with code *number*

Syntax

reject message with code *number*

Parameters

number

qos-direction

A numeric value.

This value is an integer from 1–2000000000.

Description

After executing the current policy rule, the generated code is propagated back to the VoD server.

Optional Policy-Processing Actions

The following optional policy-processing actions are available.

remove all policy context properties

Syntax

remove all policy context properties

remove policy context property *name*

Syntax

remove policy context property *property-name*

Parameters

property-name

String. May contain policy rule variables (see [Policy Rule Variables](#)) to perform parameter substitution within the property name.

Click OK.

Description

Removes a policy context property.

send notification to syslog with ``message text`` and severity ``severity level``

Syntax

send notification to syslog with ``message`` and severity ``level``

Parameters

message

String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

Click **OK**.

level

The sevlog severity. One of the following:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

Click **OK**.

Description

Sends a message to the syslog service containing the specified message text and at the specified severity level.

Note: Policies written before V7.5 that used the action `send alert` with ``text`` and severity ``severity level`` will be converted to use this action, which sends a notification to the syslog instead of an alarm to the CMP system.

set policy context property *name* to *value*

Syntax

set policy context property *property-name* to *value*

Parameters

property-name

String.

May contain policy rule variables (see [Policy Rule Variables](#)) to perform parameter substitution within the property name.

Click **OK**.

value

String.

Click **OK**.

Description

Sets and saves a subscriber property in the SPR. You can specify that the property is not saved if the policy rejects the message.

Policy Rule Variables

During policy rule execution within the MPE device, some actions (for example, **send notification**) allow for substitution of policy rule variables with contextual information. Each time the policy rules are evaluated, the unique set of policy rule variables is referred to as the policy context. This section summarizes these policy rule variables.

Using Policy Rule Variables

One use of policy rule variables is in an action to perform substitution of textual information into a text message that is being used for some type of logging. The variable is inserted into the text message when you define the action.

The format of a policy rule variable is as follows:

```
{name[:default-value]}
```

The name can contain the following characters:

- A–Z
- a–z
- 0–9
- underscore (_)
- period (.)
- and backslash (\)

The following are examples of policy rule variables:

```
{Bandwidth}
```

```
{Device.Name}
```

```
{Device.Name:UNKNOWN}
```

Basic Policy Rule Variables

Under certain circumstances an MPE device can associate additional context information with a request. This information may be used during the policy rule execution. The availability of this information depends on:

- The carrier network environment (wireless, cable, or wireline) in which the MPE device is executing

- Whether the information is provisioned on the MPE device or, if present, a Subscriber Profile Repository (SPR)
- The protocol in use and how much information is available in the request (some protocols have optional information which, if specified, can be used to associate additional information)

A number of policy rule variables can provide information about the device for which a policy rule is being executed. Some of these variables are only meaningful in certain modes, while others are available in all modes. Likewise, some of these variables are only available for certain device types, while others are available for all devices.

[Table 9: Basic Policy Rule Variables](#) displays some of the basic policy rule variables that are available.

Table 9: Basic Policy Rule Variables

Variable Name	Description	Modes, Protocols, Device Type
{Policy}	The name of the policy rule that is being executed.	Any mode
{Date}	The date when the policy rule is executed, in the following format: MMM[mm]/dd [/yyyy] where MMM Specifies the month. For example: Feb mm Specifies the month numerically. For example: 02 dd Specifies the day of the month. For example: 09 yyyy Specifies the year. For example 2017	Any mode
{Time}	The time when the policy rule is executed, in the following format: hh:mm:ss.SSS .	Any mode
{Conditions}	A list of (variable, value) tuples that lists the variables whose values were referenced in the conditions of the policy rule. The list is inserted with one variable per line in the following format: variable=value .	Any mode
{Device}	The name of the device for which the policy rule is being evaluated.	Any mode
{DeviceId}	ID of the device for which the policy rule is being evaluated.	Any mode
{QosDir}	The direction of the flow for which the policy rule is being evaluated, either Up or Down.	Any mode
{Bandwidth}	The DOCSIS type of the flow for which the policy rule is being evaluated: <ul style="list-style-type: none"> • BES 	Any mode

Variable Name	Description	Modes, Protocols, Device Type
	<ul style="list-style-type: none"> • N RTP • RTP • UGS • UGSAD 	
{Device.DownstreamCapacity}	The downstream bandwidth capacity of the device.	Any device
{Device.FlowCount}	The number of active flows for the device.	Any device
{Device.Name}	The name (as defined in the CMP database) of the device.	Any device
{Device.UpstreamCapacity}	The upstream bandwidth capacity of the device.	Any device
{Element.BackupHostname}	The hostname (or IP address) of the backup network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any device
{Element.DownstreamCapacity}	The downstream bandwidth capacity of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any device
{Element.UpstreamCapacity}	The upstream bandwidth capacity of the network element associated {Element.UpstreamCapacity} with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any device
{Element.Hostname}	The hostname (or IP address) of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any device
{Element.Name}	The name (as defined in the CMP database) of the network element associated with the current device. If the device is a network element, then this is the	Any device

Variable Name	Description	Modes, Protocols, Device Type
	same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	
{Element.UpstreamCapacity}	The upstream bandwidth capacity of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any device
{Session.IMEI}	This variable expands to the IMEI of the subscriber's phone or equipment associated with the request.	Any device
{Session.IMEISV}	This variable expands to the IMEISV of the subscriber's phone or equipment associated with the request.	Any device
{User.Pool} or {User.Pool.PoolId}	The ID of the pool for the subscriber.	Wireless
{User.Pool.BillingDay}	The pool profile billing day for the subscriber.	Wireless
{User.Pool.Entitlement}	The pool profile entitlement the subscriber.	Wireless
{User.Pool.Tier}	The pool profile tier for the subscriber pool.	Wireless
{User.Pool. <i>custom</i> }	A pool profile custom field for the subscriber.	Wireless
{User.Pool.State. <i>prop</i> }	A pool state property for the subscriber.	Wireless
{User.Quota. <i>name</i> .ServiceSpecific}	The total initial service-specific events for the subscriber in the quota <i>name</i> . This variable applies to subscriber-level and pool-level quota defined on the MPE device.	Wireless
{User.Quota. <i>name</i> .Time}	The total initial time in seconds for the subscriber in the quota <i>name</i> . This variable applies to subscriber-level and pool-level quota defined on the device.	Wireless
{User.Quota. <i>name</i> .Volume}	The total initial volume in bytes for the subscriber in the quota <i>name</i> . This variable applies to subscriber-level and pool-level quota defined on the device.	Wireless

Policy Rule Examples

The following are examples of policy rules.

Orange_GWR

```
where the device type is Interface
  and where the network element type is B-RAS
  and where the device will be handling greater than 200M bps downstream
  bandwidth
  and where the device will be handling less than 2500M bps downstream
  bandwidth
  and where the device will be handling greater than 25 percent of
  downstream capacity

send notification with `LC002, {Element.Name},{Interface.Name},
{Interface.DownstreamCapacity},{Device.FlowCount},{Account.AccountId},
{AccountTier.Name},{Bandwidth},{Account.EndpointId}` and severity `Warning`
continue processing message
```

Red_GWR

```
where the device type is Interface
  and where the network element type is B-RAS
  and where the device will be handling greater than 2500M bps downstream
  bandwidth
  and where the device will be handling greater than 50 percent of
  downstream capacity

send notification with `LC002, {Element.Name},{Interface.Name},
{Interface.DownstreamCapacity},{Device.FlowCount},{Account.AccountId},
{AccountTier.Name},{Bandwidth},{Account.EndpointId}` and severity `Alert`
reject message
```

Reject_Subscriber_Session

```
where the account will be handling greater than 100 percent of downstream
  limit

send notification with `SR002, {Account.AccountId}, {AccountTier.Name},
{Bandwidth}, {Account.EndpointId}` and severity `Alert`
reject message
```

Policy rule variable

The following example illustrates the use of a policy rule variable.

```
where the device type is Interface
  and where the policy context property donotreject does not exist
  and where the device will be handling greater than 70 percent of
```

downstream capacity

reject message

Chapter 8

Managing Policy Rules

Topics:

- [Displaying a Policy.....130](#)
- [Deploying Policy Rules.....130](#)
- [Modifying and Deleting a Policy.....133](#)
- [Policy Templates.....134](#)
- [Managing a Policy Group.....136](#)
- [Importing and Exporting Policies, Policy Groups, and Templates.....142](#)

Policy rules are created and saved within the CMP database and then deployed to MPE devices. The CMP system lets you create and modify the details within policy rules, as well as edit the order in which policy rules are applied to a protocol message.

To create policy rules, see [Understanding and Creating Policy Rules](#). This chapter describes how to manage your library of policy rules and policy groups.

Displaying a Policy

To display a policy:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**. The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy. The policy is displayed. [Figure 13: Sample Policy Description](#) shows an example.



Figure 13: Sample Policy Description

You can choose from two logical views of policy conditions:

- A tree format (shown)
- A Boolean expression format similar to SQL

To switch between one views, click **Toggle View**.

Deploying Policy Rules

Deploying a policy (or policy group) is the act of transferring the policy from the CMP policy database to an MPE device. After a policy is deployed, the rules defined within the policy or policy group are used as decision-making criteria by the MPE device.

[Figure 14: Policy Deployment](#) shows how policies P1 through P7 are created in the CMP database and then deployed individually to different MPE devices within the network. Each of the policies is associated individually with the MPE device where it is deployed. In the example, each policy server

(MPE device) displays the policies that have been deployed to it and the order in which they are applied to policy requests, from top to bottom.

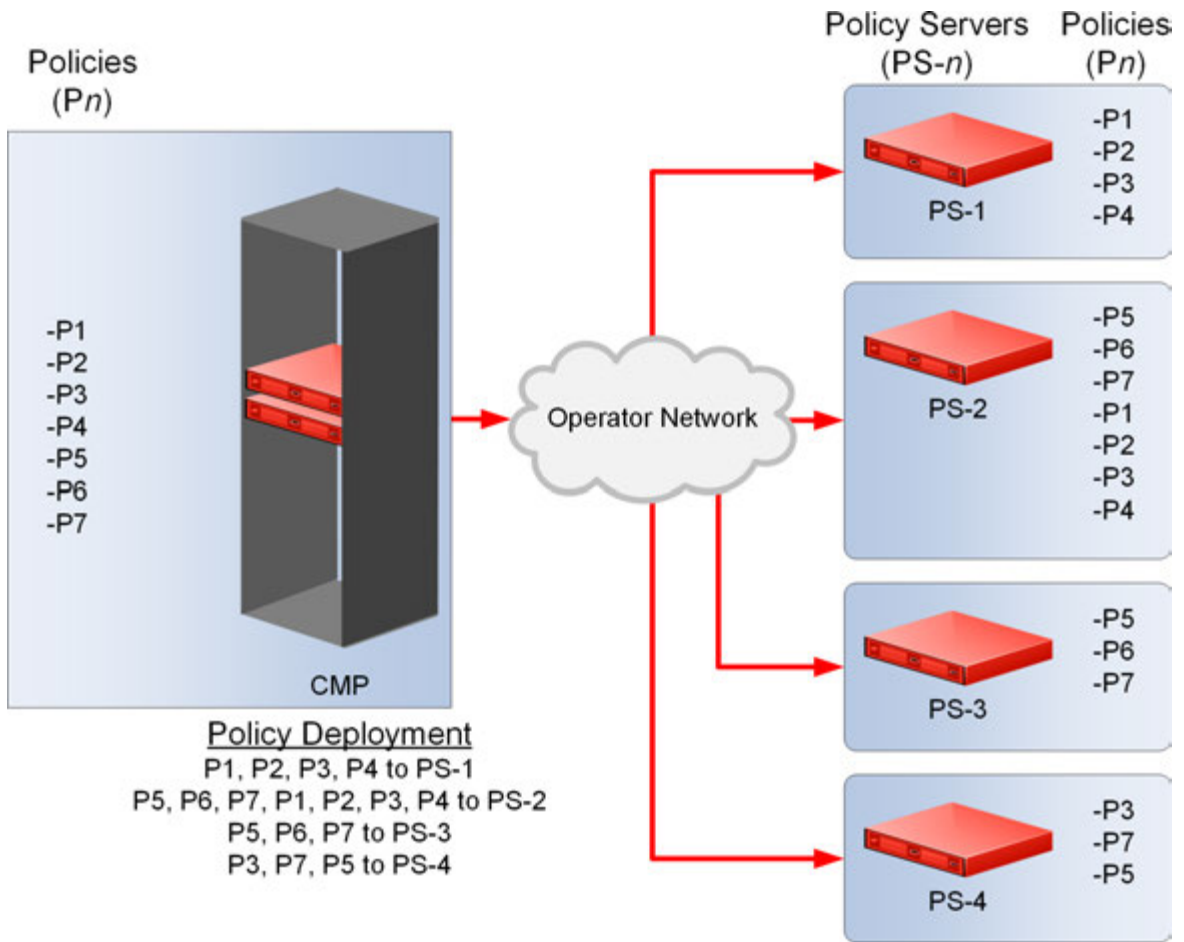


Figure 14: Policy Deployment

Figure 15: Policy Group Deployment shows how the same library of policies can be grouped first and then deployed as policy groups. When a policy group is created, the policies are arranged in the order in which they are to be evaluated. Grouping policies makes deployment of multiple policies easier and helps to ensure consistency in how policies are applied to policy requests on different MPE devices.

