

Oracle® Communications Policy Management

Configuration Management Platform Wireless User's Guide

Release 12.1.2

E71642 Revision 01

June 2016

Copyright © 2014, 2016, 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: About This Guide.....	19
Introduction.....	20
How This Guide is Organized.....	20
Scope and Audience.....	21
Related Publications.....	21
Policy and Protocol Specifications.....	21
Locate Product Documentation on the Oracle Help Center Site.....	22
Customer Training.....	22
My Oracle Support (MOS).....	23
Emergency Response.....	23
 Chapter 2: Oracle Communications Policy Management System.....	 24
Elements of the Oracle Communications Policy Management Solution.....	25
Multimedia Policy Engine Devices.....	27
Multi-Protocol Routing Agent Devices.....	29
Subscriber Profile Repository.....	31
Configuration Management Platform System.....	31
Specifications for Using the CMP System.....	31
Logging In.....	32
Logging In to a Standby or Secondary-Site CMP System.....	32
GUI Overview.....	32
CMP Icons.....	34
Shortcut Selection Keys.....	35
Network Configuration Management Platform.....	35
Device Configuration in a Network CMP.....	36
Network CMP Tier Capabilities.....	37
About Specialized Communications Protocols.....	40
About RADIUS Protocol.....	40
About Diameter Protocol.....	40
About TACACS Plus Protocol.....	40
Overview of Main Tasks.....	41
 Chapter 3: Configuring the Policy Management Topology.....	 42

About the Policy Management Topology.....	43
High Availability.....	44
Georedundant Spare Servers.....	45
CMP Georedundancy.....	46
Georedundancy for Non-CMP Servers.....	46
Primary and Secondary Sites.....	48
Georedundant Site Preferences.....	49
Server Status.....	49
Policy Management Network Segmentation.....	50
Virtualization.....	52
Setting Up the Topology.....	54
Setting Up a CMP Cluster.....	55
Setting Up a Non-CMP Cluster.....	58
Setting Up a Georedundant Site.....	61
Setting Up a Georedundant Non-CMP Cluster.....	62
Example: Setting Up Georedundancy.....	68
Modifying the Topology.....	74
Modifying a Georedundant Site.....	74
Removing a Site from the Topology.....	74
Modifying a non-CMP Cluster.....	75
Modifying a CMP Cluster.....	76
Removing a Cluster from the Topology.....	76
Reversing Georedundant Cluster Preference.....	77
Demoting a Georedundant CMP Cluster.....	77
Promoting a Georedundant CMP Cluster.....	79
Changing Server Status to Forced Standby.....	80
Configuring SNMP Settings.....	81
Platform Configuration Settings.....	83
Configuring the Upsync Log Alarm Threshold.....	83
Configuring Concurrent Bulk Transfers.....	83

Chapter 4: Managing Multimedia Policy Engine Devices.....85

Managing Policy Server Profiles.....	86
Creating a Policy Server Profile.....	86
About Policy Server Administration.....	87
Configuring a Policy Server Profile.....	87
Modifying a Policy Server Profile.....	88
Deleting a Policy Server Profile.....	88
Managing Configuration and Virtual Templates.....	89
Creating a Configuration Template.....	89

Creating a Configuration Template.....	90
Modifying a Template.....	90
Changing the Template Priority.....	91
Creating a Virtual Template.....	92
Configuring MPE Protocol Options.....	92
Associations Configuration Options.....	93
Subscriber Indexing Configuration Options.....	94
General Configuration Options.....	94
RADIUS-S Configuration Options.....	96
Diameter Configuration Options.....	96
S9 Configuration Options.....	98
User Profile Lookup Retry and Session Updates Configuration Options.....	98
Diameter AF Default Profiles Configuration Options.....	98
Default Charging Servers Configuration Options.....	99
SMS Relay Configuration Options.....	99
SMPP Configuration Options.....	99
SMS/XML Configuration Options.....	100
Primary SMSC Host Configuration Options.....	100
Secondary SMSC Host Configuration Options.....	101
SMTP Configuration Options.....	102
Generic Notification Configuration Options.....	103
RADIUS Configuration Options.....	103
Analytics Configuration Options.....	104
Configuring Data Source Interfaces.....	104
Configuring an LDAP Data Source.....	106
Configuring an Sh Data Source.....	110
Configuring an Sy Data Source.....	112
Policy Server Groups.....	115
Creating a Policy Server Group.....	116
Adding a Policy Server to a Policy Server Group.....	116
Creating a Policy Server Sub-group.....	116
Renaming a Policy Server Group.....	117
Removing a Policy Server Profile from a Policy Server Group.....	117
Deleting a Policy Server Group.....	117
About Reapplying a Configuration.....	118
Reapplying the Configuration to a Single Device.....	118
Reapplying the Configuration to a Group of Devices.....	119
Rediscovering a Cluster.....	119
Resetting Counters.....	119
Enabling or Disabling All Sh Connections.....	120
Checking the Status of an MPE Server.....	120

Policy Server Reports.....	121
Cluster Information Report.....	123
Time Period.....	123
Policy Statistics.....	123
Quota Profile Statistics.....	124
Traffic Profile Statistics.....	125
Session Cleanup Statistics.....	125
Sy Reconciliation Statistics.....	125
Protocol Statistics.....	126
Latency Statistics.....	127
Event Trigger Statistics.....	128
Error Statistics.....	128
Data Source Statistics.....	128
Database Statistics.....	131
KPI Interval Statistics.....	131
Viewing Policy Server Logs.....	132
Viewing the Trace Log.....	132
Syslog Support.....	134
The SMS Log.....	134
The SMPP Log.....	134
The SMTP Log.....	134
The HTTP Log.....	135
Configuring Log Settings.....	135
Analytics Data Stream.....	137
 Chapter 5: Configuring Protocol Routing.....	 139
Configuring Diameter Peers.....	140
Configuring Diameter Realm Based Peer Routes.....	142
 Chapter 6: Configuring Advanced Device Settings.....	 144
Configuring Expert Settings.....	145
Configuring Service Overrides.....	151
About Overload Controls.....	153
Configuring MPE and MRA Load Shedding Rules.....	154
MPE Default Load Shedding Rules.....	155
MRA Default Load Shedding Rules.....	157
Resetting Configuration Keys to Defaults.....	157
Filtering the Configuration Keys.....	158
Exporting the Configuration Keys.....	159

Chapter 7: Managing Network Elements.....160

About Network Elements.....	161
Defining a Network Element.....	161
Modifying a Network Element.....	162
Deleting Network Elements.....	162
Deleting Multiple Network Elements.....	163
Finding a Network Element.....	163
Configuring Options for Network Elements.....	164
Configuring the PDSN Network Element.....	164
Configuring the Home Agent Network Element.....	165
Configuring a GGSN Network Element.....	165
Configuring the HSGW Network Element.....	166
Configuring the PGW Network Element.....	167
Configuring the SGW Network Element.....	167
Configuring a DPI Network Element.....	168
Configuring a DSR Network Element.....	169
Associating a Network Element with an MPE Device.....	170
Working with Network Element Groups.....	171
Creating a Network Element Group.....	171
Adding a Network Element to a Network Element Group.....	171
Creating a Network Element Sub-group.....	172
Deleting a Network Element from a Network Element Group.....	172
Modifying a Network Element Group or Sub-Group.....	173
Deleting a Network Element Group or Sub-group.....	173

Chapter 8: Managing the Protocol Timer Profiles Function.....174

About Protocol Timer Profiles.....	175
Viewing a Protocol Timer Profile.....	176
Creating a Protocol Timer Profile.....	176
Modifying a Protocol Timer Profile.....	178
Deleting a Protocol Timer Profile.....	178

Chapter 9: Managing Charging Servers.....180

About Charging Servers.....	181
Defining a Charging Server.....	181
Modifying a Charging Server.....	182
Deleting a Charging Server.....	182
Associating a Charging Server with an MPE Device.....	183

Chapter 10: Mapping Serving Gateways to MCCs/MNCs.....184

About Mapping Serving Gateways to MCCs/MNCs.....	185
Creating a Mapping.....	185
Modifying a Mapping.....	185
Deleting a Mapping.....	186

Chapter 11: About Subscriber Profile Repositories.....187

About Subscriber Profile Repositories.....	188
Configuring the CMP System to Manage SPR Subscriber Data.....	189
Configuring the SPR Connection.....	189
Modifying the SPR Connection.....	190
About Subscriber Profiles.....	190
Finding a Subscriber Profile.....	190
Creating a Subscriber Profile.....	191
Modifying a Subscriber Profile.....	192
Deleting a Subscriber Profile.....	192
About Subscriber Quota Categories.....	193
Viewing Subscriber Quota Information Associated with a Subscriber.....	193
Adding a Subscriber Quota Category.....	194
Modifying a Subscriber Quota Category.....	195
Deleting a Subscriber Quota Category.....	195
About Subscriber Entity States.....	196
Viewing Subscriber Entity States Associated with a Subscriber.....	196
Creating a Subscriber Entity State Property.....	196
Modifying a Subscriber Entity State Property.....	197
Deleting a Subscriber Entity State Property.....	197
About Pool Profiles.....	198
About Pool Types.....	198
Querying by Pool ID.....	198
Creating a Pooled Quota Group.....	199
Adding a Member to a Basic Pooled Quota Group.....	199
Modifying a Pool Profile.....	200
Deleting a Pool Profile.....	201
About Pool Quota Profiles.....	201
Creating a Pool Quota Profile.....	201
Modifying a Pool Quota Profile.....	202
Deleting a Pool Quota Profile.....	203
About Pool States.....	203
Creating a Pool State.....	203

Modifying a Pool State.....	204
Deleting a Pool State.....	204
About Subscriber Dynamic Quotas.....	205
Viewing Subscriber Dynamic Quota Information.....	205
Adding a Subscriber Dynamic Quota Category.....	205
Modifying a Subscriber Dynamic Quota Category.....	207
Resetting a Subscriber Dynamic Quota.....	207
Deleting a Subscriber Dynamic Quota Category.....	208
 Chapter 12: Managing Subscribers.....	209
Creating a Subscriber Tier.....	210
Deleting a Tier.....	210
Creating an Entitlement.....	211
Deleting an Entitlement.....	211
Displaying Static Session and Binding Data for a Subscriber.....	212
 Chapter 13: Managing Policy Front End Devices.....	214
Configuring the CMP System to Manage an MRA Cluster.....	215
Defining an MRA Cluster Profile.....	215
Modifying an MRA Cluster Profile.....	216
Associating Network Elements with an MRA Device.....	216
Configuring MRA Protocol Options.....	217
Configuring Diameter Peers.....	219
Configuring Diameter Host Based Peer Routes.....	221
Configuring Diameter Realm Based Peer Routes.....	223
Examples of JAVA Regular Expressions for MRA Routes.....	224
Working with MRA Groups.....	225
Creating an MRA Group.....	225
Adding an MRA Cluster Profile to an MRA Group.....	225
Removing an MRA Cluster Profile from an MRA Group.....	226
Deleting an MRA Group or Sub-group.....	226
Enabling Stateless Routing.....	226
Reapplying the Configuration to Policy Management Devices.....	227
Resetting Counters.....	228
About Stateless Routing.....	228
Enabling Stateless Routing.....	229
Modifying the Stateless Migration Mode in an Existing MRA.....	229
Loading MPE/MRA Configuration Data when Adding Diameter Peer.....	230

Chapter 14: Managing S-CMP Devices.....231

About S-CMP Devices.....	232
Creating an S-CMP Device.....	232
Opening an S-CMP Device from an NW-CMP.....	233
Modifying an S-CMP Device.....	233
Reapplying the Configuration to S-CMP Devices.....	233
Deleting an S-CMP Device.....	234
About S-CMP Groups.....	234
Creating an S-CMP Group.....	234
Adding S-CMP Devices to a Policy Server Group.....	235
Creating an S-CMP Sub-group.....	235
Renaming an S-CMP Group.....	235
Deleting an S-CMP Group.....	236

Chapter 15: System-Wide Report.....237

KPI Dashboard.....	238
Mapping Display to KPIs.....	240
Mapping Reports Display to KPIs.....	244
About Color Threshold Configuration.....	266
Subscriber Activity Log.....	266
Subscriber Activity Log Limitations.....	267
Viewing a Subscriber Activity Log.....	267
Configuring Subscriber Activity Logs.....	268
Adding Subscriber Identifiers.....	269
Configuring Subscriber Activity Log Backup Settings.....	270
Editing a Subscriber Identifier.....	271
Deleting a Subscriber Identifier from the Activity Log.....	271
Viewing Subscriber Activity Log History.....	272
Viewing the Trending Reports.....	272
Viewing MRA Binding Count.....	273
Viewing PDN Connection Count.....	273
Viewing Session Count.....	274
Viewing Transaction Per Second.....	275
Custom Trending Reports.....	276
Viewing Alarms.....	279
Viewing Active Alarms.....	280
Viewing the Alarm History Report.....	281
Viewing Session Reports.....	283
Viewing the AF Session Report.....	283

Viewing the PDN Connection Report.....	285
Viewing the PDN APN Suffix Report.....	286
Viewing Other Reports.....	287
Viewing the Connection Status Report.....	287
Viewing the Protocol Errors Report.....	289
Viewing the Policy Statistics Report.....	290
Viewing the MPE/MRA Replication Statistics Report.....	291
Viewing the SGW Failure Report.....	294
 Chapter 16: Upgrade Manager.....	296
Overview of Upgrade Manager.....	297
Overview of Upgrade.....	297
About ISO Files on Servers.....	297
Pushing a Script to the Servers (Upgrade From Release 11.5 Only).....	298
Adding an ISO File to a Server.....	298
Deleting ISO Files from the Servers.....	299
Manually Adding ISO Files to the Servers.....	299
About Performing an Upgrade.....	300
Preparing for an Upgrade.....	301
Preparing to install a Patch or Patch Set	301
Selecting an ISO for Upgrade.....	302
Upgrading a Release 11.5 Primary-site CMP Cluster.....	303
Upgrading a Primary-site CMP Cluster.....	304
Upgrading a Georedundant Cluster.....	306
Viewing the Upgrade Log.....	308
Upgrade Manager Page Elements.....	309
About Rolling Back an Upgrade.....	312
Rolling Back an Upgrade.....	313
Rolling Back a Release 11.5 Primary-site CMP Cluster.....	314
ISO Maintenance Page Elements.....	316
 Chapter 17: Global Configuration.....	319
Setting the Precedence Range.....	320
Setting UE-Initiated Procedures.....	321
Setting Stats Settings.....	321
Setting Quota Settings.....	322
Setting eMPS ARP Settings.....	323
Setting S9 Settings.....	324
Setting PDN APN Suffixes.....	324
Configuring the Activity Log.....	325

Configuring Custom APNs.....	326
About Emergency APNs Settings.....	327
Adding Emergency APNs Settings.....	327
Deleting Emergency APNs Settings.....	327
Adding Emergency Service-URNs Settings.....	328
Deleting Emergency Service-URNs.....	328
Chapter 18: System Administration.....	329
Configuring System Settings.....	330
Importing and Exporting Configurable Objects.....	332
User Privileges and Import/Export.....	332
About Importing Configuration Objects.....	333
About Exporting Configuration Objects.....	335
About the Manager Reports.....	341
Viewing Manager Reports.....	341
Viewing the Trace Log.....	342
Filtering the Trace Log.....	343
Configuring the Trace Log.....	343
Modifying the Trace Log Configuration.....	344
Viewing the Audit Log.....	344
Searching for Audit Log Entries.....	346
Exporting or Purging Audit Log Data.....	347
Managing Scheduled Tasks.....	347
Configuring a Scheduled Task.....	349
Rescheduling a Task.....	350
Enabling or Disabling a Scheduled Task.....	350
About Managing Users.....	351
Creating a Customer User Management System Profile.....	351
About User Roles.....	352
About User Scopes.....	355
About User Profiles.....	357
About External Authentication.....	360
Changing a Password.....	367
Appendix A: CMP Modes.....	368
About Mode Settings.....	369
Appendix B: Generated Statistics.....	373
List of Generated Statistics.....	374

Glossary.....	376
----------------------	------------

List of Figures

Figure 1: The Policy Management Solution and MPE Devices.....	26
Figure 2: Diameter Interfaces to the MPE Device.....	29
Figure 3: Typical MRA Network.....	30
Figure 4: Layout of the CMP Window – Wireless Mode.....	33
Figure 5: Policy Management Network Configuration Management Platform.....	36
Figure 6: Device Configuration Flow Using Configuration Templates.....	37
Figure 7: Example Policy Management Topology.....	43
Figure 8: High Availability.....	44
Figure 9: Clusters with Active, Standby, and Spare Servers.....	45
Figure 10: CMP Georedundancy.....	46
Figure 11: Non-CMP Georedundant Configuration.....	47
Figure 12: Example of Primary and Secondary Sites.....	49
Figure 13: Segmented Policy Management Network.....	51
Figure 14: Virtualization Architecture.....	52
Figure 15: Policy Management Minimum Virtualized Topology.....	53
Figure 16: Cluster Settings Page for Wireless CMP Cluster.....	56
Figure 17: Sample MRA Cluster Topology Configuration.....	61
Figure 18: Sample BoD Cluster Site 1 Configuration.....	67
Figure 19: Sample BoD Cluster Site 2 Configuration.....	68
Figure 20: Site Configuration.....	70
Figure 21: Example of Primary Site Settings.....	71
Figure 22: Group View	121

Figure 23: Sample Protocol Statistics.....	126
Figure 24: Sample Error Statistics.....	128
Figure 25: Add Diameter Peer.....	140
Figure 26: Select Network Elements.....	170
Figure 27: Session Viewer Page.....	213
Figure 28: Select Network Elements.....	217
Figure 29: Add Diameter Peer.....	219
Figure 30: Enabling Stateless Routing.....	227
Figure 31: Enabling Stateless Routing.....	229
Figure 32: Example of KPI Dashboard with MRA Devices Managed by the CMP System.....	238
Figure 33: Trending Report Definition Configuration Page.....	277
Figure 34: Sample Active Alarms Report.....	280
Figure 35: Alert Details.....	282
Figure 36: Sample Connection Status Report.....	288
Figure 37: Sample MPE/MRA Replication Statistics Report.....	291
Figure 38: Sample Upgrade Log.....	309
Figure 39: Sample Upgrade Manager Page.....	310
Figure 40: Sample ISO Maintenance Page.....	316
Figure 41: Sample Password Strength Policy.....	332
Figure 42: Bulk Export Window.....	336
Figure 43: Audit Log.....	345
Figure 44: Audit Log Details.....	346
Figure 45: Sample RADIUS User Information Flat File.....	362
Figure 46: Sample VSA Dictionary File For RADIUS.....	362
Figure 47: Sample User for RADIUS Server.....	363

Figure 48: Mode Settings Page.....	372
------------------------------------	-----