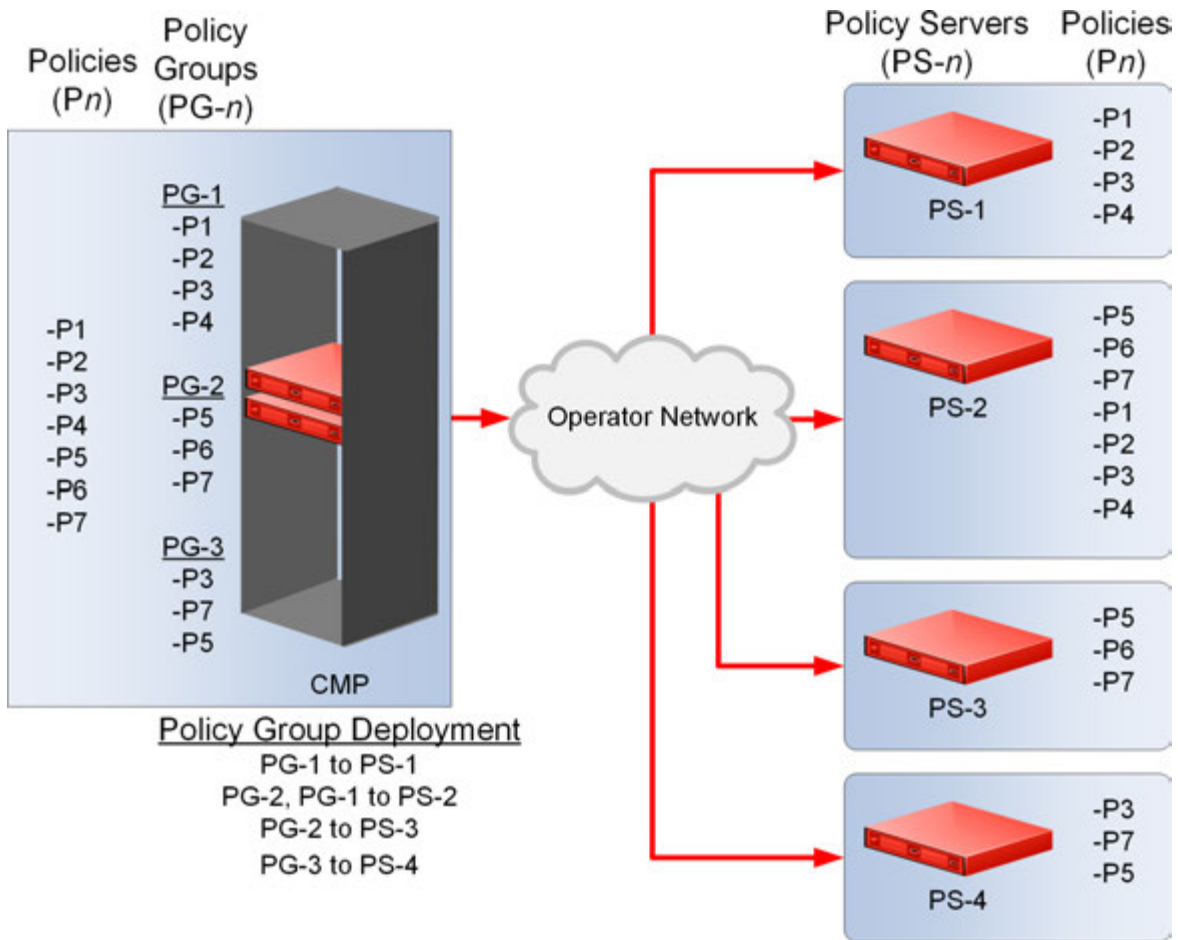


Figure 15: Policy Group Deployment

When you first create a policy rule, that rule exists only within the CMP database. After the policy rule is deployed, any change to the policy rule is automatically redeployed when you complete your changes. Automatic redeployment also applies to policy groups as well: any change to a policy group triggers automatic redeployment. If you add a policy rule that was not previously deployed to a policy group that is deployed to one or more MPE devices, then the rule is deployed automatically to those MPE devices.

Figure 16: Policy Redeployment shows that when a policy (P3) is modified, its associated groups (PG-1 and PG-3) are redeployed automatically.

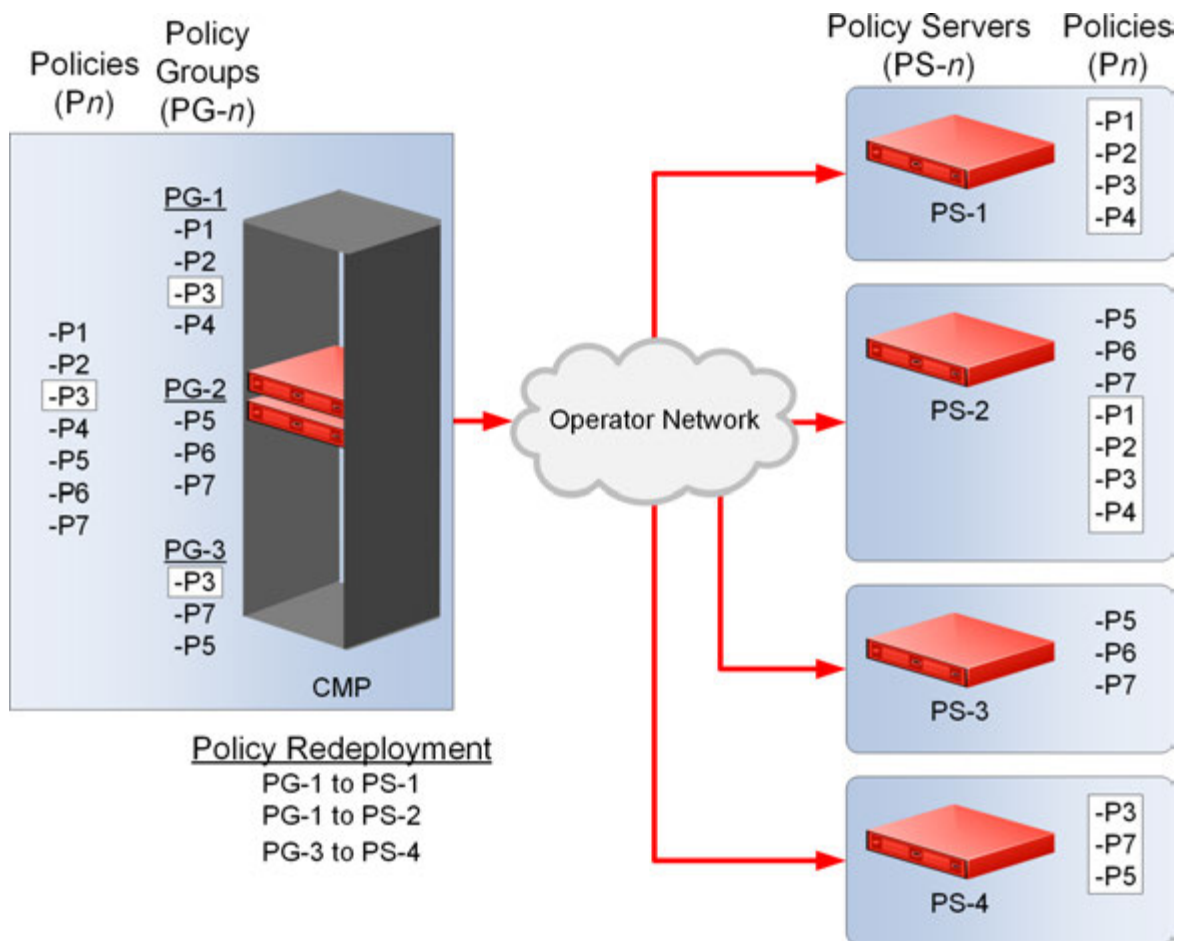


Figure 16: Policy Redeployment

Modifying and Deleting a Policy

Policies can be modified and then redeployed to MPE devices. When a policy that resides in multiple policy groups is modified, the changes are propagated to the various groups.

Modifying a Policy

To modify an existing policy:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Administration** page opens in the work area, listing the available policies.
3. Select the policy you want to edit.
The **Policy Administration** page displays information about the policy.
4. Click **Modify**.

The policy wizard opens in a **Modify Policy** tab.

5. Edit the policy information.

See [Creating a Policy](#) for details on the fields within the policy wizard.

6. When you finish, click **Finish**.

The policy is modified. The modified policy is now ready to be added to a policy group (see [Adding a Policy or a Policy Group to a Policy Group](#)), or deployed to one or more MPE devices (see [Deploying a Policy or Policy Group to MPE Devices](#)).

Note: Redeployment of a policy is automatically performed to those MPE devices where the policy was initially deployed.

Deleting a Policy

Policies, policies within a policy group, and entire policy groups can be removed from an MPE device when they are no longer needed. Because the policy still resides in the CMP database, it can be redeployed at a later date if needed. If a policy is no longer needed, it can be deleted from the CMP database as well.

Note: Deleting a policy from the CMP database automatically removes the policy from all associated MPE devices.

To delete a policy:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Administration** page opens in the work area, displaying all defined policies.
3. Use one of the following methods to select the policy to delete:
 - From the work area, click the **Delete** icon located to the right of the policy you want to delete.
 - From the policy group tree, select the policy. The **Policy Administration** page opens. Click **Delete**.

A confirmation message displays.

4. Click **OK** to delete the policy.

The policy is deleted.

To remove a deployed policy from an MPE device, see [Removing a Policy or Policy Group from an MPE Device](#).

Policy Templates

The CMP system lets you create policy templates to simplify the creation of multiple policies with similar conditions and actions. A policy template is similar to a policy, except that some (or all) of the parameters in the conditions and actions are not completely defined. Those parameters are defined later, when you use the policy template to create policy rules.

The policy template wizard is used to create or modify a policy template. This wizard is similar to the policy wizard; however, the policy template wizard allows parameters to be only partially defined.

For example, a template may only be configured for policy requests requiring bandwidth above a certain value, but not define the exact bandwidth value. You can then specify a specific bandwidth value when you use the template to create the new policy rule.

Creating a Policy Template

To create a policy template:

1. From the **Policy Management** section of the navigation pane, select **Template Library**.
The content tree displays the **Template Library** group.
2. Select the **Template Library** group.
The **Template Administration** page opens in the work area.
3. Click **Create Template**.
The **Create New Policy Template** window opens.
4. Select the base policy or policy template with which to begin:
 - **Blank** — No policy template attributes are pre-defined.
 - **Use Template** — Select an existing template with pre-defined attributes. Modify the template as needed, then save the template with a new template name.
 - **Copy Existing Policy** — Select an existing policy. Modify the policy, then save the policy as a policy template.
5. Edit the policy information from one or more of the policy wizard pages.
See [Creating a Policy](#) for details on the fields within the policy wizard.
6. When you finish, click **Finish**.
The window closes.

The policy template is created.

Modifying a Policy Template

You can edit a policy template to make changes. Modifying a policy template does not modify previously configured policies.

To modify an existing policy template:

1. From the **Policy Management** section of the navigation pane, select **Template Library**.
The content tree displays the **Template Library** group.
2. Select the **Template Library** group.
The **Template Administration** page opens in the work area.
3. Select the template you want to modify.
The **Template Administration** page displays a description of the template.
4. Click **Modify**.
The **Modify Policy** tab opens with the last step of the template creation process. [Figure 17: Modify Policy Template Window](#) shows an example.
5. The wizard begins at the last step of the template creation process. Click **Back** to return to where you want to edit the template and modify the information.
6. When you finish, click **Finish** to save the modified template.

The template is modified.

Modify Policy

Name: Please specify a name.

Apply ADC rule by default

Description (click on an underlined value to edit it):

where the request is creating a new flow

✕ apply ADC-Rule1 to request
accept message

Tables Conditions Actions **Name**

Back Finish Cancel

Figure 17: Modify Policy Template Window

Deleting a Policy Template

To delete a policy template:

1. From the **Policy Management** section of the navigation pane, select **Template Library**.
The **Template Administration** page opens in the work area, displaying all defined policy templates.
2. Use one of the following methods to select the policy template to delete:
 - From the work area, click the **Delete** icon, located to the right of the policy template you want to delete.
 - From the template library, select the template. The **Template Administration** page displays the template. Click **Delete**.

A confirmation message displays.

3. Click **OK** to delete the policy template.

The policy template is deleted.

Managing a Policy Group

The CMP system lets you create policy groups. Policy groups are an organizational aid that provide for flexible policy management. You save policies to a group in the order in which you want an MPE device to apply them to a policy request. If needed, you can change that order. You can save a policy to multiple policy groups and add a policy to, or remove it from, a policy group at any time. You can also group, or nest, policy groups.

Creating a Policy Group

To create a new policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **Policy Administration** page opens in the work area, listing available policies.
3. Click **Create Group**.
The group naming field opens in the work area.
4. Enter the name to assign to the new group.
The name can be up to 64 characters long and must not contain quotation marks (") or commas (,).
5. Click **Save**.

The new group information is saved to the CMP database and displayed in the content tree.

Adding a Policy or a Policy Group to a Policy Group

After you create a policy group, you can add policies to the group. You can also add policy groups to a policy group.

Note: It is recommended that you only nest policy groups two levels deep.

To add one or more policies or policy groups to a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy group to which you want to add the policy or policy group.
The **Policy Administration** page opens in the work area, listing the policies and policy groups currently in the group.
3. Click **Modify**.
The **Policy Administration** page opens in the work area.
4. Click **Add**.
A window opens, displaying the policies and policy groups available.
5. You can optionally filter the list by policies or policy groups. From the list, select **Policy** to display policies, **Group** to display policy groups, or **All** (default) to list both policies and policy groups.
6. Select the policy or group to add to this group and click **Add**. Use Shift/click to select multiple policies or policy groups. By default policies and policy groups are added after the first item in the group; to change the insert position, change the value in the **Location** field.
The policies or policy groups are added to the policy group in the specified location and the window closes.

Note: Policies or policy groups are applied to messages in the order in which they appear in the policy group. You can change the sequential order (see [Changing the Sequence of Deployed Policies or Policy Groups](#)).

7. Click **Save**.

The added policies and policy groups are displayed in the policy group tree. You can deploy the policy group to the policy servers (see [Deploying a Policy or Policy Group to MPE Devices](#)).

Note: If this group had been deployed previously, it is automatically redeployed at this time, ensuring the MPE devices are synchronized with the CMP database.

Removing a Policy from a Policy Group

Removing a policy from a policy group that has been saved to the CMP database only removes the policy from the selected policy group. The policy remains in the **ALL** group, as well as any other group to which it had been added. (To remove a policy from all groups in the Policy Library, see [Removing a Policy or Policy Group from an MPE Device](#).)

To remove a policy from a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy group.
The **Policy Administration** page opens in the work area, listing the policies it contains.
3. Remove the policy using one of the following methods:
 - From the content tree, select the policy within the policy group; the profile information for the policy is displayed. Click **Remove**.
 - From the content tree, select the policy group and click **Modify**. Select the remove icon, located to the right of the policy you want to remove.