List of Tables

Table 1: Top Level Objects by Management Tier.....	38
Table 2: Expert Settings for MPE.....	145
Table 3: Expert Settings for MRA.....	150
Table 4: MPE Busyness Level 1.....	156
Table 5: MPE Busyness Level 2.....	156
Table 6: MPE Busyness Level 3.....	156
Table 7: MPE Busyness Level 4.....	156
Table 8: MRA Busyness Level 1.....	157
Table 9: MRA Busyness Level 2	157
Table 10: Supported Diameter Applications and Messages.....	175
Table 11: Supported Diameter Applications and Messages.....	177
Table 12: MRA Protocol Configuration Options.....	217
Table 13: KPI Definitions for MRA Devices.....	240
Table 14: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System.....	242
Table 15: KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System.....	243
Table 16: Policy Statistics.....	244
Table 17: Quota Profile Statistics Details.....	245
Table 18: Diameter Application Function (AF) Statistics.....	245
Table 19: Diameter AF Peer Stats (in Diameter AF Stats window).....	246
Table 20: Diameter Policy Charging Enforcement Function (PCEF) Statistics.....	247
Table 21: Diameter Charging Function (CTF) Statistics.....	248

Table 22: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics.....	249
Table 23: Diameter TDF Statistics.....	250
Table 24: Diameter Sh / Sh Peer Statistics.....	252
Table 25: Diameter S9 Statistics.....	253
Table 26: Diameter Distributed Routing and Management Application (DRMA) Statistics.....	255
Table 27: Diameter DRA Statistics.....	257
Table 28: Diameter Sy Statistics.....	258
Table 29: RADIUS Statistics.....	259
Table 30: Diameter Latency Statistics.....	261
Table 31: Diameter Event Trigger Statistics.....	261
Table 32: Diameter Protocol Error Statistics.....	262
Table 33: Diameter Connection Error Statistics.....	262
Table 34: LDAP Data Source Statistics.....	262
Table 35: Sh Data Source Statistics.....	263
Table 36: Sy Data Source Statistics.....	265
Table 37: KPI Interval Statistics.....	265
Table 38: Status and Related Icons.....	270
Table 39: Blade State Values in MPE/MRA Replication Stats Report.....	291
Table 40: Sync State Values in MPE/MRA Replication Stats Report.....	292
Table 41: Priority Table in MPE/MRA Replication Stats Report.....	293
Table 42: Upgrade Manager Page Elements.....	310
Table 43: ISO Maintenance Page Elements.....	316

Chapter 1

About This Guide

Topics:

- [*Introduction.....20*](#)
- [*How This Guide is Organized.....20*](#)
- [*Scope and Audience.....21*](#)
- [*Related Publications.....21*](#)
- [*Locate Product Documentation on the Oracle Help Center Site.....22*](#)
- [*Customer Training.....22*](#)
- [*My Oracle Support \(MOS\).....23*](#)
- [*Emergency Response.....23*](#)

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 wireless network.

How This Guide is Organized

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

- [About This Guide](#) provides general information about the organization of this guide, related documentation, and how to get technical assistance.
 - [Oracle Communications Policy Management System](#) provides an overview of the Oracle Communications Policy Management Multimedia Policy Engine (MPE) device, which manages multiple network-based client sessions; the network in which the MPE device operates; policies; and 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.
 - [Configuring Protocol Routing](#) describes how to configure protocol routing.
 - [Configuring Advanced Device Settings](#) describes how to specify advanced settings for MPE or MRA devices.
 - [Managing Network Elements](#) describes how to manage network elements.
 - [Managing the Protocol Timer Profiles Function](#) describes how to manage protocol timer profiles.
 - [Managing Charging Servers](#) describes how to manage charging servers.
 - [Mapping Serving Gateways to MCCs/MNCs](#) describes how to map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs).
 - [About Subscriber Profile Repositories](#) describes how to manage a Subscriber Profile Repository (SPR).
 - [Managing Subscribers](#) describes how to manage subscriber tiers, entitlements, and quota usage within the CMP system.
 - [Managing Policy Front End Devices](#) describes the Oracle Communications Policy Management Policy Front End (also known as the MRA), a standalone entity that supports MPE devices and is manageable by the CMP system.
 - [Managing S-CMP Devices](#) describes how to configure and organize S-CMP devices in a tiered CMP system.
- Note:** This function is restricted. See [About Mode Settings](#) for more information.
- [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.
 - [Global Configuration](#) describes how to configure global settings in the CMP system.
 - [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.
- The appendix, [Generated Statistics](#) available statistics for generated scheduled tasks.

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

For information about additional publications that are related to this document, refer to the Oracle Help Center site. See [Locate Product Documentation on the Oracle Help Center Site](#) for more information.

Policy and Protocol Specifications

The following specifications provide information on cable and wireless protocols:

- Internet Engineering Task Force (IETF) specifications:
 - RADIUS RFCs:
 - RFC 2865: RADIUS
 - RFC 2866: RADIUS Accounting
 - RFC 3576: Dynamic Authorization Extensions to RADIUS
 - Diameter RFCs:
 - RFC 3539: Authentication, Authorization and Accounting (AAA) Transport Profile
 - RFC 3588: Diameter Base Protocol
 - TACACS+ RFC 1492: An Access Control Protocol, Sometimes Called TACACS
 - RFC 3164: The BSD syslog Protocol
- 3rd Generation Partnership Project (3GPP) technical specifications:
 - 3GPP TS 23.003: Numbering, addressing and identification (Release 12)
 - 3GPP TS 23.203: Policy and charging control architecture (Release 13.2)
 - 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses (Release 13)
 - 3GPP TS 29.208: End-to-end Quality of Service (QoS) signalling flows (Release 6)
 - 3GPP TS 29.209: Policy control over Gq interface (Release 6)
 - 3GPP TS 29.211: Rx Interface and Rx/Gx signalling flows (Release 6)
 - 3GPP TS 29.212: Policy and Charging Control over Gx/Sd reference point (Release 13.0)

- 3GPP TS 29.213: Policy and Charging Control signalling flows and QoS parameter mapping (Release 12.x6)
- 3GPP TS 29.214: Policy and Charging Control over Rx reference point (Release 13.0)
- 3GPP TS 29.219: Policy and Charging Control: Spending limit reporting over Sy reference point (Release 11.3)
- 3GPP TS 29.229: Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 8)
- 3GPP TS 29.273: Evolved Packet System (EPS); 3GPP EPS AAA interfaces (Release 12.6)
- 3GPP TS 32.240: Charging architecture and principles (Release 8)
- 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging applications (Release 8)
- 3rd Generation Partnership Project 2 (3GPP2) technical specifications:
 - 3GPP2 X.S0013-012-0: Service Based Bearer Control — Stage 2
 - 3GPP2 X.S0013-013-0: Service Based Bearer Control — Tx Interface Stage 3
 - 3GPP2 X.S0013-014-0: Service Based Bearer Control — Ty Interface Stage 3

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

Oracle Communications Policy Management System

Topics:

- *Elements of the Oracle Communications Policy Management Solution.....25*
- *Multimedia Policy Engine Devices.....27*
- *Multi-Protocol Routing Agent Devices.....29*
- *Subscriber Profile Repository.....31*
- *Configuration Management Platform System.....31*
- *Network Configuration Management Platform.....35*
- *About Specialized Communications Protocols...40*
- *Overview of Main Tasks.....41*

This chapter provides an overview of the Policy Management system and its components. The major components include:

- The Oracle Communications Policy Management Configuration Management Platform (CMP) system controls MPE devices and associated applications.
- The Multimedia Policy Engine (MPE) device manages multiple network-based client sessions.
- The Multi-Protocol Routing Agent (MRA) device maintains bindings that link subscribers to Multimedia Policy Engine (MPE) devices.
- The Oracle Communications Policy Management Network Configuration Management Platform (NW-CMP) is the tiered network approach to the Policy Management system.

Elements of the Oracle Communications Policy Management Solution

The major elements of a Policy Management network are as follows:

- Oracle Communications Policy Management Multimedia Policy Engine (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. MPE devices communicate with clients using Diameter application interfaces, and can communicate with an online charging system (OCS) directly using an Sy interface. MPE devices can send Short Message Service (SMS) or Simple Mail Transfer Protocol (SMTP) notifications to subscribers, and analytics data stream (ADS) information, as a series of policy event records (PERs), to third-party systems for analysis. The Policy Management network scales by adding additional MPE devices. See *Policy Wizard Reference* for information on how to create, organize, and manage policies and the elements they control.
- Subscriber Profile Repository (SPR) — Contains subscriber or subscription information. MPE devices can operate with either the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) product or a third-party SPR system. The communication protocol can be Sh or Lightweight Directory Access Protocol (LDAP). The ESPR product supports a RESTful application programming interface (API) to provisioning and OCS systems.
- Diameter Routing Application — In a large Policy Management network implementation, Oracle Communications Policy Management Policy Front End (also known as MRA) or Oracle Communications Diameter Signaling Router (DSR) systems, operating either statelessly (statically) or statefully (dynamically), communicate with clients, distributing and load-balancing sessions between pools of MPE devices. DSR systems are multi-application Diameter routing agents that can support segmented Policy Management networks. A large Policy Management network scales by adding additional MRA and MPE devices.
- Oracle Communications Policy Management Configuration Management Platform (CMP) — Provides the policy console. The CMP system contains a centralized database of policy rules, policy objects, and network objects. Carriers can exchange database information in eXtensible Markup Language (XML) format with office support or back-office support systems (OSS/BSS). A system can communicate Policy Management network management information with network management stations (NMSs) using Simple Network Management Protocol (SNMP).
- Notification Server—Provides a way to generate custom notifications to available web services. Notifications are generated by a new policy action. The destination, content and attributes of the notification are configurable by the operator and allow for flexible notifications within a HTTP request message.

Note: Notification servers are only available when SMPP or XML modes are enabled. See [CMP Modes](#) for details.