The modified policy group is redeployed, ensuring that the MPE devices are resynchronized with the CMP database.

Note: If the policy group has never been deployed, you can now deploy it to MPE devices (see [Deploying a Policy or Policy Group to MPE Devices](#)).

Changing the Sequence of Policies or Policy Groups Within a Policy Group

The order in which policies or policy groups appear in a policy group is the order in which they are deployed and applied to policy requests. You can modify the order of policies or policy groups, both inside and outside of a policy group.

To change the order of the policies or policy groups within a group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy group.
The **Policy Administration** page opens in the work area, displaying policies or policy groups in their current sequential order.
3. Click **Modify**.
The **Manage Policies** page opens.
4. Use any of the following options to change the sequence of policies or policy groups within the group:
 - Use the  (top) and  (bottom) icons, located to the left of policies or policy groups. The  (top) icon moves the item it to the top of the list. The  (bottom) icon moves the item it to the bottom of the list.
 - Drag and drop policies or policy groups to a different position in the sequence.

- Change the sequence numbers, located to the left of policies or policy groups. Click **Update Order** to refresh the display.
- Optionally, you can click **Undo** or **Redo** to step back and forth through your changes.

5. Click **Save**.

The modified policy group is redeployed, ensuring that the MPE devices are resynchronized with the CMP database.

Note: If the policy group has never been deployed, you can now deploy it to MPE devices (see [Deploying a Policy or Policy Group to MPE Devices](#)).

Displaying Policy Details Contained Within a Policy Group

To display the policies within a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy group.
The **Policy Administration** page opens in the work area, listing the policies it contains.
3. Click **Show Details**.
The configured policies, including the configured parameters for the policies, are displayed. To switch between logical views of policy conditions, click **Toggle View**.
4. When you finish, click **Cancel**.

Deploying a Policy or Policy Group to MPE Devices

The basic procedure for deploying either a policy or a policy group to MPE devices is the same. The following procedure uses the example of deploying a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy or policy group to deploy.
The **Policy Administration** page opens in the work area, listing the policies it contains.
3. Click **Deploy**.
The policy server tree is displayed, listing all possible target policy servers (MPE devices) and server groups. You can expand the tree view if necessary.
4. Select the target MPE devices or policy server groups.

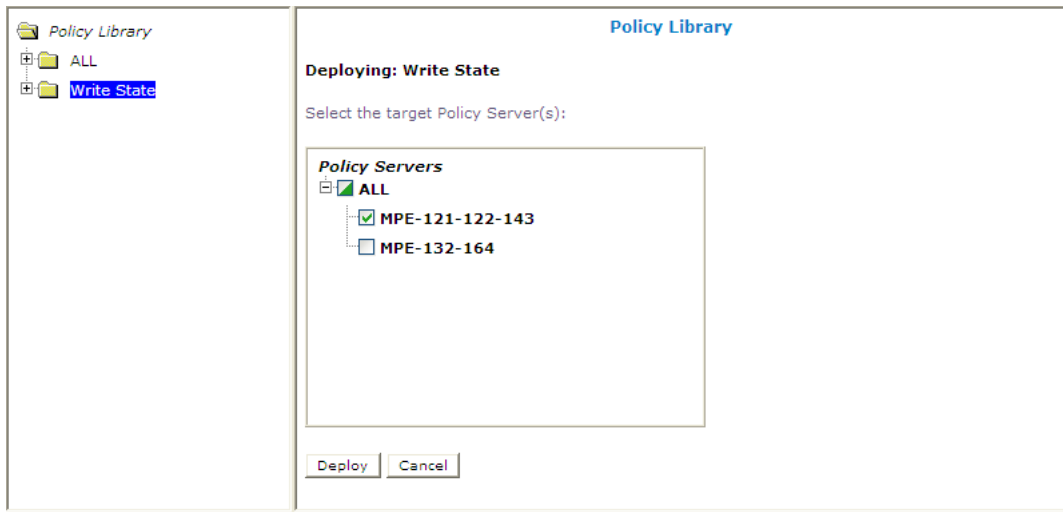


Figure 18: Policy server selection window

An icon indicates whether you have selected some (☑) or all (☑) MPE devices to which to deploy the policy or policy group.

5. Click **Deploy.**

A confirmation message displays followed by a list of MPE devices to which the policy or policy group was deployed.

The policy information is saved to each selected MPE device.

Removing a Policy from a Policy Group on an MPE Device

To remove a policy from within a policy group that was deployed to an MPE device, modify the policy group on the CMP system; the policy group is automatically redeployed. (To remove an entire policy group from an MPE device, see [Removing a Policy or Policy Group from an MPE Device](#).)

To remove a policy from a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the desired policy group.
The **Policy Administration** page opens in the work area, listing the policies the group contains.
3. Remove the desired policy using one of the following methods:
 - From the **Policy Library** tree, select the policy. The **Policy Administration** page displays the profile information. Click **Remove**.
 - Click **Modify** and then select the Remove icon located next to the policy you want to remove.

The modified policy group is redeployed, ensuring that the MPE devices are resynchronized with the CMP database.

Note: If the policy group has never been deployed, you can now deploy it to MPE devices (see [Deploying a Policy or Policy Group to MPE Devices](#)).

Removing a Policy or Policy Group from an MPE Device

Removing a deployed policy or policy group from an MPE device is performed from the **Policy Server Administration** page.

To remove a policy or policy group from an MPE device:





1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the MPE device.
The **Policy Server Administration** page opens in the work area, displaying information about the MPE device.
3. Select the **Policies** tab.
4. Click **Modify**.
The **Manage Policies** page opens.
5. Click the **Remove** icon, located to the right of the policy or policy group that you want to remove.
The policy or policy group is removed from the list.
6. Repeat step 5 as required.
7. When you finish, click **Save**.
A confirmation message displays.

The policy or policy group is redeployed to the MPE device, minus the removed policy or policy group.

Changing the Sequence of Deployed Policies or Policy Groups

Changing the sequential order of deployed policies or policy groups is performed directly on an MPE device using the **Policy Server Administration** page.

To change the sequential order of policies or policy groups:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the MPE device.
The **Policy Server Administration** page opens in the work area, displaying information about the MPE device.
3. Select the **Policies** tab.
4. Click **Modify**.
The **Manage Policies** page opens in the work area.
5. Use any of the following options to change the sequential positioning of the policies or policy groups:
 - Use the  (top) and  (bottom) icons, located to the left of policies or policy groups. The  (top) icon moves the item it to the top of the list. The  (bottom) icon moves the item it to the bottom of the list.
 - Drag and drop policies or policy groups to a different position in the sequence.
 - Change the sequence numbers, located to the left of policies or policy groups. Click **Update Order** to refresh the display.
 - Optionally, you can click **Undo** or **Redo** to step back and forth through your changes.

6. Click **Save**.

The policies or policy groups are redeployed to the MPE device in their new sequential order. A confirmation message displays in the work area.

Importing and Exporting Policies, Policy Groups, and Templates

Policies, policy groups, and templates can be exported from the CMP database for inspection or backup purposes. These items are exported as a whole and cannot be exported individually, as every policy, policy group, and policy template in the database is saved to a single file when performing the export function.

For information only, exported policies are marked with policy version numbers as well as the version number of the CMP software under which they were created. This does not affect importation of policies created under different versions of the CMP software.

Importing Policies

To import a policy file into the policy library:

1. From the **Policy Management** section of the navigation pane, select **Policy Import / Export**. The **Import/Export** page opens.
2. Click **Browse** to locate the policy file to import.
3. Select a collision handling option:
 - **Delete all before importing** — All policies, policy groups, and templates currently in the CMP database are deleted first; then the imported versions are saved to the MPE device.
 - **Overwrite with imported version** — All items are imported. If the CMP database currently contains any policies, policy groups, or templates using the same names as the ones being imported, they are overwritten with the imported versions.
 - **Reject any that already exist** — All items are imported except for imported versions with the same name as any policy, policy group, or template currently in the CMP database.
 - **Any collisions prevent all importing** (default) — No items are imported if any of the imported versions has the same name as any policy, policy group, or template currently in the CMP database.
4. Click **Import**.

The policies are imported.

If you try to import an invalid file you receive a validation error similar to the following: You must correct the following errors before proceeding: There is a problem with the import file. The name is required, the file must be present, and the file must be in the correct format.

Exporting Policies

To export the policies or policy templates that reside in the policy library:

1. From the **Policy Management** section of the navigation pane, select **Policy Import / Export**.

The **Import/Export** page opens.

2. Select the type of export: **Policies** (default) or **Templates**.
3. Select the policy group to export: **All** (default) or a named group.
4. Click **Export** to export the policy group in XML format, or **Text** to export the policy group in descriptive format. Policies exported in text format cannot be imported.
A standard **File Download** window opens.
5. Click **Save**.
A standard **Save As** window opens.
6. Assign a name to the policy file. The default is **PolicyExport.xml**.
7. Use the browse function to map the location, and click **Save**.
When the policies are successfully exported, a standard Download Complete window opens.
8. Select **Close** to exit the **Download Complete** window.

The policies or templates are exported to a file.

Managing Subscribers

Topics:

- *Creating a Tier.....145*
- *Displaying Subscriber Activity History.....145*
- *Displaying Real-time Subscriber Statistics.....146*
- *Deleting a Tier.....147*
- *Creating an Account.....147*
- *Modifying an Account.....148*
- *Updating Accounts.....148*
- *Deleting an Account.....149*
- *Static IP Addresses.....149*
- *Provisioning Static IP Addresses Using XML.151*

This chapter describes how to create and manage subscriber tiers and accounts within the CMP system.

Creating a Tier

Tiers are categories that you can define and then apply to groups of subscribers. For example, you can create a series of tiers with different bandwidth limits. Once you define tiers, you can use them in policy rules.

To create a subscriber tier:

1. From the **Subscriber** section of the navigation pane, select **Tiers**.
The content tree displays the **Tiers** folder.
2. Select the **Tiers** folder.
The **Tier Administration** page opens.
3. Click **Create Tier**.
The **New Tier** page opens.
4. Enter information as follows:
 - a) **Name** (required) — Name of the tier.
The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
 - b) **Description/Location** — Free-form text.
Enter up to 250 characters.
 - c) **Downstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the downstream direction in bits per second.
You can enter a value followed by M or G; for example, 4G for 4 gigabits per second.
 - d) **Upstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the upstream direction in bits per second.
You can enter a value followed by M or G; for example, 10M for 10 megabits per second.
5. When you finish, click **Save**.
The tier is added to the CMP database.

You can now use the tier in policy rules.

Displaying Subscriber Activity History

To display subscriber account activity:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.
The content tree displays the Subscriber Account page.
2. On the Subscriber Account page, type in search terms in one or both of the **Search** fields:
 - **Account ID** — You can use as wildcard characters an asterisk (*) to represent any string or a question mark (?) to represent any single character. Searches are case insensitive. The search string must represent the entire account ID; for example, if the account ID is "Account50619," you can find it using the search strings "**Account***" or "***50619**" or "**Account506??**," but not using the search strings "**Account**" or "**506**" or "**619**."

Note: Using wildcard characters can result in longer search times.

- **Static IP Address** — An IP address in the form *n.n.n.n*. You can use as wildcard characters an asterisk (*) to represent any string or a question mark (?) to represent any single character. Searches are case insensitive.

3. Click **Search**.

The Subscriber Account Search page opens. The **Status** column describes the state of synchronization between each account and the MPE devices with which it is associated. The status values are as follows:

- **up-to-date** — The account information is current on the MPE devices with which it is associated.
- **Update Pending** — The account is either new, not yet associated with any MPE device, or has been changed, but the changes have not been sent to any MPE device.
- **Delete Pending** — The account is marked for deletion, but has not yet been removed from the MPE devices.

4. Click on an account ID.

The Subscriber Account page opens. From this page you can do the following:

- To modify account information, click **Modify**. (See [Modifying an Account](#).)
- To delete the account, click **Delete**. (See [Deleting an Account](#).)
- To display the static IP address of the account, click the Static IP Address tab; the Static IP Address page opens. From this page you can modify or delete the static IP address of this account. (See [Static IP Addresses](#).)
- To display real-time statistics for the account, click the Real-time Statistic tab; the Real-Time Statistics page opens. To refresh the data on this page, click **Refresh**. (See [Displaying Real-time Subscriber Statistics](#).)

5. When you finish, click **Back to Search Results**.

The previous page is displayed.

Displaying Real-time Subscriber Statistics

Dynamic statistical information for a subscriber account appears on the Real-time Statistic tab of the Subscriber Account page. The following information is displayed:


- **Policy Server** — the MPE device associated with the subscriber
- **Current IP Address** — the IP address associated with the subscriber (if applicable)
- **Total Bandwidth Allocated** — the total bandwidth, in Kbps, of all VoD sessions associated with the subscriber
- **Total VOD Session Count** — the number of VoD sessions associated with the subscriber

To refresh the display, click **Refresh**. The MPE device is queried.

To export data in XML format, click **Export**; the browser file download window opens. The data is exported in the same format used by the OSSI XML interface. (For format information, see the [OSSI XML Interface Definitions Reference](#).)

Deleting a Tier

To delete a tier:

1. From the **Subscriber** section of the navigation pane, select **Tiers**.
The **Tiers** folder appears in the content tree.
2. Delete the tier using one of the following methods:
 - From the work area, click  (trash can icon), located to the right of the tier.
 - From the content tree, select the tier and click **Delete**.

A confirmation message displays.

3. Click **OK**.

You have deleted the tier.

Creating an Account

Subscriber accounts are usually created external to the CMP system. However, you can create or delete an individual subscriber account.

To create a subscriber account:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.
The **Subscriber Account** page opens.
2. Click **Create Account**.
The **New Account** page opens.
3. Enter information as follows:
 - a) **Account ID** (required) — Name of the account.
 - b) **Subscriber Data** — Additional data associated with the account, such as the specific router interface.
Enter up to 250 characters.
 - c) **Network Element** (required) — The network element associated with this subscriber.
 - d) **Subscriber Group** — If during a VoD reserve request the subscriber's account record contains a reference to an existing subscriber group network element, the network element is dynamically added to the path that the VoD request used. This charges all of the VoD session's resources against all network elements in the defined path as well as the associated subscriber group.
 - e) **Downstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the downstream direction in bits per second.
You can enter a value followed by M or G; for example, 4G for 4 gigabits per second. Leave blank to use the tier value.
 - f) **Upstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the upstream direction in bits per second.
You can enter a value followed by M or G; for example, 10M for 10 megabits per second. Leave blank to use the tier value.

g) **Tier** — The tier associated with this account.