Policy Management applications execute on a range of hardware platforms:

- Oracle Server X5-2 rack-mount servers (RMSs)
- Hewlett-Packard (HP) G6, G7, Gen 8, and Gen 9 RMS and c-Class blade servers

On all the hardware platforms with the exception of HP G6, Policy Management applications can execute as virtual machines within a network functions virtualization (NFV) infrastructure.

Figure 1: The Policy Management Solution and MPE Devices shows how the Policy Management solution fits into and interacts with other elements of a wireless network.

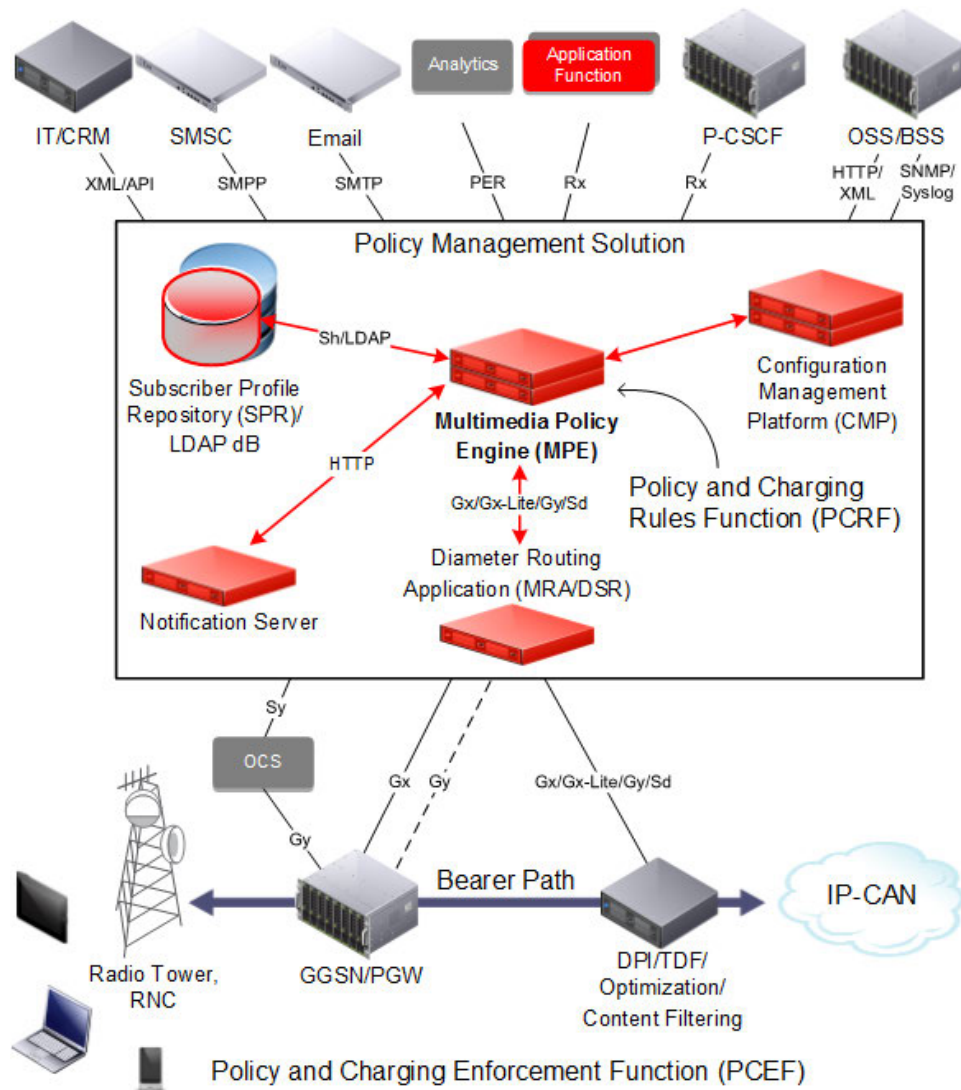


Figure 1: The Policy Management Solution and MPE Devices

Policy Management systems support both IPv4 and IPv6 addressing for signaling networks or peer connections. You can configure any or all signaling interfaces for IPv4 or IPv6.

In addition to signaling interfaces and networks, Policy Management systems allow for hardware platform management through out-of-band remote access to individual devices, hardware enclosure on-board administrators, and enclosure switches. The platform management network is called the Integrated Lights-out Management (iLO) network, and operates independently of the Policy Management applications running on individual devices. The iLO network allows for access across devices restarts, which is needed for maintenance activities such as installations and upgrades.

Note: For support purposes, the iLO addresses must be remotely accessible.

The Product Management and Configuration (PM&C) application, configured on Policy Management devices during initial hardware installation, provides system-level management functions at specific sites. The PM&C application supports platform-related maintenance, software installation, provisioning,

and upgrades. PM&C uses an internal control network (IntCtrl) with internal, non-routable addresses. The PM&C application is independent of, but required for, the Policy Management application.

Note: Refer to the Tekelec Platform PMAC documentation for more information: *PM&C Incremental Upgrade*, *PM&C Disaster Recovery*, and *Oracle Communications Policy Management Bare Metal Installation Guide*.

Multimedia Policy Engine Devices

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). It fully supports all 3GPP Release 7, 8, 9, and 10 policy and charging control (PCC) interfaces. The MPE device includes a simple, powerful, and flexible policy rules engine. The policy rules engine operates on triggers from any interface or from internal timers; evaluates conditions; and then performs appropriate actions. 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
- How applications and subscribers are treated

Refer to *Policy Wizard Reference* for information on how to create, organize, and manage policies and the elements they control.

Figure 2: Diameter Interfaces to the MPE Device shows the various interfaces to external devices and functions supported by an MPE device. These interfaces include the following:

- A Policy and Charging Enforcement Function (PCEF) receives and processes requests to start new sessions for subscribers. Examples of PCEFs include a Gateway GPRS Support Node (GGSN), a Packet Data Network Gateway (PGW), and a High-Speed Gateway (HSGW). MPE devices act as servers for PCEFs, using the Diameter Gx and Gxx interfaces to:
 - Receive requests for policy decisions
 - Send those policy decisions, as PCC rules, to PCEFs for implementation
 - Remove PCC rules from PCEFs
 - Receive traffic plane events from PCEFs

(Additionally, gateways can communicate with online charging systems using the Diameter Gy interface, or offline charging systems using the Diameter Rf interface.) When a PCEF initiates a Gx session, it is assigned to an MPE device. Sessions for other Diameter applications, such as Gxa, Rx, and Gx Lite, that must reference the Gx session have their initial requests correlated to the same MPE device that hosts the Gx session.

- An Application Function (AF) is a network element offering applications that require dynamic policy or charging control over the IP Connectivity Access Network (IP-CAN) user plane. An example of an AF is a Proxy Call Session Control Function (P-CSCF) device. MPE devices act as servers for AFs, using the Diameter Rx interface, to obtain dynamic session information and to send IP-CAN specific information and notifications about bearer-level events. When an AF initiates an Rx session, it is correlated to the same MPE device that hosts the Gx session for that subscriber

based on the IP address, which must be globally unique and routable. (If a correlated Gx session cannot be found, the request is rejected with an error code.)

- A Traffic Detection Function (TDF) permits, gates, shapes, or redirects service traffic. An example of a TDF is a deep packet inspection (DPI) device. MPE devices act as servers for TDFs, using the Diameter Sd or Gx Lite interfaces, to receive requests for policy decisions; to send those policy decisions, as PCC rules, to TDFs for implementation; to remove PCC rules from TDFs; and to receive traffic plane events from TDFs. When a TDF initiates an Sd or Gx Lite session, it is correlated to the same MPE device that hosts the Gx session for that subscriber based on the IP address. (If a correlated Gx session cannot be found, the request is rejected with an error code.)
- A Bearer Binding and Event Reporting Function (BBERF) maps a PCC rule to an IP-CAN bearer. Examples of BBERFs are serving gateways (SGW) and HSGWs. MPE devices act as servers for BBERFs, using the Diameter Gxx interface, to receive requests for policy decisions; to send those policy decisions, as PCC rules, to BBERFs for implementation; to remove PCC rules from BBERFs; and to receive traffic plane events from BBERFs. When a BBERF initiates a Gxx session, it is correlated to the same MPE device that hosts the Gx session for that subscriber based on the IMSI. If a correlated Gxa session cannot be found, an MPE device is assigned for the session and the request is processed.
- A Subscriber Profile Repository (SPR) contains subscriber or subscription information. MPE devices act as clients for SPRs, using the Diameter Sh interface, to retrieve subscriber profiles and to register for notification of changes to a subscriber's profile. MPE devices support the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application.
- A directory services database provides distributed directory information, such as user account IDs, email and equipment addresses, and phone numbers, over an IP network. MPE devices communicate with directory servers using the Lightweight Directory Access Protocol (LDAP).
- In support of voice roaming, the S9 Diameter application installs PCC rules generated in a home public land mobile network (HPLMN) into a visited PLMN (VPLMN) and report the events that may occur in the VPLMN to the HPLMN. When an AF is in the VPLMN, The Diameter Rx protocol is used over the S9 interface to exchange service session information from the visited PCRF to the home PCRF.
- An Online Charging System (OCS) calculates charges against a prepaid account for an event and returns information on how long the subscriber can use the service; this can affect, in real time, the service rendered. MPE devices communicate with OCSes using the Diameter Sy interface. (By contrast, an Offline Charging System (OFCS) calculates charges for a service to an account, and does not affect, in real time, the service rendered.) MPE devices act as clients for OCSes, using the Diameter Sy interface, to retrieve subscriber policy counters and policy counter statuses and to register for notification of changes to a subscriber's policy counters.
- The Multi-Protocol Routing Agent (MRA) (also referred to as the Policy Front End) is an optional product deployed in a large Policy Management network that maintains bindings between subscribers and MPE devices. MPE devices communicate with MRAs as proxy Diameter Routing Agents, so they exchange Diameter messages. For more information on the MRA product, refer to *Policy Front End Wireless User's Guide*.
- The CMP system is required to configure, manage, and provision MPE devices. MPE and CMP devices communicate using a proprietary protocol.

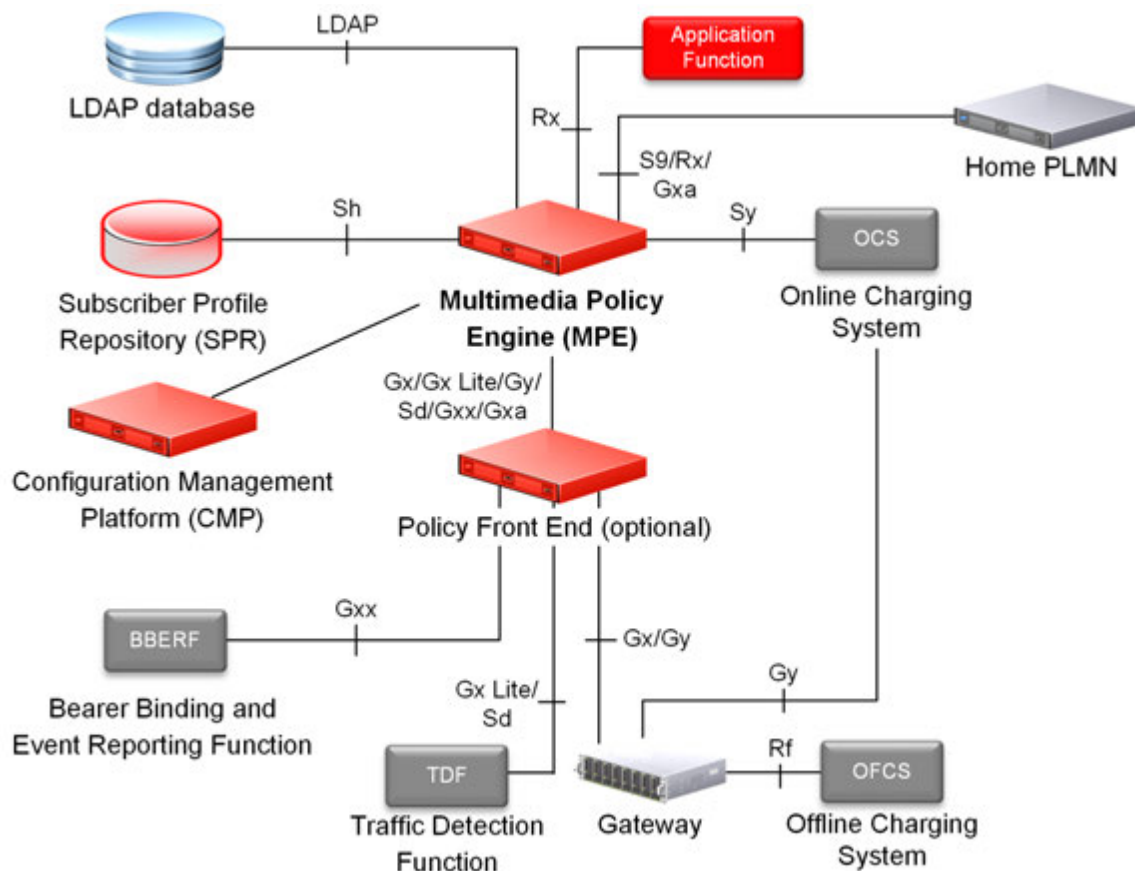


Figure 2: Diameter Interfaces to the MPE Device

Each active MPE device establishes a connection to data sources (such as SPRs and LDAP servers). An MPE device can establish connections to multiple data sources, prioritized as primary, secondary, and tertiary. Each data source can also be configured with a primary and secondary connection. The MPE device uses the highest priority connection available.

MPE and MRA devices implement a load-shedding mechanism to protect themselves during times of severe overload. The devices enter a "too busy" state when the amount of queued traffic exceeds a predefined threshold. While in this state of busyness, requests may be responded to with Diameter TOO_BUSY result codes or silently discarded.

Multi-Protocol Routing Agent Devices

The Multi-Protocol Routing Agent (MRA) (also known as the Policy Front End) is a product deployed in a Policy Management network that maintains bindings that link subscribers to Multimedia Policy Engine (MPE) devices.

An MRA device ensures that all of a subscriber's Diameter sessions established over the Gq, Ty, Gx, Gxx, Gx Lite, Sh, Sy, Rx, S9, and Sd reference points reach the same MPE device when multiple and separately addressable MPE clusters are deployed in a Diameter realm.

An MRA device implements the proxy (PA1 variant) DRA functionality whereby all Diameter Policy and Charging Control (PCC) application messages are proxied through an MRA device.

When an MRA device receives a request for a subscriber for which it has a binding to an MPE device, it routes that request to an MPE device. If an MRA device does not have a binding, it queries other MRA devices in the Policy Management network for a binding using the proprietary Distributed Routing and Management Application (DRMA) protocol. If another MRA device has the binding, the MRA device routes the request to it. If no other MRA device has a binding, the MRA device that received the request creates one.

An MRA device can route requests across multiple MRA clusters within the Policy Management network. Multiple MRA clusters can be deployed in the same domain, (or realm), interconnected as Diameter peers. Each MRA cluster is responsible for a set, or pool, of MPE clusters as a domain of responsibility. Each MRA cluster is a peer with the MPE clusters in its domain of responsibility. The following diagram shows a typical MRA configuration.

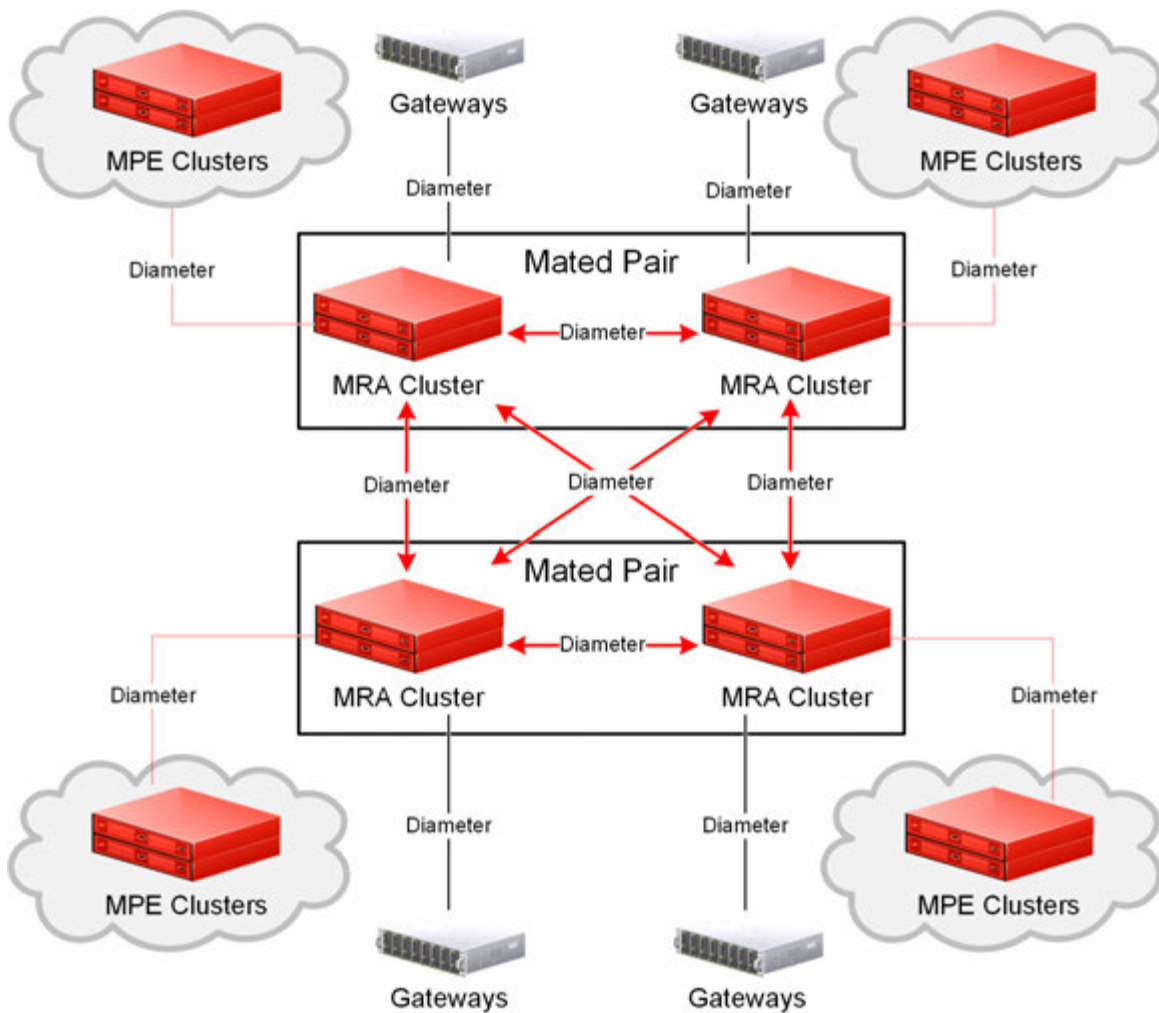


Figure 3: Typical MRA Network

Subscriber Profile Repository

A Subscriber Profile Repository (SPR) database provides a scalable, consolidated database back-end for subscriber and profile data that can be leveraged across the Oracle Communications product portfolio. An SPR can utilize multiple application front-ends with the database.