4. Click **Save**.

The account is added to the CMP database.

Modifying an Account

To modify an account:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.
The **Subscriber Account** page opens.
2. Use the search function to locate and display an account (see [Displaying Subscriber Activity History](#)).
The account is displayed.
3. Click on the account.
The **Subscriber Account** page displays information about that account.
4. Click **Modify**.
The **Modify Account** page opens.
5. Make changes as required.
(See [Creating an Account](#) for information on the fields on this page.)
6. Click **Save**.

The account information is modified, and the change is deployed to all associated MPE devices.

Note: If an associated MPE device is offline or unreachable, the subscriber account information is not deployed. See [Updating Accounts](#) for information on updating accounts.

Updating Accounts

Subscriber account information can be imported to, created on, or modified on a CMP system, but the information may not immediately be associated with an MPE device. For example, MPE devices can be offline when subscriber accounts are being deployed. This leaves accounts in a state where their new information is pending update, and the changes must be deployed (or pushed) to MPE devices. You can use the CMP system to deploy subscriber account information.

The update status of accounts is displayed in on the Subscriber Account Search page. A status of Update Pending indicates that an account update is pending.

To update all pending accounts:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.
The **Subscriber Account** page opens.
2. Click **Push Pending Accounts to MPE**.
All pending subscriber data updates are deployed to all MPE devices controlled by this CMP system. If the operation takes more than five seconds, a progress bar appears.

If a hardware failure or other such event results in a new MPE device coming online to replace an older one, then the topology and subscriber data need to be reapplied to the new system. The **Reapply Configuration** button, on the System tab of the Policy Server Administration page, redistributes

topology information to the new MPE device. The **Reapply Subscriber Configuration** button, on the same page, redistributes subscriber account information. This function completely deploys all associated accounts (not just pending changes) to an MPE device, and provides a way to resynchronize the CMP and MPE device subscriber databases.

To update all subscriber account information:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.

The content tree displays a list of policy server groups; the initial group is **ALL**.

2. From the content tree, select the MPE device to update.

The Policy Server Administration page opens in the work area.

3. On the System tab, click **Reapply Subscriber Configuration**.

All subscriber data is deployed to the MPE device, and an entry is written to the audit log. If the operation takes more than five seconds, a progress bar appears.

Deleting an Account

To delete an account:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.

The **Subscriber Account** page opens.

2. Use the search function to locate and display an account (see [Displaying Subscriber Activity History](#)).

The account is displayed.

3. Click **Delete**.

A confirmation message appears.

4. Click **OK**.

The account is deleted.

Static IP Addresses

The Policy Management product supports static IP addresses in the subscriber account definitions that are defined on (or provisioned to) the CMP system, and in the session handling function within MPE devices.

The OSSI XML code includes an optional IP address range definition within the subscriber account definition. This definition consists of a single starting IP address and the number of addresses in the range. A single account can have up to 125 static IP addresses.

Once provisioned, these subscriber records are pushed to the responsible MPE device by the CMP system.

The static IP address is manageable through the CMP system. Access to static IP address management is based on user permissions. The following functions are available:

- You can update and modify accounts with an IP address range. Changes are validated to ensure that duplicate static IP address are not created. (There is no provision to validate against a gateway router subnet definition.)
- You can search for accounts by IP address string. This search uses the same wildcards as the account ID search string and can be used either alone or in combination with the current account ID search string to retrieve accounts.
- Static IP objects are included in exported XML. The Static IP XML block is additive and existing Account XML imports/exports are backward compatible with the system.
- Modifications or exportations generate an audit log message for each operation indicating the operation that was performed, the username of the operator performing the action, and the generic status of the operation.

The MPE device maps static IP address fields to account records. Static IP addresses are stored in a separate database table. This separation ensures that static IP addresses are not disturbed during COPS-PR re-synchronization.

If a subscriber account has both static IP and dynamic IP addresses, all addresses are valid for processing VoD session requests. Also, if a subscriber account is configured with a static IP address, and a B-RAS server sends the same address as a dynamic IP address, then the B-RAS dynamic IP address is used.

When an IP address is learned (from the dynamic COPS-PR information flow) that is already defined as a static address (from the subscriber database update), a trace log entry is generated (Error level). This check is also performed at every video session request, and the same event is generated if necessary.

Configuring a Static IP Address

Account information is normally imported from an XML file. However, the CMP system lets you create an account manually. Static IP address information can only be added to an existing account.

To modify the static IP address of a subscriber account:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.
The **Subscriber Account** page opens.
2. Use the search function to locate and display an account (see [Displaying Subscriber Activity History](#)).
The account is displayed.
3. Select an account ID.
The **Subscriber Account** page opens.
4. On the **Static IP Address** tab, click **Modify**.
The **Modify Account** page opens.
5. Enter the following information:
 - **Static IP Address** — An IP address, in the format **n.n.n.n**.
 - **Static IP Count** — The number of addresses in the range. A single account can have up to 125 static IP addresses.
6. Click **Save**.

The account information is modified.

Deleting a Static IP Address from a Subscriber Account

To delete static IP addresses from a subscriber account:

1. From the **Subscriber** section of the navigation pane, select **Accounts**.
The **Subscriber Account** page opens.
2. Use the search function to locate and display an account (see [Displaying Subscriber Activity History](#)).
The account is displayed.
3. Click on an account ID.
The **Subscriber Account** page opens.
4. On the Static IP Address tab, click **Delete**.
A confirmation message appears.
5. Click **Save**.

The static IP addresses are removed from this subscriber account.

Provisioning Static IP Addresses Using XML

You can add, update, or delete static IP addresses through the OSSI XML Interface. The `<AddAccount>` and `<UpdateAccount>` tags include optional Static IP addresses within the subscriber account definition. This definition consists of a single starting IP address and the number of addresses in the range. A maximum of 125 static IP addresses can be associated with a single account.

For example, the following definition specifies an IP address range of 10.0.1.1, 10.0.1.2, 10.0.1.3, ..., 10.0.1.125:

```
<?xml version="1.0" encoding="UTF-8"?>
<XmlInterfaceRequest>
  <AddAccount>
    <Account>
      <AccountId>47/VAXA/261188/ /VZVA</AccountId>
      <SubscriberData>11/3.30251</SubscriberData>
      <NetworkElementName>FRBGVAFB1FW
      </NetworkElementName>
      <StaticIp>
        <IpAddress>10.0.1.1</IpAddress>
        <IpCount>125</IpCount>
      </StaticIp>
      <TierRef>
        <Name>INFOSPEED_F'FTPV_AA</Name>
      </TierRef>
    </Account>
  </AddAccount>
</XmlInterfaceRequest>
```

Only one IP address range is allowed per subscriber. Validation is performed to ensure that duplicate static IP addresses are not provisioned.

Note: There is no validation against the gateway router subnet definition.

The `<QueryAccount>` tag includes XML for static IP objects as part of the response.

To change the address range, use the `<UpdateAccountType>` tag to redefine the range, which replaces the previous definition. Modifying the `<IpCount>` value separately is not supported.

For more information, see the *OSSI XML Interface Definitions Reference Guide*.

Chapter 10

System-Wide Report

Topics:

- [Viewing Active Alarms.....153](#)
- [Viewing the Alarm History Report.....154](#)

This chapter describes the reports available on the function of Policy Management systems in your network. Reports can display platform alarms, network protocol events, and Policy Management application errors.

Viewing Active Alarms

The Active Alarms summary provides an aggregate view of time stamped alarm notifications for Policy Management systems. The display is refreshed every ten seconds and appears in the upper right corner of all CMP pages. Alarms remain active until they are reset.

The Active Alarms report provides details about active alarms. To view the Active Alarms report:

- From the **System Wide Reports** section of the navigation pane, select **Active Alarms**.
- The **Active Alarms** section expands to show the available alarm reports.

Figure 19: Sample Active Alarms Report shows a sample active alarm report.

Server	Server Type	Severity	Alarm ID	Age/Auto Clear	Description	Time	Operation
mpe202 10.60.30.202	MPE	Minor	32509	10h 30m 14s / ---	Server NTP Daemon Not Synchronized	09/12/2013 03:52:37 EDT	
cmp200 10.60.30.200	CMP	Minor	32509	10h 26m 4s / ---	Server NTP Daemon Not Synchronized	09/12/2013 03:56:46 EDT	

Figure 19: Sample Active Alarms Report

The alarm levels are as follows:

- **Critical** — Service is being interrupted. (Critical alarms are displayed in red.)
- **Major** — Service may be interrupted if the issue is not corrected. (Major alarms are displayed in orange.)
- **Minor** — Non-service affecting fault. (Minor alarms are displayed in purple.)

Notifications, which have a severity of Info, are not displayed in the Active Alarms report, but are written to the trace log. For more information, see [Viewing the Trace Log](#).

Note: Alarms generated by Policy Management systems running software lower than release 7.5 are mapped to these levels as follows: Emergency or Critical map to Critical; Alert or Error map to Major; Warning or Notice map to Minor.

The Age/Auto Clear column shows how long an alarm has been active (that is, how long since it was raised) and how long the alarm will display before being automatically cleared. The Auto Clear time is shown as --- (three hyphens) if the alarm is not automatically cleared.

The following options are available:

- To sort the report on any column, click the column title.
- To display online help for an alarm, click its ID.
- To hide an alarm, click the hide icon (), located to the right of each row. All instances of alarms with that ID reported from that server are hidden from display (but shown in the Hidden Filter, which you can use to restore the display of those alarms).

Note: Hiding an alarm only affects the current user. Other users will see the alarm if they display the **Active Alarms** page.

- To manually clear an alarm, click the Clear icon (🗑️), located to the right of each row. You are prompted, *This alarm will be cleared. Are you sure?* Click **OK**.
- To pause the display of alarms, click **Pause**. To resume the display, click **Refresh**.
- To select what information is displayed, click **Columns** and select from the list.
- To control what alarms and alarm classes are displayed on the page, click **Filters** and select from the list:
 - The **Search Filter** tab has three controls. The **Server** control lets you display alarms from all servers (default) or a specific server. The **Server Type** control lets you display alarms from all Policy Management products (default) or just **CMP** or **MPE** systems. The **Severity** control lets you display alarms of all severities (default), critical and major alarms, critical alarms, major alarms, or minor alarms.
 - The **Hidden Filter** tab shows alarms, by server and alarm ID, that are currently hidden from display. Click 🗑️, to the right of an entry, to remove it from the list of hidden items and display it in the page again.
- **Printable Format** — The current alarms are displayed in a separate window.
- **Save as CSV** — A comma-separated value (CSV) file named `report.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **Export PDF** — A Portable Document Format (PDF) file named `report.pdf` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.

Viewing the Alarm History Report

The Alarm History Report displays historical alarm information.

To view the alarm history report:

1. From the **System Wide Reports** section of the navigation pane, select **Alarm History Report**. The Alarm History report opens.

Note: If you are using Internet Explorer, the window appears behind the main window.

The window displays up to 50,000 alarms, sorted by age.

Note: If you wish to view the most recent alarms, and there are more than 50,000 alarms in the database, specify a start date/time that includes the present.

2. To view older alarms, reduce the number of alarms displayed, or locate a specific alarm or group of alarms, you can define filtering criteria using the following fields:
 - **Start Date** — Filter out alerts before a specific date/time. Click the calendar icon to specify a date/time.
 - **End Date** — Filter out alerts after a specific date/time. Click the calendar icon to specify a date/time.
 - **Severity** — Filter alerts by severity level. Select a level from the list. The default is **All**.
 - **Cluster or Server** — Select the cluster or server within the cluster to view the alarms.
 - **Active Alarms** — Select to view only active alarms; the default is to display both active and cleared alarms.


- **Aggregate** — Select to aggregate alarms that have the same IP address, alarm ID, and severity. (This function is limited to 50,000 alarms.)
3. After entering filtering information, click **Filter** to refresh the display with the filtering applied. The alarm list is filtered.
 4. When you finish, click **Close** to close the window.

Alarms contain the following information:

- **Occurrence** — The most recent time this alert was triggered.
- **Severity** — The severity of the alert:
 - **Critical** — Service is being interrupted (displays in red).
 - **Major** — Service may be interrupted if the issue is not corrected (displays in orange).
 - **Minor** — Non-service affecting fault (displays in purple).
 - **Info** — Informational message only.
 - **Clear** — Alarm has been cleared.

Note: Alarms generated by Policy Management systems running software lower than release 7.5 are mapped to these levels as follows: Emergency or Critical map to Critical; Alert or Error map to Major; Warning or Notice map to Minor.

- **Alarm ID** — When clicked, the alarm ID provides online help information.
- **Text** — User-readable text of the alert.
- **OAM VIP** — OAM IP address in IPv4 format.
- **Server** — Name and IP address, in IPv4 format, or FQDN of the device from which this alarm was generated.

To view alert details, click  (binoculars icon), located to the right of the alert. A window displays additional information.

For example:

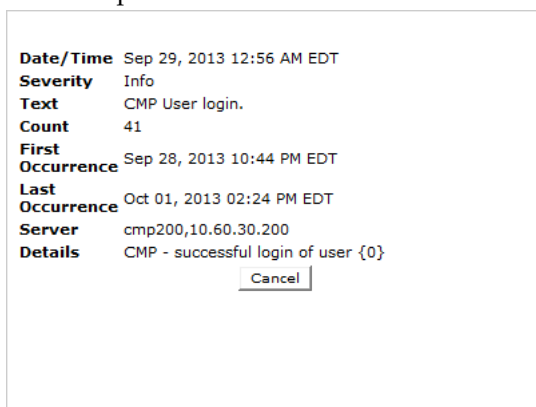


Figure 20: Alert Details

Chapter 11

Upgrade Manager

Topics:

- [About ISO Files on Servers.....157](#)
- [About Performing an Upgrade.....160](#)

The Upgrade Manager allows you to manage upgrade ISOs and perform software upgrades on servers in the topology. During the upgrade process, the System Maintenance page displays the upgrade status. Note that access to these GUI options can be affected by settings on the role setting page.