Policy Management supports the following SPR systems:

- Oracle Communications Subscriber Database Management (SDM) database
- Oracle Communications User Data Repository (UDR) database
- Oracle Communications Enhanced Subscriber Profile Repository (ESPR)
- Third-party SPR system

Currently, Oracle Communications User Data Repository (UDR) supports the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application, a function used for the storage and management of subscriber policy control and pool data. UDR uses XML-REST and XML-SOAP interfaces for creating, retrieving, modifying, and deleting subscriber and pool data.

Refer to the documentation for your specific SPR system for more detailed information.

Configuration Management Platform System

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

- Configuration and management of MPE devices
- Configuration and management of MRA devices
- Configuration of connections to Subscriber Profile Repository (SPR) servers
- Definition of network elements
- Management and deployment of policy rules
- Management 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

Specifications for Using the CMP System

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

- | | |
|---------------------|---|
| Web Browsers | <ul style="list-style-type: none"> • Mozilla Firefox® release 10.0 or later • Google Chrome version 20.0 or later |
|---------------------|---|

Monitor	Resolution of 1024 x 768 or greater
----------------	-------------------------------------

Logging In

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

Before logging in, you need to know the following:

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

Note: The profile **admin** has full access privileges and is the assumed profile used in all procedures described in this document. The default password for the **admin** profile 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.

Logging In to a Standby or Secondary-Site CMP System

Most of the procedures in this document begin with you logged in to the active server of the primary CMP system. A few procedures require you to log in to the active server of a secondary CMP system, and it is also possible to log in to the standby server of a CMP cluster. The functions available on other servers are limited.

- If you log in to the standby server of a primary CMP cluster, the work area displays the prompt:
Warning: This server you signed in is the Primary Standby Server.
- If you log in to the active server of a secondary CMP cluster, the work area displays the prompt:
Warning: This server you signed in is the Secondary Active Server.
- If you log in to the standby server of a secondary CMP cluster, the work area displays the prompt:
Warning: This server you signed in is the Secondary Standby Server.

In all cases, you are limited to the **Platform Setting** functions: **Platform Configuration Settings** and **Topology Settings**. Status information for all other servers is not available and is displayed as **out-of-service**.

GUI Overview

You interact with the CMP system through an intuitive and portable graphical user interface (GUI) supporting industry-standard web technologies (the SSL family of secure communication protocols, HTTP, HTTPS, IPv4, IPv6, and XML). [Figure 4: Layout of the CMP Window – Wireless Mode](#) shows the layout of the CMP GUI.

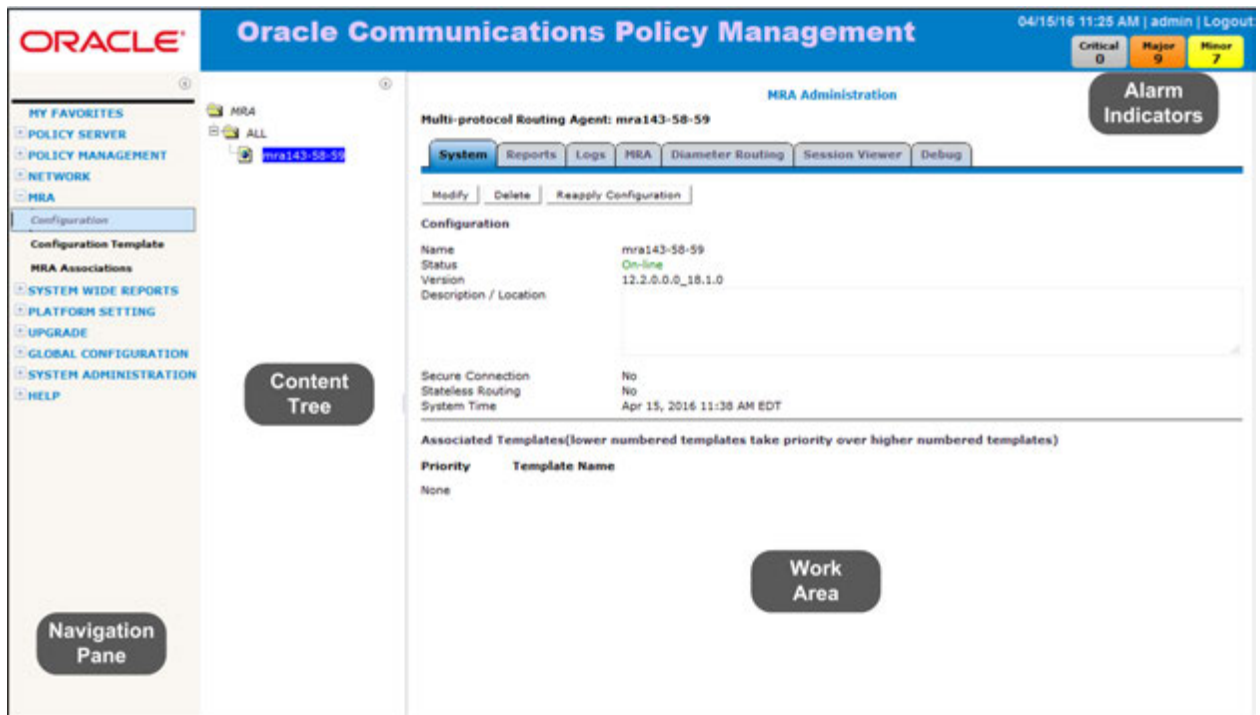


Figure 4: Layout of the CMP Window – Wireless Mode



















The CMP system's window is divided into the following sections:







- 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** 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.
Note: The content tree section is not visible with all navigation selections.
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.
- Work Area** Contains information that relates to choices in both the navigation pane and the content tree. This is the area where you perform all work.
- Alarm Indicators** Provides visual indicators that show the number of active alarms.

CMP Mode Indicator	Indicates the current CMP mode. NW-CMP for Network mode or S-CMP for System mode. If there is not a mode indicated, the mode is CMP .
---------------------------	--

CMP Icons

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

 Add	Use this icon to add an item to a list.
 Calendar	Use this icon to select a date and, in some cases, time.
 Clone	Use this icon to duplicate a selection in a list.
 Critical error	Displays in reports to indicate a critical error during the blade replication process.
 or  Delete	When visible in the work area, selecting the Delete icon deletes an item, removing it from the 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.
 Details	The binoculars icon displays when there is more details for an item.
 Edit	Use this icon to modify a selection in a list.
 External Connection	When visible in the work area, indicates which server currently has the external connection (the active server).
 Gear	The gear icon displays when a policy references another policy or policy group.
 Hide	When visible in the work area, selecting the hide icon removes the item from the current view but does not delete the item. Note: The item is only hidden during the current session. The item will be visible the next time a user logs into the CMP system.
 Manual	Displays when a field is configured by the user. Hover over this icon to see the name of the device.
 Major error	Displays in reports to indicate a major error during the blade replication process.
 Minor error	Displays in reports to indicate a minor error during the blade replication process.
 or  Up/Down	The up and down arrow icons are displayed when you can change the sequential order of items in a list.
 Left/Right	The left and right arrow icons are displayed when it is possible to move an item from one list to another.
 OK status	Displays in reports to indicate that the blade replication process completed without error.

 Remove	Removes an item from the group. The item is still listed in the ALL group and any other group that has an association with the item. For example, if you remove MPE device PS_1 from policy server group PS_Group2, PS_1 still displays in the ALL group.
 Selection	This icon occurs in the Policy Wizard. The icon is used to select conditions and actions to add to a policy rule.
 Synch broken	When visible in the Upgrade Manager, indicates that the CMP system does not have current information on a server.
 Template	Displays when a field is configured by template. Hover over this icon to see the name of the template. Click the icon to view the template.
 Virtual Machine	Displays when a Policy Management application is running on a virtual machine (VM).
 View Cart	Displays the list of configurable objects selected for the Export action.

Shortcut Selection Keys

The CMP interface 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, press the Ctrl key as you click each item.

Network Configuration Management Platform

The Oracle Communications Policy Management Network Configuration Management Platform provides centralized management for systems containing multiple CMP servers.



Restriction: The use of this function is restricted to specific environments and should not be enabled without authorization.

This configuration is a tiered configuration that uses two types of CMP servers:

- Network Configuration Management Platform (NW-CMP)
- System Configuration Management Platform (S-CMP)

The NW-CMP server manages the entire system by managing one or more S-CMP servers. The NW-CMP sends configuration updates to the S-CMP servers and the S-CMP configures MPE and MRA devices.

The NW-CMP server configures Network tier objects. Examples of network tier objects are policies, network elements, and configuration templates. After the network tier objects are configured on the NW-CMP, the objects are distributed to S-CMP servers. On the S-CMP the network tier objects can be

associated with MRA or MPE servers. Network tier objects cannot be created, modified, or deleted on S-CMP servers.

The S-CMP servers configure system tier objects. System tier objects are MPE and MRA devices. These objects are used to apply configurations to individual servers. The MPE and MRA configurations can change individual server configuration parameters or associate network tier objects with an MPE or MRA device. [Figure 5: Policy Management Network Configuration Management Platform](#) shows the structure of a Network Configuration Management Platform system.

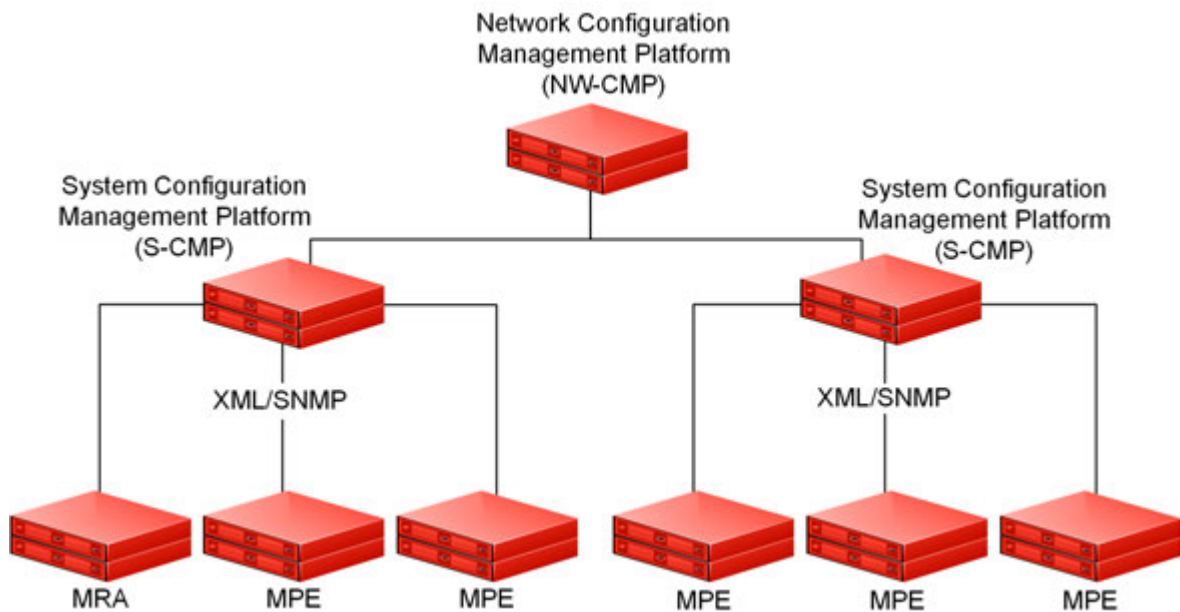


Figure 5: Policy Management Network Configuration Management Platform

Device Configuration in a Network CMP

Configuration of MPE and MRA servers in a tiered CMP configuration can be done manually or with configuration templates. In a manual configuration, the Network tier objects are created on the NW-CMP server and then associated with individual MPE or MRA servers using S-CMP servers. While the manual configuration method takes advantage of the network-wide configuration capability, it requires significant configuration of individual servers and can have consistency problems.

Using configuration templates is a more efficient and consistent method of configuring MPE and MRA servers across the entire CMP system. Since configuration template objects are configured at the Network tier, all configuration templates are created and distributed by an NW-CMP server. Configuration templates are only viewable on S-CMP servers. When using configuration templates, the configuration of parameters and the association of configuration objects are consistent across all devices in the CMP system. After a configuration template is created on the NW-CMP server, the template is distributed to all S-CMP servers and is available for configuring individual servers.

It is recommended that a global configuration template is created for each server type. The global configuration template is then distributed from the NW-CMP server to all S-CMP servers. Then the global template is associated with the appropriate server. This results in a single global configuration template object used network-wide on all servers of the same type. Since all the servers are associated with the same global objects, applying a configuration change from the NW-CMP server becomes as

simple as making a change either in a configuration template or in another global object (such as a policy) referenced by this configuration template. Any change to the configuration template is immediately propagated from the NW-CMP server through the S-CMP servers to all associated servers.

To simplify the association of a configuration template to devices, virtual configuration templates can be used. A Virtual Configuration template is a configuration template that consists of a reference to a standard configuration template. Any place the virtual configuration template is used, it is replaced by the definition of the standard configuration template. The virtual configuration template can make changes to configuration of servers as easy as changing the virtual configuration template reference from one standard configuration template to another standard configuration template.

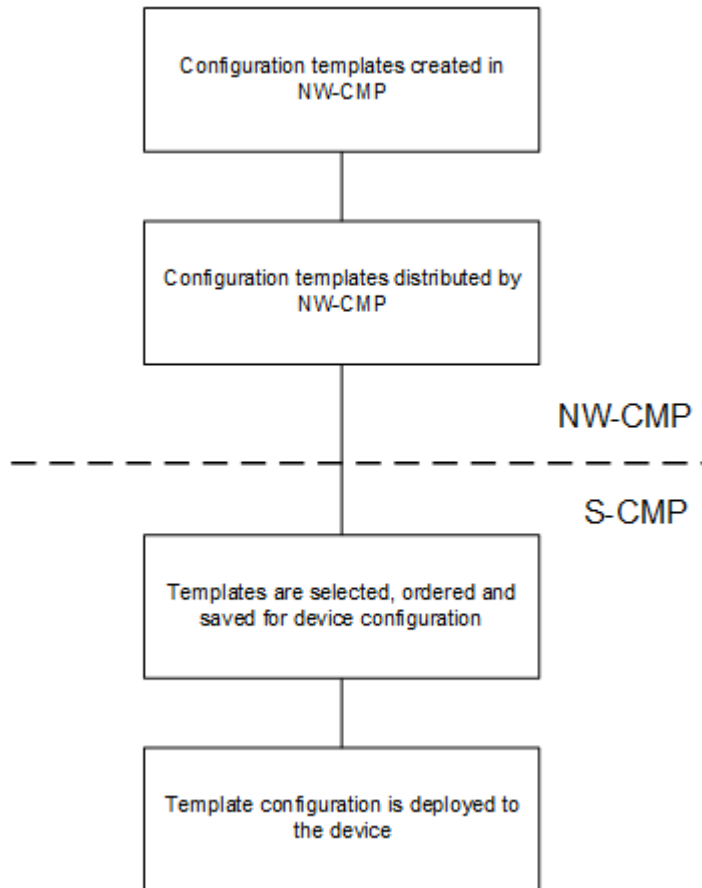


Figure 6: Device Configuration Flow Using Configuration Templates

Network CMP Tier Capabilities

In a tiered CMP system, most menu items are available on both the NW-CMP or S-CMP. However, some menu items are hidden in the navigation pane, depending on the server. For example, when logged into an NW-CMP server, only the **KPI Dashboard** and **Alarms** reports are available in the **System Wide Reports** section. But, when logged into an S-CMP, all reports are visible in the **System Wide Reports** section.

Table 1: Top Level Objects by Management Tier lists the tiers (NW-CMP or S-CMP) where top level objects are configured.

Table 1: Top Level Objects by Management Tier

Top Level Object	Location in UI	Tier
Application	Policy Server > Applications	NW-CMP
AVP Definition	Policy Server > Custom AVP Definitions	NW-CMP
Charging Server	Policy Server > Charging Servers	NW-CMP
Configuration Template	Policy Server > Configuration Templates MRA > Configuration Templates	NW-CMP
Match List	Policy Server > Match Lists	NW-CMP
MPE	Policy Server > Configuration	S-CMP
MPE Group	Policy Server > Configuration	S-CMP
Notification Server	Policy Server > Notification Server	NW-CMP
MRA	MRA > Configuration	S-CMP
MRA Group	MRA > Configuration	S-CMP
S-CMP	S-CMP > Configuration	NW-CMP
S-CMP Group	S-CMP > Configuration	NW-CMP
Network Element	Network > Network Elements	NW-CMP
Network Element Group	Network > Network Elements	NW-CMP
Policy	Policy Management > Policy Library	NW-CMP
Policy Group	Policy Management > Policy Library	NW-CMP
Policy Table	Policy Management > Policy Table Library	NW-CMP
Policy Template	Policy Management > Template Library	NW-CMP
Policy Checkpoint	Policy Management > Policy Checkpoint/Restore	NW-CMP
Tier	Subscriber > Tiers	NW-CMP
Entitlement	Subscriber > Entitlements	NW-CMP
Retry Profile	Policy Server > Retry Profiles	NW-CMP

Top Level Object	Location in UI	Tier
Serving Gateway/MCC-MNC Mapping	Policy Server > Serving Gateway/MCC-MNC Mapping	NW-CMP
Time Period	Policy Server > Time Periods	NW-CMP
LI Mediation Functions	Policy Server > LI Mediation Functions	NW-CMP
Traffic Profile	Policy Server > Traffic Profiles	NW-CMP
Traffic Profile Group	Policy Server > Traffic Profiles	NW-CMP
Monitoring Key	Policy Server > Monitoring Key	NW-CMP
Roaming Profiles	Policy Server > Roaming Profiles	NW-CMP
Protocol Timer Profiles	Policy Server > Protocol Timer Profiles	NW-CMP
Custom Vendors	Policy Server > Custom Vendors	NW-CMP
Quota Conventions	Policy Server > Quota Conventions	NW-CMP
Quota Passes	Policy Server > Quota Conventions > Passes	NW-CMP
Quota Plans	Policy Server > Quota Conventions > Plans	NW-CMP
User	System Administrator > User Management	NW-CMP
User Role	System Administrator > User Management	NW-CMP
User Scope ¹	System Administrator > User Management	NW-CMP
External Authentication	System Administrator > User Management	NW-CMP
Global Configuration	Global Configuration > Global Configuration Settings	S-CMP
Mode Settings	HELP > About	NW-CMP

¹ Since MPEs/MRAs are managed in S-CMP, users can associate MRA/MPE groups to a scope in S-CMP, while they cannot associate NE groups to a scope. NE groups can only be associated to a scope in NW-CMP.

About Specialized Communications Protocols

The Oracle Communications Policy Management system supports a variety of specialized communications protocols.

About RADIUS Protocol

The RADIUS (Remote Authentication Dial-In User Service) networking protocol supports Authentication, Authorization, and Accounting (AAA) management for users. One of the Internet Engineering Task Force (IETF) standards, RADIUS is a client/server protocol that manages network access.

The RADIUS protocol uses access credentials (like a username and password) to authenticate and authorize (via a RADIUS server) a user's or an equipment's access to the requested network. After the access request is accepted, an `Accounting Start` message is transmitted by the network access server (NAS) to the RADIUS server to indicate the start of the user's or equipment's network access.