It is recommended that you contact My Oracle Support before performing an upgrade. See <https://support.oracle.com> for more information.

About ISO Files on Servers

Policy Management software upgrade procedures are distributed and stored for use as ISO files, which are archive files of optical (DVD) discs. ISO files are also called ISOs. You can automatically or manually distribute, or “push,” ISO files to either servers or clusters.

Use the **ISO Maintenance** option to monitor the current upgrade status for all servers on the system, monitor the ISO download process, and perform upgrade-related operations. Operations performed from this page include distributing ISO files to servers, deleting ISO files from servers, and pushing an upgrade script to servers. An audit log is generated for each operation.

ISO Maintenance Elements

On the **Upgrade Manager** menu, **ISO Maintenance** is an option. All servers in the topology appear in the server table on this page. Servers display in groups by cluster; clusters can be collapsed or expanded by clicking the [-] or [+] icons in the first column of the table. Server information is updated every ten seconds.

There are three types of elements that appear on the **ISO Maintenance** GUI page: Checkboxes to select servers on which to perform operations, the table of filtered servers, and pulldown menus (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for performing operations. The following list describes all of these elements.

Table 10: ISO Maintenance Elements

Element	Description
<Checkbox>	Use the checkbox column to check mark the servers on which an operation is to be performed. If you check mark a main cluster server, all servers in that cluster are check marked. Note that at least one server must be check marked before you can select an operation from the Operations pulldown menu.
Name	Displays the server names of all filtered servers. When a server is downloading an ISO file, a special download icon appears next to the name.
Appl Type	Displays the type of application running on each server. The Filters pulldown menu lets you select CMP Site1 Cluster , MPE , or All servers.
IP	Displays the OAM server IP address of each server. The Filters pulldown menu lets you select only a server with a specific IP address or All servers.
Running Release	Displays the current Policy Management software release of each server. The Filters pulldown menu lets you display a specific release only or All releases.
ISO	Displays the ISOs or CD-ROM on each server. Use the checkbox to select the ISO to delete during the Delete ISO operation.
Columns	Use the Columns pulldown menu to change the columns that appear in this table. By default, all columns appear. To change which columns appear,

Element	Description
	uncheck the columns to be removed from the page. The Name column is mandatory.
Filters	Use the Filters pulldown menu to select a subset of servers to appear on this page. On this menu are the following pulldown filter submenus: Appl Type , IP , and Running Release . These filters are set to All by default, so all servers appear initially. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	<p>Use the Operations pulldown menu to select an ISO operation to perform.</p> <p>Note: The servers on which the operation is being performed must be check marked (in the first column of the table) before that or any operation can be selected. The operations that appear in the pulldown menu depend on the state of the servers that are selected; that is, when more than one server is selected, only the operations that are available on all of these servers appear.</p> <p>Possible operations are Push Script, Upload ISO, and Delete ISO. As a protective feature, when a command is executed, a warning message pops up, asking if you are sure you want to execute this operation (click OK or Cancel). When OK is clicked, a progress bar displays the status of the command completion in a pop-up window. Note that once the operation is confirmed, it cannot be cancelled.</p>

Viewing the ISO Status of Servers

Use this procedure to view the status of in-service servers before, during, and after a software upgrade.

1. From the **Upgrade Manager** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page appears.
2. (Optional) Click **Filters** and specify the criteria to customize the list of servers that display in the table.
3. (Optional) Click **Columns** and select columns to customize the table.

All in-service servers that meet the filter criteria are listed. Server information is updated every ten seconds.

Pushing a Script to a Server

Use this procedure to push the upgrade script to the remote servers receiving the software upgrade. This step is required before a software upgrade can occur on a server. An error message displays in the Upgrade Status column until Push Script has been run.

1. From the **Upgrade Manager** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page appears.
2. Select the server(s) receiving the upgrade script.
3. Click on the **Operations** menu and select **Push Script**.
A confirmation message appears.
4. Click **OK**.

A progress bar displays the progress of the operation.
The upgrade script is downloaded to the selected servers.

Adding an ISO File to a Server

Use this procedure to download an upgrade ISO file to a remote server in preparation for a software upgrade.

1. From the **Upgrade Manager** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page appears.
2. Select the server(s) to receive the ISO file.
3. Click the **Operations** menu and select **Upload ISO**.
An **Upload/Add ISO** window appears.
4. Enter the ISO Server Hostname or IP address, User, Password, and ISO file full path for the ISO file being added.

Option	Description
Mode	Mode used to transfer file to remote servers. Currently, SCP is available.
ISO Server Hostname/IP	Enter the name or address of the server receiving the ISO file. This field is required.
User	Enter your user name. This field is required.
Password	Enter your password. This field is required.
ISO file full path	Enter the location where the ISO file is to be stored on the remote server. This field is required.

5. Click **Add**.
The transfer process begins to the selected servers. A download icon appears in the Name column for the servers receiving the ISO file during the file transfer process. A progress bar displays during the operation. Once the process completes, the icon disappears.

The ISO file is distributed to the servers.

Deleting an ISO File from a Server

Use this procedure to delete an ISO file from a remote server.

1. From the **Upgrade Manager** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page appears.
2. Select the servers from which the ISO file is being removed.
3. Select the ISO file on the server that is being removed.
4. Click the **Operations** menu and select **Delete ISO**.
A confirmation message appears.
5. Click **OK**.
A progress bar displays the progress of this operation.

The selected ISO files are deleted from the selected remote servers.

About Performing an Upgrade

The information in this section is a general overview of what happens during the upgrade process. Steps for performing an upgrade are provided by the Oracle [My Oracle Support \(MOS\)](#).



Caution: Use only the upgrade procedure provided by the Oracle Customer Care Center. Before upgrading any system, please go to the Oracle Customer Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade. Once you begin an upgrade, any changes to the configuration (such as creating or editing network elements or policies) may be lost.



Warning: It is recommended that you contact the Oracle Customer Care Center and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

A server must display **Forced Standby** in the Server State column on the **System Maintenance** page before a software upgrade can be performed on that server.

About Preparing for an Upgrade

Upgrading a server requires a large amount of preparation. Detailed information about preparing for an upgrade is available at the My Oracle Support website.



Caution: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, go to the My Oracle Support website and review any relevant Technical Service Bulletins (TSBs). Use only the upgrade procedure provided by My Oracle Support.

System Maintenance Elements


On the **Upgrade Manager** menu, **System Maintenance** is an option. All servers in the topology appear in the server table on this page. Servers display in groups by cluster; clusters can be collapsed or expanded by clicking the [-] or [+] icons in the first column of the table. Server information is updated every ten seconds.

There are three types of elements that appear on the **Upgrade Manager** GUI page: Checkboxes to select servers/ISOs on which to perform operations, the table of filtered servers, and menus (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for performing operations. The following list describes all of these elements.

Table 11: System Maintenance Elements

Element	Description
<Checkbox>	Use the checkbox column to check mark the servers on which an operation is to be performed. If you check mark a main cluster server, all servers in that cluster are check marked. Note that at least one server must be check marked before you can select an operation from the Operations menu.

Element	Description
Name	Displays the server name of each server. When a server is in the process of being upgraded, a special upgrade icon appears next to the name. Likewise, if a server upgrade has failed, a special failed icon appears next to the name.
Appl Type	Displays the type of application running on each server. The Filters menu lets you select CMP Site1 Cluster , MPE , or All servers.
IP	Displays the IP address of each server. The Filters menu displays only the server with a specific IP address or All servers.
Server State	Displays the state of each server. The server state can appear in different colors, depending on the state displayed. The Filters menu displays Active , Standby , Out-Of-Service , Force Standby , or All servers.
ISO	Displays the ISOs or CD-ROMs on each server. Use the checkbox to select an ISO to use during an upgrade on that server.
Prev Release	Displays the previous Policy software release of each server, if known. The Filters menu displays a specific release only or All releases.
Running Release	Displays the current Policy Management software release of each server. The Filters menu displays a specific release only or All releases.
Replication Status	Displays On or Off.
Upgrade Status	Displays details of last upgrade performed on each server.
Columns	Use the Columns menu to change the columns that appear on this page. By default, all columns appear. To change which columns appear, uncheck the columns to be removed from the page. The Name column is mandatory.
Filters	Use the Filters menu to select a subset of servers to appear on this page. On this menu are the following filter submenus: Appl Type , IP , State , Prev Release , and Running Release . These filters are set to All by default, so initially all servers appear. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	Use the Operations menu to select an upgrade operation to perform. Note: The servers on which the operation is being performed must be selected (in the first column of the table) before that or any operation can be selected. The operations that appear in the menu depend on the state of the servers that are selected; that is, when more than one server is selected, only the operations that are available on all of these servers appear. As a protective feature, when a command is executed, a warning message pops up, asking if you are sure you want to execute this operation (you can click OK). If you click OK , a progress bar displays the status of the command completion in a pop-up window. Once an operation is confirmed, it cannot be cancelled.
Push Script	Pushes script to remote server. Upgrade Manager uses the script to communicate with the remote server and to perform the upgrade or backout.
Upload ISO	Adds ISO to the specified Policy Management products (CMP/MPE).

Element	Description
Force Standby	<p>Forces server to standby status. A server must be in Forced Standby status before you can complete an upgrade.</p>  <p>CAUTION Setting Force Standby for all servers in a cluster effectively removes the cluster from service.</p> <p>Note: You cannot force both servers of a CMP cluster into standby status.</p>
Turn Off Replication	Turns off replication.
Prepare Upgrade	Turns off COMCOL replication of database tables.
Switch ForceStandby	Switches the upgraded server to Active and the previously active server to Forced Standby to upgrade it.
Accept Upgrade	Completes the upgrade process. This operation is available for servers in the Pending state. A server must be in Forced Standby status before an upgrade can be completed. Once this operation is performed, the upgrade cannot be backed out.
Reject Upgrade	Backs out of the upgrade process. This operation is available for servers in the Pending state. A server must be in Forced Standby status before an upgrade can be rejected.

Viewing Upgrade Status of Servers

Use this procedure to view the status of in-service servers before, during, and after a software upgrade.

1. From the **Upgrade Manager** section of the navigation pane, select **System Maintenance**.
The **System Maintenance** page appears.
2. (Optional) Click **Filters** and specify the information to customize the list of servers that display in the table.
3. (Optional) Click **Columns** to select columns display in the table.

All in-service servers that meet the filter criteria are listed. Server information is updated every ten seconds.

Changing maxMsgSize Configuration After Upgrading from 10.4 to 10.4.x

Use this procedure to ensure that the value of DIAMETER.MaxMsgSize is set to 64K after upgrading Policy Management from version 10.4 to version 10.4.x.

To change the maxMsgSize configuration after upgrading from 10.4 to 10.4.x:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the MPE device.
The **Policy Server Administration** page opens in the work area, displaying information about the MPE device.

3. Select the **Policy Server** tab.
The Policy Server configuration settings are displayed.
4. Click **Advanced**.
The **Advanced Configuration Settings** page appears.
5. Click **Add**.
The **Add Configuration Key Value** dialog box appears.
6. In the **Configuration Key** field, enter DIAMETER.MaxMsgSize.
7. In the **Value** field, enter 65536.
8. Click **Save**.
9. Click **Save**.
The message The configuration was applied successfully. appears if the configuration was successful.

The value of DIAMETER.MaxMsgSize is configured to the 10.4.x default value of 64k.

Chapter 12

System Administration

Topics:

- *Configuring System Settings.....165*
- *Importing and Exporting Configurable Objects.....167*
- *The Manager Report.....170*
- *The Trace Log.....170*
- *Viewing the Audit Log.....172*
- *Managing Scheduled Tasks.....175*
- *Configuring a Task.....175*
- *About Managing Users.....177*
- *Changing a Password.....184*

This chapter describes functions reserved for CMP system administrators.

Note: Some options are visible only when you are logged in with administrative rights to the CMP system. However, the **Change Password** option is available to all users.

Configuring System Settings

Within the CMP system you can define the settings that control system behavior.

To define system settings:

1. From the **System Administration** section of the navigation pane, select **System Settings**.
The **System Settings** page opens in the work area, displaying the current system settings.
2. Click **Modify**.
The **System Settings** page opens.
3. In the **Configuration** section, define the following:
 - a) **Idle Timeout (minutes; 0=never)** — The interval of time, in minutes, that a session is kept alive.
The default value is 30 minutes; a value of zero indicates the session remains active indefinitely.
 - b) **Account Inactivity Lockout (days; 0=never)** — The maximum number of days since the last successful login after which a user is locked out.
If the user fails to log in for the defined number of days, the user is locked out and cannot gain access to the system until an administrator resets the account. The default value is 21 days; a value of zero indicates no limit (the user is never locked out for inactivity).
 - c) **Maximum Concurrent Sessions Per User Account (0=unlimited)** — The maximum number of times a defined user can be logged in simultaneously. A value of zero indicates no limit.
If more than the configured number of concurrent users try to log in (for example, a second user if this value is set to 1), they are blocked at the login page with the message *Your account already has the maximum number of concurrent sessions.*
 - d) **Password Expiration Period (days; 0=never)** — The number of days a password can be used before it expires. Enter a value from 7 to 365, or 0 to indicate that the password never expires.
 - e) **Password Expiration Warning Period (days; default=3)** — The number of days before a password expires to begin displaying a window to users after login warning that their password is expiring.
 - f) **Admin User Password Expiration** — By default, the password for the admin user never expires.
If you select this option, the **admin** user is subject to the same password expiration policies as other users.
 - g) **Block users when password expires** — By default, once a password expires, the user must immediately change it at the next login.
If you select this option, if their password expires, users cannot log in at all. (If you select **Admin User Password Expiration** and the **admin** user's password expires, the user can still log in but must immediately select a new password.)
 - h) **Minimum Password Length** — The minimum allowable length in characters for a password, from 6 to 64 characters.
The default is six characters.
 - i) **Login Banner Title** — The title that displays at the top of the login page. The default is **welcome**.
You can enter up to ten characters.
 - j) **Login Banner Text** — The text that displays on the login page. You can enter up to 10,000 characters.
 - k) **Top Banner Text** — The text that displays in the banner at the top of the GUI page. By default, the text displayed is "Policy Management: *hostname*" (where *hostname* is the name of the system).

If you enter text in this field, it will overwrite this default. You can enter up to 50 characters. You can select the font, size, and color of the text.

4. In the **Invalid Login Threshold** settings section, define the following:
 - a) **Enable** — Enables login threshold control.
By default, this feature is enabled; clear the check box to disable this feature.
 - b) **Invalid Login Threshold Value** — Defines the maximum number of consecutive failed logins after which action is taken.
Enter a value from 1 through 500; the default is 3 attempts.
 - c) **Actions upon Crossing Threshold** — The system action to take if a user reaches the invalid login threshold:
 - **Lock user** — prevents users from logging in if they reach the invalid login threshold.
 - **Send trace log message** — If a user account reaches the threshold, an incident is written to the trace log, including the username and the IP address (in IPv4 format) from which the login attempts were made. The default level is **Warning**; to change the event level, select a different level from the list.

5. The **Password Strength Settings** section lists four character categories: lowercase letters, uppercase letters, numerals, and non-alphabetic characters. You can specify a password strength policy that requires users to create passwords by drawing from these categories:
 - **Require at least categories below** — By default, this setting is 0 (disabled). Select it to require users to include password characters from between one to four of the categories.
 - **Require at least lower-case letters (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 lowercase letters in their passwords.
 - **Require at least upper-case letters (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 uppercase letters in their passwords.
 - **Require at least numerals (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 numerals in their passwords.
 - **Require at least non-alphabetic characters (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 nonalphabetic characters in their passwords.
 - **Force users with weak password to change password at their next login** — By default, this setting is 0 (disabled). Select it to require users to conform to a new password policy effective the next time they log in.

6. Click **Save**.

The system settings are configured.

Figure 21: Sample Password Strength Policy shows an example of settings that establish a password strength policy requiring user passwords to contain at least one uppercase letter, four numerals, and one non-alphabetic character. (A password that would satisfy this policy is P@ssword1357.) Users whose passwords do not meet these requirements will be forced to change their passwords the next time they log in.

Password Strength Settings

Lower-case letter

Upper-case letter

Numeral

Non-alphanumeric character

Require at least categories of the above

Require at least lower-case letter(s) (1-64)

Require at least upper-case letter(s) (1-64)

Require at least numeral(s) (1-64)

Require at least non-alphanumeric character(s) (1-64)

Force users with weak password to change password at their next login

Figure 21: Sample Password Strength Policy

Importing and Exporting Configurable Objects

In addition to defining manageable objects manually, you can add them to the CMP database using the OSSI XML Interface or by importing them from an XML file. You can also export a list of objects of various types to an XML output file. This section describes the OSSI XML interface and the XML bulk import and export processes.

This section describes how to perform a simple or a bulk export of configurable objects and how to import object configurations into the CMP system.

Using the OSSI XML Interface

The OSSI XML interface provides access to raw data in the system directly via HTTP. The system data is entered and returned as XML documents in accordance with a defined schema. The schema for the input XML is provided to specify exactly which attributes of a manageable object are permitted on import, as well as the formatting for those attributes.

You can also define object groups as part of the XML file and import them within the same file. Groups let you define a logical organization of objects within the CMP database at the time of import. Group structures include not only group attributes, but also relationships between groups, subgroups, and objects.

The OSSI XML interface includes the following:

- **Topology Interface** — Allows you to query and manage network elements within the system
- **Operational Measurements (OM) Interface** — Allows you to retrieve statistical data from the system

For detailed information, see the document *OSSI XML Interface Definitions Reference Guide*.

Importing an XML File to Input Objects

During the import process, object definitions are read one at a time from the user-specified XML file. Each object is then validated and checked against the existing database for collisions (duplications). Collisions are detected based on the object name, which is a unique database key. If the object already exists within the system, the existing object's attributes are updated (overwritten) by the attributes specified in the XML file being imported. If the object does not exist within the system, the object is created and imported as a new object. A blank element value is replaced with a default or null value, as appropriate.

An XML import is limited to 20,000,000 bytes. If you try to import a file larger than that the import will fail with a result code of 102 (input stream error).

Note: Export the existing database of objects before starting an import operation to ensure that you can recreate the previous state if necessary (see).

To use an XML file to input defined objects:

1. From the **System Administration** section of the navigation pane, select **Import/Export**.

The Import/Export page opens in the work area.

Note: Do not select **Policy Import/Export**, in the **Policy Management** section; that is a different function.

2. On the Import/Export page, enter the file name of the XML import file, or click **Browse** and, from the standard file open window that appears, locate it.
3. Select the type of import: * (specifies import all types), **Network Elements**, **Paths**, **Accounts**, **Tiers**, **Applications**, **Roles**, **Scopes**, or **Users**. * is the default value.

If you select **Network Elements**, additional filtering fields appear to help you manage the volume of data being imported; you can filter by network element name, element ID, or Diameter identifier. If you select **Accounts**, an additional filtering field appears to help you manage the volume of data being imported; you can filter by account ID. Each additional field accepts a string that can include the wildcard characters * (to represent any string) and ? (to represent any character). By default, all elements matching the filter are included. For each field you can select the operators **AND**, **OR**, **AND NOT**, or **OR NOT**; if you select an operator, an additional statement field appears. You can specify up to six logical combinations of filtering statements.

Note: The concatenation of all filters is left associative. For example, C1 AND C2 OR C3 equals (C1 AND C2) OR C3. The NOT operator affects the succeeding statement(s); for example, C1 AND NOT C2 AND C3 equals C1 AND (NOT C2) AND C3.

4. Click **Import**.

Data from the XML file is imported. If the operation takes more than five seconds, a progress bar appears.

Following the import, status messages provide the total counts of all successful imports, updates, and failures. Click **Details** (the button is below the status messages) to open a window containing detailed warnings and errors for each object. The error messages contain identifying information for the XML structure that caused the error, allowing you to pinpoint and fix problems in the XML file.

For each User element, ensure that Role and Scope data is also defined. The recommended sequence of elements in the XML import file is Network Element, Role, Scope, and then User.

If an imported user password does not satisfy the current password rules, the user will have to change passwords on first login. Password expiration timestamps are imported, so the passwords will expire on the schedule of the CMP system from which they were exported.

Exporting an XML File

The Export feature creates an XML file containing definitions for objects within the CMP database, in the same schema used on import. You can back up data by exporting it to an XML file, and restore it by importing the same file. The export file can also be transferred to a third-party system. To export an XML file:

1. From the **System Administration** section of the navigation pane, select **Import/Export**. The **Import/Export** page opens in the work area.

Note: Do not select **Policy Import/Export**, in the **Policy Management** section; that is a different function.

2. Select the type of export:
 - **Network Elements** (default)
 - **Paths**
 - **Accounts**
 - **Tiers**
 - **Applications**
 - **Roles**
 - **Scopes**
 - **Users**

If you select **Network Elements**, additional filtering fields appear to help you manage the volume of data being exported; you can filter by network element name, element ID, or Diameter identifier. If you select **Accounts**, additional filtering fields appear to help you manage the volume of data being exported; you can filter by account ID, network element name, or MPE device. Each additional field accepts a string that can include the wildcard characters * (to represent any string) and ? (to represent any character). By default, all elements matching the filter are included. For each field you can select the following operators:

- **AND**
- **OR**
- **AND NOT**
- **OR NOT**

If you select an operator, an additional statement field appears. You can specify up to six logical combinations of filtering statements.

Note: The concatenation of all filters is left associative. For example, C1 AND C2 OR C3 equals (C1 AND C2) OR C3. The NOT operator affects the succeeding statement(s); for example, C1 AND NOT C2 AND C3 equals C1 AND (NOT C2) AND C3.

3. Click **Export**.
A standard file download window opens, and you are prompted to open or save the file.
4. Click **Save** to save the file.
Data exported to an XML file. If the operation takes more than five seconds, a progress bar appears.


User passwords are exported in encrypted text. Password expiration timestamps are retained, so the passwords will expire on the schedule of the CMP system from which they were exported.

The Manager Report

The Manager Report provides information about the CMP cluster itself. This information is similar to the Cluster Information Report for clusters. The display is refreshed every ten seconds.

To view the Manager Report, select **Reports** from the **System Administration** section of the navigation pane.

The following information is displayed in the Manager Report:

- **Cluster Name and Designation** — The name of the cluster, whether it is the primary (**P**) or secondary (**S**) site, and its mode:
 - **Active:** The cluster is currently managing the Policy Management network.
 - **Standby:** The cluster is not currently managing the Policy Management network.
- **Cluster Type and Status** — A CMP system displays **Manager**. The possible values of the cluster status are the following:
 - **On-line:** If one server, it is active; if two servers, one is active and one is standby.
 - **Degraded** (two servers only): One server is active, but at least one other server is not available.
 - **Offline:** No server is active.
 - **Inconsistent** (two servers only): Both servers are active. This is a “split brain” error condition, and can only happen when the backplane link fails.
- **Blades** — The status of the servers (blades) contained within the cluster. A symbol () indicates which server currently has the external connection (that is, which blade is the active server). The report also lists the following server-specific information:
 - **Overall:** Displays the current topology state (Active, Standby, or Out-Of-Service), number of server (blade) failures, and total uptime (time providing active or standby policy or GUI service). For the definitions of these states, see [Server Status](#).
 - **Utilization:** Displays the percentage utilization of disk (of the /var/camiant filesystem), average value for the CPU utilization, and memory.

The **Actions** buttons let you restart the CMP software on a server or restart (reboot) the server itself.

To pause refreshing the display, click **Pause**. To resume refreshing, click **Resume**. To reset the display counters, click **Reset All Counters**.

The Trace Log

The trace log is part of system administration records notifications for management activity on the CMP system. For information on configuring the cluster-level messages written to the trace log, see [Configuring Log Settings](#).

Viewing the Trace Log

To view log information using the Trace Log Viewer:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
The **Trace Log** page opens in the work area.
2. Click **View Trace Log**.

The **Trace Log Viewer** window opens. While data is being retrieved, the progress message *Scanning Trace Logs* appears.

All events contain the following information:

- **Date/Time** — Event timestamp. This time is relative to the server time.
- **Code** — The event code. For information about event codes and messages, see the *Troubleshooting Reference*.
- **Severity** — Severity level of the event. Application-level trace log entries are not logged at a higher level than Error.
- **Message** — The message associated with the event. If additional information is available, the event entry shows as a link. Click on the link to see additional detail in the frame below.

By default, the window displays 25 events per page. You can change this to 50, 75, or 100 events per page by selecting a value from the **Display results per page** list.

Events that occur after the Trace Log Viewer starts are not visible until you refresh the display. To refresh the display, click one of the following buttons:

- **Show Most Recent** — Applies filter settings and refreshes the display. This displays the most recent log entries that fit the filtering criteria.
- **Next/Prev** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.
- **First/Last** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.

3. When you finish, click **Close**.

Modifying the Trace Log Configuration

To configure the trace log display:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
The Trace Log page opens in the work area, displaying the current trace log configuration.
2. Click **Modify**.
The Modify Trace Log Settings page opens.
3. Define the settings.
For a description of the settings, see [Configuring Log Settings](#).
4. Click **Save**.

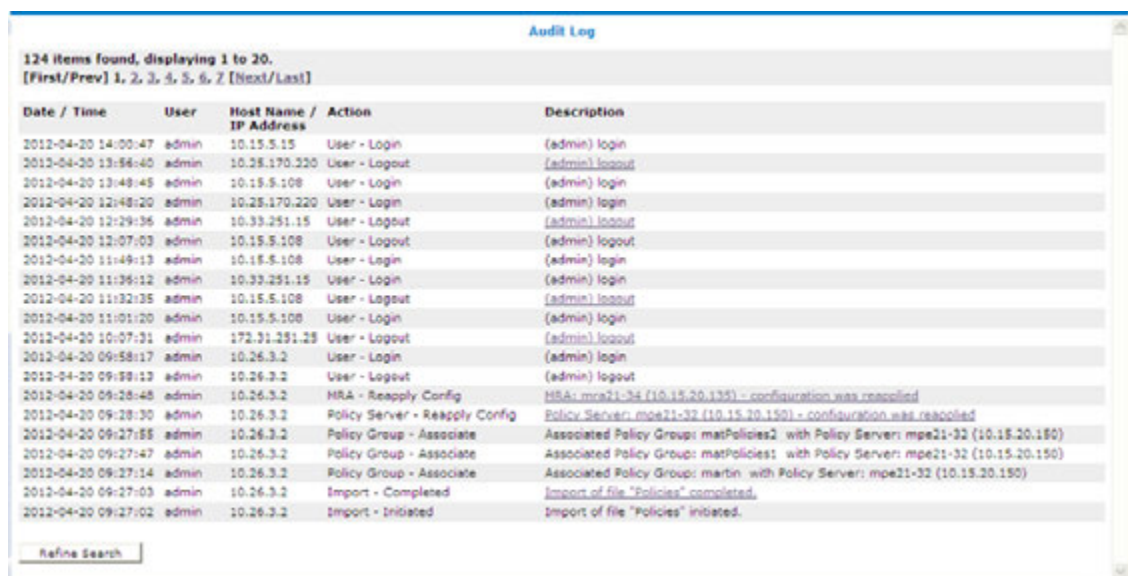
The trace log configuration is modified.

Viewing the Audit Log

You can track and view configuration changes within the CMP system. Using the audit log, you can track and monitor each configuration event, providing you better system control. The audit log is stored in the database, so it is backed up and can be restored.

To display the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**. The **Audit Log** page opens in the work area.
2. On the **Audit Log** page, click **Show All**. The Audit Log opens. (*Figure 22: Audit Log* shows an example.)



The screenshot shows the 'Audit Log' interface with a table of 124 items. The table has columns for Date / Time, User, Host Name / IP Address, Action, and Description. The first few rows show login and logout events for the 'admin' user. Later rows show configuration changes for HRA and Policy Servers, and the completion of a file import.

Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 14:00:47	admin	10.15.5.15	User - Login	(admin) login
2012-04-20 13:56:40	admin	10.25.170.220	User - Logout	(admin) logout
2012-04-20 13:49:45	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 12:49:20	admin	10.25.170.220	User - Login	(admin) login
2012-04-20 12:29:36	admin	10.33.251.15	User - Logout	(admin) logout
2012-04-20 12:07:03	admin	10.15.5.108	User - Logout	(admin) logout
2012-04-20 11:49:13	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 11:36:12	admin	10.33.251.15	User - Login	(admin) login
2012-04-20 11:32:35	admin	10.15.5.108	User - Logout	(admin) logout
2012-04-20 11:01:20	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 10:07:31	admin	172.31.251.28	User - Logout	(admin) logout
2012-04-20 09:58:17	admin	10.26.3.2	User - Login	(admin) login
2012-04-20 09:58:13	admin	10.26.3.2	User - Logout	(admin) logout
2012-04-20 09:28:48	admin	10.26.3.2	HRA - Reapply Config	HRA: mra21-34 (10.15.20.135) - configuration was reappplied
2012-04-20 09:28:30	admin	10.26.3.2	Policy Server - Reapply Config	Policy Server: mpe21-32 (10.15.20.150) - configuration was reappplied
2012-04-20 09:27:55	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: matPolicies2 with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:47	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: matPolicies1 with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:14	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: marbin with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:03	admin	10.26.3.2	Import - Completed	Import of file "Policies" completed.
2012-04-20 09:27:02	admin	10.26.3.2	Import - Initiated	Import of file "Policies" initiated.

Figure 22: Audit Log

For a detailed description of an item, click the underlined description. The details of the event display. (*Figure 23: Audit Log Details* shows an example.)

To filter search results, click **Refine Search**, located at the bottom of the page. (See *Searching for Audit Log Entries*.)

Audit Log				
124 Items found, displaying 21 to 40.				
[First/Prev] 1, 2, 3, 4, 5, 6, 7 [Next/Last]				
Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 09:26:39	admin	10.26.3.2	Import - Completed	Import of file "PolicyTableDataExport.xml" completed.
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Batch Create	Batch Created Policy Table Library
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 Device specific flow or session
2012-04-20 09:26:33	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 AprChargingRuleList
2012-04-20 09:26:29	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: marTable1
2012-04-20 09:26:24	admin	10.26.3.2	Import - Initiated	Import of file "PolicyTableDataExport.xml" initiated.
2012-04-20 09:26:17	admin	10.26.3.2	Import - Completed	Import of file "TrafficProfileExport.xml" completed.
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: netcom.sp_5
Name: netcom.sp_5 QoSProfileType: Predefined POC Rule Rule Name: netcom.sp_5 Description:				
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: netcom.sp_2
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: surf.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: surf.sp_0
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmspn.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmspn.sp_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_42
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_22
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: internet1_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: internet1_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: blackberry.net_5

Figure 23: Audit Log Details

Searching for Audit Log Entries

To search for entries in the Audit Log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**. The **Audit Log** page opens in the work area.
2. Click **Search**. The **Audit Log Search Restrictions** page opens.
3. Define the following items, depending on how restrictive you want the audit log search to be:
 - **From/To** — Enter the start and end dates and times for this search.
 - **Action by User Names** — Enter the name of the user or users to audit.
 - **Action on Policy Servers / MRAs** — Enter the name of the Policy Management device to audit.
 - **Audit Log Items to Show** — Specifies a category of items to audit for display:
 - Policy Server
 - Scheduled Task
 - Network Element
 - Network Element Group
 - Network Element Link
 - Application
 - Policy
 - Policy Group
 - Account
 - Tier

- **Path**
- **User**
- **Audit**
- **Alarm**
- **OM Statistics**
- **MPE Manager**
- **Upgrade Manager**
- **Topology Setting**
- **Global Configuration Settings**

When you select some categories, a **Name** field appears, which lets you enter a search string; leave the field blank to include all items. When you select any category, an **Actions** link appears, which lets you select individual audit log items within the category. By default all items in the category are selected, but you can select individual items instead.


By default you can specify three item categories; click **More Lines** to add an additional item category.

- **Results Forms** — Specifies the number of items per page to display, along with which data to display (most recent or oldest items).
4. When you finish defining the search parameters, click **Search**.
The Audit Log displays search results.

Exporting Audit Log Data

You can export audit log data to a text file. The file name is `AuditLogExport.txt`.

To export data from the audit logs:


1. From the **System Administration** section of the navigation pane, select **Audit Log**.
The **Audit Log** page opens in the work area.
2. Click **Export/Purge**.
The **Export and Purge Audit Log Items** page opens.
3. In the **Items to Export** section, select one of the following options:
 - a) **Export All Items** — Writes all audit log entries.
 - b) **Export Through Date** — Click  (calendar icon), and select a date.
4. When you finish, click **Export**.
A standard **File Download** window opens; you can open or save the export file.

The audit log is exported.

Purging Audit Log Data

To purge data from the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
The **Audit Log** page opens in the work area.
2. Click **Export/Purge**.
The **Export and Purge Audit Log Items** page opens.

3. In the **Items to Purge** section, click  (calendar icon) and select a date.
4. When you finish, click **Purge**.
You are prompted with a confirmation message.
5. Click **OK**.

The data is purged from the audit log.

Managing Scheduled Tasks

The CMP system runs batch jobs to complete certain operations. These tasks are scheduled to run at regular intervals, with some tasks scheduled to run in a certain order. You can change the scheduling of these tasks to better manage network load or to propagate a network element change to the Policy Management devices on demand. You can also abort a running task.



Caution: Oracle recommends that you follow the order in which scheduled tasks are listed. Serious system problems can occur if the order is changed. Consult My Oracle Support before changing the order of task execution.

The tasks include:

Configuring a Task

To configure an individual task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.
The **Scheduled Task Administration** page opens in the work area.
2. To display details about a task, click the task name.
The current settings and status are displayed.

For example:

Scheduled Task Administration

Name	OM Statistics
Description	The task to retrieve OM statistics.
Last Exit Status	Success
Current State	Idle
Last Start Time	Jun 7, 2013 2:30:00 PM
Last End Time	Jun 7, 2013 2:30:02 PM
Next Run Time	Jun 7, 2013 2:45:00 PM
Run Interval	15 mins 0 sec

Settings

Number of days to keep statistical data (1 - 30) 7

Reschedule Settings Disable Refresh Cancel

Server time: Jun 07, 2013 02:32 PM EDT

Figure 24: Schedule Task Administration - OM Statistics

3. The options for this task are as follows:

- **Reschedule** — Click to reschedule the time that this task is performed on the Policy Management device.

For example:

Scheduled Task Administration

Name OM Statistics

Schedule by Interval

Next Run Time 06/07/2013 14:45

Run Interval Hours: 0 Minutes: 15

Following Another Task

Task to Follow <none>

Save Cancel

Server time: Jun 07, 2013 02:32 PM EDT

Figure 25: Scheduled Task Administration

- **Schedule by Interval (Next Run Time or Run Interval)** — Defines the run interval for the task to follow.

Valid run intervals are from 0 to 24 hours in 5-minute increments.

- **Following Another Task** — Schedules the task run time as following the completion of another scheduled task selected from the list.

- **Settings** — Number of days to keep data; the default is seven days. Available for the OM Statistics and Replication Statistics tasks only.
- **Disable** or **Enable** — Disables or enables the next scheduled execution of this process.

If you click **Disable**, a confirmation message displays. Click **OK**. The task is disabled and will not run at the next scheduled time, and the button changes to **Enable**.

- **Refresh** — Refreshes the page.
- **Cancel** — Returns to the previous page.

About Managing Users

The CMP system lets you configure the following user attributes:

Roles	What a user can do within the CMP system.
Scopes	What network element groups and Policy Management device groups a user can control, which provides a context for a role.
Users	After you define roles and scopes, you can apply them to user profiles.

Configuring Roles

Assigning roles to the various users that access the CMP system lets you control who can configure and access what within the CMP system. The default roles are:

- **Viewer** — Permits read-only access to functions associated with Policy Management device management and configuration. Access is also permitted to limited system administration functions, such as **Change Password**.
- **Operator** — Permits full read/write access to all Policy Management device management and configuration functions. Access is also permitted to all system administration functions except user administration.
- **Administrator** — Permits full read/write access to all functions. You cannot delete the Administrator role.

Creating a Role

To create a role:

1. From the **System Administration** section of the navigation pane, select **User Management**. The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group. The **Role Administration** page opens in the work area, displaying existing roles.
3. Click **Create Role**. The **New Role** page opens. By default, all access for privileges are set to either **Hide** (that is, the functions do not appear to users of the role, so access must be explicitly granted) or **Read-Only** (that is, information can be displayed but not changed).
4. Enter the **Name** for the new role.

Maximum of 64 characters.

5. Enter a **Description/Location** (optional).
Free-form text.
6. **Policy Server Privileges** — Defines access to the following MPE device management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
 - **Configuration**
 - **Applications**
 - **Network Element**
 - **AVP Definitions**
 - **Custom VSA Definitions**
 - **Global Configuration Settings**
7. **Subscriber Privileges** — Defines access to the subscriber functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
 - **Accounts**
 - **Subscriber Tier**
8. **Network Privileges** — Defines access to the network management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
 - **Topology**
 - **Paths**
9. **Policy Management Privileges** — Defines access to the policy management functions:
 - **Policy Library** (with the access **Hide**, **Read-Only**, **Read and Deploy**, or **Read, Deploy, and Write**)
 - **Template Library** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **Policy Table Library** (with the access **Hide**, **Read-Only**, or **Read-Write**) (not supported)
 - **Policy Import/Export** (with the access **Hide**, **Read-Only**, or **Read-Write**)
10. **System Wide Reports Privileges** — Defines access to the system-wide reports functions:
 - **Trending Reports Configuration**
11. **Platform Setting Privileges** — Defines access to the platform setting functions:
 - **Platform Setting** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
 - **Server Operation** (with the privileges **Hide** or **Read-Write**)
12. **Upgrade Manager Privileges** — Defines access to software upgrade functions:
 - **ISO Maintenance** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **System Maintenance** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
13. **System Administration Privileges** — Defines access to system administration functions:
 - **XML Import / Export** (with the access **Hide** or **Show**)
 - **Reports** (with the access **Hide** or **Show**)
 - **Operational Measurements** (with the access **Hide** or **Read-Only**)
 - **User Management** (with the access **Hide**, **Read-Only**, or **Read-Write**)

- **Scheduled Tasks** (with the access **Hide** or **Read-Write**)
- **Trace Log of Policy Server** (with the access **Read-Only** or **Read-Write**)
- **Trace Log** (with the access **Read-Only** or **Read-Write**)
- **Audit Log** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Audit Log User Info** (with the access **Hide** or **Show**)
- **Alarms** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Password Strength** (with the access **Read-Only** or **Read-Write**)
- **Push Method for Statistics** (with the access **Read-Only** or **Read-Write**)

If set to **Read-Only**, the following fields are displayed for the **Stats File Generator** (see [Managing Scheduled Tasks](#)) setting:

- **Name**
- **Description**
- **Last Exit Status**
- **Current State**
- **Last Start Time**
- **Last End Time**
- **Follows Task**

Task Settings

- **Local Repository** — Root directory of the local repository.
- **Maximum age to keep files (hours)** — Stats file retention period. Default is 72 hours.
- **File Format** — Either CSV or XML (default).
- **Stats Type** — Any stats type can be selected to generate stats. If you do not select a stats type, the task will not run normally.

Note: There are a total of four synchronized tasks which are supported but cannot be edited.

14. When you finish, click **Save**.

Privileges are assigned to the role.

Modifying a Role

To modify a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
The **Role Administration** page opens in the work area, displaying existing roles.
3. Select the role to modify.
The **Role** page opens.
4. Click **Modify**.
The **Modify Role** page opens.
5. Modify role information as necessary.
See [Creating a Role](#) for a description of the fields contained within this page.
6. Click **Save**.

The role is modified.

Deleting a Role

You can delete any role except the Administrator role. You cannot delete a role that is in use.

To delete a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
The **Role Administration** page opens in the work area, displaying existing roles.
3. Delete the role using one of the following methods:
 - From the work area, click the Delete icon located next to the role to delete.
 - From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

A confirmation message displays.

4. Click **OK**.

The role's information is deleted from the CMP database.

Creating a New Scope

You can configure scopes that contain selections of network element groups and Policy Management device groups that provide a context for a role. This lets you control what areas or devices in a network a user can manage. The default scope, **Global**, contains all items defined within the CMP database. Once you define a scope you can assign it to users.

To configure a new scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
2. In the content tree, click **Scopes**.
The **Scope Administration** page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. Click **Create Scope**.
The **New Scope** page opens.
4. Enter the **Name**
The name for the scope (up to 64 characters).
5. Enter the **Description/Location** (optional).
Free-form text.
6. Select the policy server groups included in this scope.
7. Select the network element groups included in this scope.
8. When you finish, click **Save** to create the scope.

The scope is created.

Modifying a Scope


To modify a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
2. In the content tree, click **Scopes**.
The **Scope Administration** page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. Select the scope you want to modify.
The scope description opens.
4. Click **Modify**.
The **Modify Scope** page opens. *Creating a New Scope* describes the fields on this page.
5. Modify scope information as necessary.
6. When you finish, click **Save**.

The scope is modified.

Deleting a Scope

You can delete any scope except **Global**. To delete a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
2. From the content tree, click **Scopes**.
The **Scope Administration** page opens in the work area, displaying existing scopes.
3. Delete the scope using one of the following methods:
 - From the work area, click  (trash can icon) located to the right of the scope to delete.
 - From the content tree, select the scope to delete (scope information displays in the work area), then click **Delete**.

A confirmation message appears.

4. Click **OK**.

The scope is deleted.

Creating a User Profile

The User Management functions include the tools necessary to create, modify, or delete system user profiles.

The CMP system is configured initially with the following default user profiles and passwords:

- admin/policies (you cannot delete this profile)
- operator/policies
- viewer/policies

Each default user profile has an associated role assigned to it. The **admin** user is the only profile that cannot be deleted or have its username modified. Also, the **admin** user is the only user who can create, modify, or delete other users. The password assigned to the **admin** user can be changed. For security

reasons, it is recommended that you change this value from the default value as soon as the system is installed.

Note: When logging in, the username is not case sensitive; however, the password is case sensitive.

To create a new user profile:

1. Log into the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
The **User Administration** page opens in the work area, displaying existing users.

Note: The **Log Out All Users** button is visible only to the **admin** user.

4. Click **Create User**.
The **New User** page opens.
5. Define the following information:
 - a) **Username** — Assign a name to the user profile of up to 64 characters (this value is not case sensitive).
 - b) **Description/Location** (optional) — Free-form text.
 - c) **Password** — Assign a password to the user profile.
This value is case sensitive and must contain at least six characters; alphabetic, numeric, and special characters are allowed. This value must conform to the password strength rules.
 - d) **Confirm Password** — Re-enter the password to confirm the value entered above.
 - e) **Password Expiration Period(days; 0=never)** — The number of days a password can be used before it expires. (This overrides the system setting.)
Enter a value from 7 to 365, or 0 to indicate that the password never expires. The default is the system setting.
 - f) **Force to Change Password** — If selected, this user must change passwords when he or she next logs in.
 - g) **Role** — Select a role from the drop list to assign to the user profile.
 - h) **Scopes** — Select one or more scopes to assign to the user profile.
6. When you finish, click **Save**.

The user profile is created and stored in the **Users** group.

Modifying a User Profile

To modify a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
The **User Administration** page opens in the work area, displaying existing users.
4. Select the user profile from the content tree.
The profile information page opens.
5. Click **Modify**.
The **Modify User** page opens.

6. Modify the user profile.
For field descriptions, see [Creating a User Profile](#).
7. Click **Save**.

The user profile is modified.

Deleting a User Profile

You can delete any user profile except **admin**. To delete a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
The **User Administration** page opens in the work area, displaying existing users.
4. Delete the user profile using one of the following methods:
 - From the work area, select the ✕(X icon), located to the right of the profile you want to delete.
 - From the content tree, select the user profile that you want to delete (profile information displays in the work area), then click **Delete**.

A confirmation message displays.

5. Click **OK** to delete the user profile.

The user profile is deleted.

About Locking and Unlocking User Accounts

A user is locked out after exceeding the login failure threshold, or if the **admin** user locks the user out. A locked-out user sees the following message on the login page when attempting to log in: `Your account is locked. Please contact the Administrator.`

Note: The **admin** account cannot lock the **admin** account.

The CMP system allows you to perform the following actions:

- [Locking an Account](#)
- [Unlocking an Account](#)

Locking an Account

To lock a user account:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
The **User Administration** page opens in the work area, displaying existing users.
4. Select the user profile from the content tree.
The **User Administration** page opens.
5. Click **Lock**.

A confirmation message appears.

6. Click **OK**.

The account is locked. The page displays the message `User account locked successfully`. The **Lock** button becomes an **Unlock** button. On the **User Administration** page, the Locked Status for the user shows `Locked`.

Unlocking an Account

To unlock a user account:

1. Log in to the CMP system as **admin**.

2. From the **System Administration** section of the navigation pane, select **User Management**. The content tree displays the **User Management** group.

3. Select the user profile from the content tree. The **User Administration** page opens.

4. Click **Unlock**. A confirmation message appears.

5. Click **OK**. The account is unlocked. The page displays the message `User account unlocked successfully`. The **Unlock** button becomes a **Lock** button. On the **User Administration** page, the Locked Status for the user shows `Unlocked by Admin`.

Changing a Password

The Change Password option lets users change their password. This system administration function is available to all users.

Note: The **admin** user can change the password for any user.

Note: To reset the administrator password, contact My Oracle Support.

To change your password:

1. From the **System Administration** section of the navigation pane, select **Change Password**.

The **Change Password** page opens. If your account is set up with a password expiration period, the expiration date is displayed.

2. Enter the following information:

a) **Current Password** — The present value of the password.

b) **New Password** — The value of the new password.

This value is case sensitive and must conform to the password strength rules. The password cannot contain the user name.

c) **Confirm Password** — Enter the new password value again.

If your new password does not conform to the password strength rules, a validation error message appears; for example:

Password Expired

The password for this account must be changed.

Validation Error

You must correct the following error(s) before proceeding:

- The password does not coincide with password strength.
- The password **MUST** contain characters from at least 4 categories in lower-case letters, upper-case letters, numerals and non-alphanumeric characters.
- The password **MUST** contain at least 1 lower-case letters.
- The password **MUST** contain at least 1 upper-case letters.
- The password **MUST** contain at least 1 numerals.
- The password **MUST** contain at least 1 non-alphanumeric characters.

Username:

Current Password:

New Password:

Confirm Password:

3. When you finish, click **Change Password**.

Your password is changed.

Appendix

A

CMP Modes

Topics:

- [The Mode Settings Page.....187](#)

The functions available in the CMP system are determined by the operating modes and sub-modes selected when the software is installed. Functions that can change include:

- Items on the navigation pane
- Tabs on the **Policy Server Administration** page
- Protocols supported
- Configuration options
- Policy options available in the policy wizard
- Reports available

Normally, servers are pre-configured before delivery. However, if it becomes necessary to replace a server or reinstall the software in the field, the mode selection screen becomes visible, and you must reset the operational modes as appropriate for your environment before you can use the product.

This appendix briefly describes the modes and sub-modes available.



Caution: CMP modes should only be set in consultation with My Oracle Support. Setting modes inappropriately could result in the loss of network element connectivity, policy function, statistical data, and cluster redundancy.

The Mode Settings Page

When you use a web browser to connect to a CMP system after the software is first installed, the **Mode Settings** page opens ([Figure 26: Mode Settings Page](#)). Select modes, sub-modes, and management options, and then click **OK**. The browser page closes and you are automatically logged out. When you next log in, the CMP system reopens in the selected mode.

The management options are as follows:

- **Manage Policy Servers** — Manage MPE devices
- **Manage SIP-AM Servers** — Manage Session Initiation Protocol Application Manager (SIP-AM) servers
- **Manage CD-AM Servers** — Manage Content Distribution Network servers
- **Manage MA Servers** — Manage Management Agent servers
- **Manage Policies** — Enable the policy wizard
- **Manage MRAs** — Manage Policy Front End servers
- **Manage SPR Subscriber Data** — Manage Subscriber Profile Repository servers
- **Manage Geo-Redundant MPE/MRA/BoD** — Manage georedundant MPE or MRA clusters
- **Manager is HA (clustered)** — Enable High Availability features
- **Manage Analytic Data** — Enable output of policy event records

Cable Mode Enables support of a cable carrier environment. Functions are described in the *Configuration Management Platform Cable User's Guide*.

PCMM Supports PacketCable MultiMedia functions.

DQOS Supports Dynamic Quality of Service functions. (This mode enables a configuration that is no longer supported.)

Diameter AF Supports Diameter AF.

Wireless Mode Enables support of a wireless carrier environment. Functions are described in the *Configuration Management Platform Wireless User's Guide*.

Diameter 3GPP Supports Diameter 3GPP protocol.

Diameter 3GPP2 Supports Diameter 3GPP2 protocol.

PCC Extensions Supports Policy and Charging Control functions.

Quotas Gx Supports a subscriber quota environment using the Diameter Gx protocol. The Gx protocol supports deep packet inspection (DPI) devices.

Quotas Gy Supports a subscriber quota environment using the Diameter Gy protocol.

LI Supports Lawful Intercept functions. Described in the *Configuring Lawful Intercept Application Note*.

SCE-Gx Supports the Cisco Service Control Engine Gx protocol. If this mode is selected, Diameter 3GPP and RADIUS must also be selected, and other Gx sub-modes must not be selected.

	Gx-Lite	Supports the Gx-Lite protocol, a simplified version of 3GPP Gx for use by non-GGSN PCEF vendors that do not have access to network-level information.
	Cisco Gx	Supports the Cisco Gx protocol.
	DSR	Supports Policy Management network segmentation using an Oracle Communications Diameter Signaling Router system.
SMS Mode		Enables support of SMS servers. Functions are described in the <i>Configuration Management Platform Wireless User's Guide</i> .
	SMPP	Supports SMS using SMPP protocol.
	XML	Supports SMS using XML.
SPR Mode		Enables support of a Subscriber Profile Repository. Select only one sub-mode. Functions of the Oracle Communications Enhanced Subscriber Profile Repository are described in the ESPR documentation.
	Subscriber Profiles	Supports subscriber profile functions.
	Quota	Supports subscriber quotas.
Wireline Mode		Enables support of a wireline carrier environment. Functions are described in the <i>Configuration Management Platform Wireline User's Guide</i> .
SPC Mode		Enables the COPS Application Manager product, which accepts service provisioning requests from a Session Border Controller over the Common Open Policy Service (COPS) protocol. Functions are described in the <i>Service Provisioning over COPS Application Manager User's Guide</i> .
RADIUS Mode		Enables support of RADIUS AAA.

Mode

Mode Settings

Category	Item	Status
Cable	PCMM	<input type="checkbox"/>
	DQOS	<input type="checkbox"/>
	Diameter AF	<input type="checkbox"/>
Wireless	Diameter 3GPP	<input type="checkbox"/>
	Diameter 3GPP2	<input type="checkbox"/>
	PCC Extensions	<input type="checkbox"/>
	Quotas Gx	<input type="checkbox"/>
	Quotas Gy	<input type="checkbox"/>
	LI	<input type="checkbox"/>
	SCE-Gx	<input type="checkbox"/>
	Gx-Lite	<input type="checkbox"/>
	Cisco Gx	<input type="checkbox"/>
	DSR	<input type="checkbox"/>
	SMS	SMPP
XML		<input type="checkbox"/>
SPR		
Subscriber Profiles	<input type="checkbox"/>	
Quota	<input type="checkbox"/>	
Wireline	<input checked="" type="checkbox"/>	
SPC	<input type="checkbox"/>	
RADIUS	<input type="checkbox"/>	

Manage Policy Servers	<input checked="" type="checkbox"/>
Manage SIP-AM Servers	<input type="checkbox"/>
Manage CD-AM Servers	<input type="checkbox"/>
Manage MA Servers	<input type="checkbox"/>
Manage Policies	<input checked="" type="checkbox"/>
Manage MRAs	<input type="checkbox"/>
Manage SPR Subscriber Data	<input type="checkbox"/>
Manage Geo-Redundant MPE/MRA	<input type="checkbox"/>
Manager is HA (clustered)	<input checked="" type="checkbox"/>
Manage Analytic Data	<input type="checkbox"/>

Figure 26: Mode Settings Page

#

3GPP
3rd Generation Partnership Project
The standards body for wireless communications.

3GPP2
3rd Generation Partnership Project
2

A

AF
Application Function (such as P-CSCF)

application
The telecommunications software that is hosted on the platform. A service provided to subscribers to a network; for example, voice over IP (VoIP), video on demand (VoD), video conferencing, or gaming.

B

C

CMP
Configuration Management Platform
A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.

COPS
Common Open Policy Service
A protocol that is part of the internet protocol suite as defined by the IETF's RFC 2748. COPS

C

specifies a simple client/server model for supporting policy control over Quality of Service (QoS) signaling protocols (e.g., RSVP).

D

Diameter

Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment.

E

event

In Policy Management, an expected incident that is logged. Events can be used for debugging purposes.

F

failover

The capability to automatically switch to a redundant or backup server, system, or network when the previously active server, system, or network fails or terminates abnormally. In certain instances, however, automatic failover may not be desirable, and human intervention may be required to initiate the failover manually.

F

FQDN

Fully Qualified Domain Name

The complete domain name for a specific computer on the Internet (i.e., www.oracle.com).

A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GUI

Graphical User Interface

The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA

High Availability

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

HTTP

Hypertext Transfer Protocol

I

IPv4

Internet Protocol version 4

Identifies an Internet Protocol version 4 address composed of 4 bytes in a dotted decimal format (for example, nnn.nn.nnn.nn).

M

MPE

Multimedia Policy Engine

A high-performance, high-availability platform for operators to deliver and manage differentiated services over

M

high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization.

Multimedia Policy Engine See MPE.

N

network device A physical piece of equipment or a logical (software) entity connected to a network; for example, CMTS, video distribution router, gateway router, or a link. This may also include sub-components of network elements (such as an interface) or lower-level devices such as cable modems or CPEs.

network topology A map of physical equipment or logical entities in a network.

O

OSS Operations Support System
Computer systems used by telecommunications service providers, supporting processes such as maintaining network inventory, provisioning services, configuring network components, and managing faults.

OSSI Operation Support System
Interface
An interface to a “back-end” (office) system. The Configuration

O

Management Platform includes an OSSI XML interface.

P

PCC

Policy and Charging Control

Policy rules that define the conditions and actions used by a carrier network to control how subscribers and applications are treated and how network resources are allocated and used.

PCRF

Policy and Charging Rules Function

The ability to dynamically control access, services, network capacity, and charges in a network.

Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.

In the Policy Management system, PCRF is located in the MPE device.

policy and charging rules function

See PCRF.

policy group

An ordered group of policies, organized for ease of administration or deployment.

Q

QoS

Quality of Service

Control mechanisms that guarantee a certain level of performance to a data flow.

R

RADIUS

Remote Authentication Dial-In
User Service

A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

S

server

In Policy Management, a computer running Policy Management software, or a computer providing data to a Policy Management system.

SMPP

Short Message Peer-to-Peer
Protocol

An open, industry standard protocol that provides a flexible data communications interface for transfer of short message data.

SMS

Short Message Service

A communication service component of the GSM mobile communication system that uses standard communications protocols to exchange short text messages between mobile phone devices. See also GSM.

Shared Metric Service

SNMP

Simple Network Management
Protocol.

An industry-wide standard protocol used for network

S

management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

T

TPD

Tekelec Platform Development

The Oracle Communications Tekelec Platform (TPD) is a standard Linux-based operating system packaged and distributed by Oracle. TPD provides value-added features for managing installations and upgrades, diagnostics, integration of 3rd party software (open and closed source), build tools, and server management tools.

V

VoIP

Voice Over Internet Protocol

Voice communication based on the IP protocol competes with legacy voice networks, but also with Voice over Frame Relay and Voice and Telephony over ATM. Realtime response, which is characterized by minimizing frame loss and latency, is vital to voice communication. Users are only prepared to accept minimal delays in voice transmissions.

X

XML

eXtensible Markup Language

A version of the Standard Generalized Markup Language (SGML) that allows Web

X

developers to create customized tags for additional functionality.