When the user or equipment closes the network session, the NAS sends an `Accounting Stop` message to the RADIUS server including information for billing, like usage time and packets/data transferred.

The Policy Management system uses the RADIUS protocol to connect PGW-to-DPI and subscriber profile repositories.

About Diameter Protocol

The Diameter networking protocol supports Authentication, Authorization, and Accounting with Secure Transport (AAAS) management for users and equipment. One of the Internet Engineering Task Force (IETF) standards, Diameter Base protocol implements a peer-to-peer architecture where a host acts either as a client or a server depending on its deployment within the network.

The Diameter protocol defines Diameter messages that send commands or deliver notifications to other Diameter-enabled devices.

The Policy Management system uses Diameter interfaces (for example, Gx and Rx) to connect to many of its components and with components outside of the system. See [Figure 2: Diameter Interfaces to the MPE Device](#) for the Diameter-specific interfaces.

See [Related Publications](#) for a list of supported IETF Diameter specifications.

About TACACS Plus Protocol

The Cisco-developed TACACS+ (Terminal Access Controller Access-Control System Plus) networking protocol supports remote authentication and related services for networked access control through a centralized server.

Overview of Main Tasks

The major tasks involved in using MPE devices are configuration, defining network elements, defining manageable devices, managing subscribers, and administering authorized CMP users.

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

1. Configure the topology, which defines the addresses and interconnections of Policy Management clusters in your network. These steps are described in [Configuring the Policy Management Topology](#).
2. Configure policy server profiles for MPE devices. This step is described in [Managing Multimedia Policy Engine Devices](#).
3. Configure protocol routing, which enables a Policy Management device to forward requests to other Policy Management devices for further processing. This step is described in [Configuring Protocol Routing](#).
4. Configuring advanced device settings, which include expert settings, service overrides, and load shedding options. This step is described in [Configuring Advanced Device Settings](#).

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. The full set of tasks is as follows:

- Create network element profiles, including protocol options, for each network element with which Policy Management devices interact. This task is described in [Managing Network Elements](#).
- Specify which Policy Management device will interact with which network elements. This task is described in [Managing Multimedia Policy Engine Devices](#) and [Managing Policy Front End Devices](#).
- Define protocol timer profiles, which configure the Diameter response timeout values for specific applications and the different message types within an application. This task is described in [Managing the Protocol Timer Profiles Function](#).
- Define charging servers, which are applications that calculate billing charges for a wireless subscriber. This task is described in [Managing Charging Servers](#).
- Map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs). This task is described in [Mapping Serving Gateways to MCCs/MNCs](#).
- Configure Policy Front End (also called Multi-Protocol Routing Agent or MRA) devices, which are Policy Management devices that can route requests to MPE or other MRA devices. This task is described in [Managing Policy Front End Devices](#).
- Configure subscriber profile repositories and manage entity states, quotas, pools, tiers, and entitlements. These tasks are described in [About Subscriber Profile Repositories](#) and [Managing Subscribers](#).

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

- View reports on 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. These tasks are described in [System Administration](#).
- Upgrade software using the Upgrade Manager. These tasks are described in [Upgrade Manager](#).

Chapter 3

Configuring the Policy Management Topology

Topics:

- *About the Policy Management Topology.....43*
- *Setting Up the Topology.....54*
- *Modifying the Topology.....74*
- *Configuring SNMP Settings.....81*
- *Platform Configuration Settings.....83*

This chapter describes how to add Policy Management sites and devices to create a Policy Management system. It also describes how to modify the topology, configure SNMP settings and how to configure the global Platform Configuration settings.

About the Policy Management Topology

The first step is to configure a network topology for the Policy Management products (composed of CMP, MPE, and MRA devices). The topology determines the following:

- How clusters are set up
- Which sites are primary and which are secondary
- How configuration data is replicated
- How incidents (events and alarms) get reported to the CMP system or external network management systems.

Figure 7: Example Policy Management Topology illustrates a Policy Management topology consisting of a georedundant primary (CMP Site 1) and secondary (CMP Site 2) CMP cluster, an MRA cluster, and two MPE clusters.

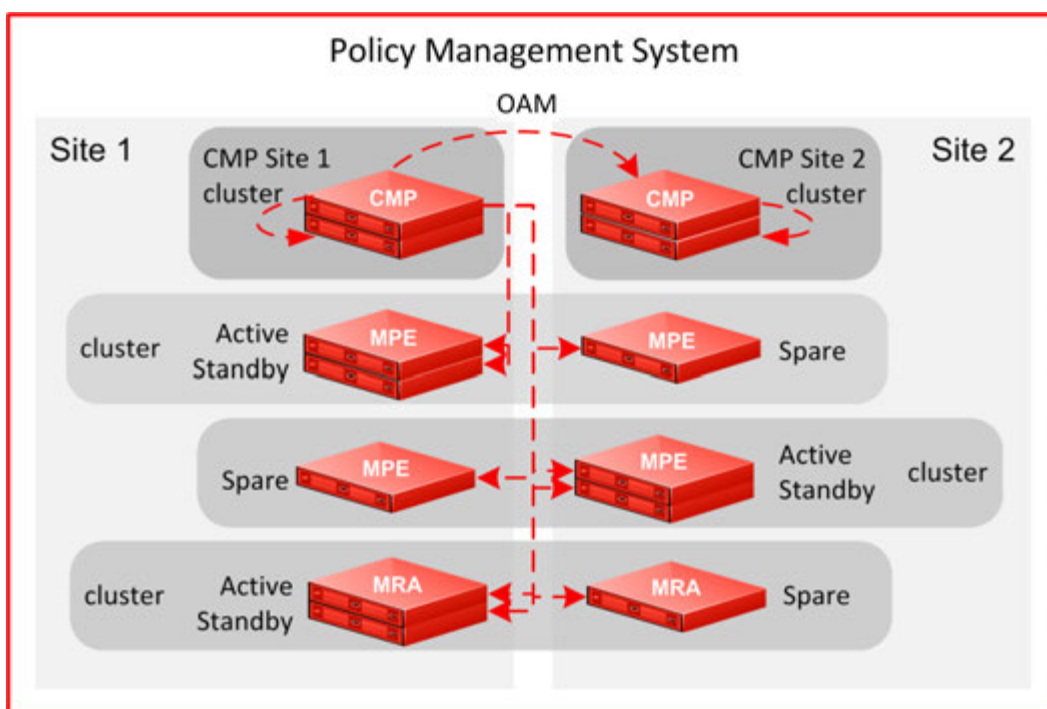


Figure 7: Example Policy Management Topology

As the figure shows:

- The active CMP Site 1 server replicates its data to its standby CMP server and the active CMP server at CMP Site 2.
- In turn, the active CMP Site 2 server replicates its data to its standby CMP server.
- Additionally, the active Site 1 CMP server replicates data to all servers in any MPE and MRA clusters in the topology, regardless of status (active, standby or spare).
- In turn, all servers and clusters merge status, events, alarms, and log data back to the active CMP server at Site 1.

High Availability

Policy Management provides High Availability (HA) to all Policy Management cluster configurations. Policy Management accomplishes HA by using two servers per cluster, an active server and a standby server. For georedundancy, a third, spare server provides additional backup support. Servers are continually monitored by the Communications Core Object Library (COMCOL) in-memory database. As shown in [Figure 8: 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.

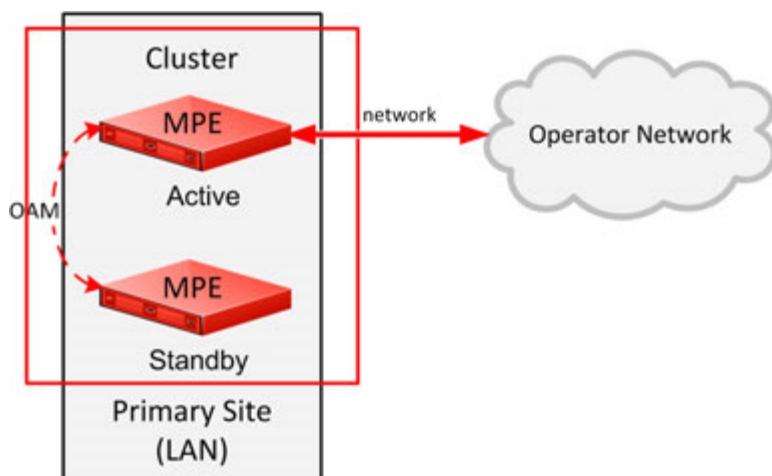


Figure 8: High Availability

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 Operation, Administration, and Management (OAM) network to replicate current state data, monitor server heartbeats, and merge trace logs and alarms.
- Note:** For georedundancy, a third, spare server is part of the cluster and receives replication data and heartbeats.
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. COMCOL database runtime processes on each server constantly monitor server status using heartbeat signals.
 5. If the active server fails, indicated by skipping a succession of heartbeats, COMCOL instructs the standby server to become the active server and take over the VIP address and connections. Because it has been receiving session state data updates through replication, it can assume processing of ongoing sessions, so the failover is automatic and transparent to other components.
 6. If the active server fails, indicated by missing a succession of heartbeats:

The terms active and standby denote roles, or states, that the servers assume, and these roles 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 of the standby server.

When the failed server recovers, it becomes the standby server, and current state data for the cluster is replicated to the server. This behavior is non-revertive; that is, if an active server fails and then recovers, it becomes the standby server, rather than resuming its role as the active server.

Georedundant Spare Servers

As shown in *Figure 9: Clusters with Active, Standby, and Spare Servers*, an MPE or MRA cluster can contain an additional georedundant server, called a spare server. The active server will replicate its database to the standby server as well as the spare server. In this configuration, the standby server is first in line to take over from the active server and the spare is second in line.

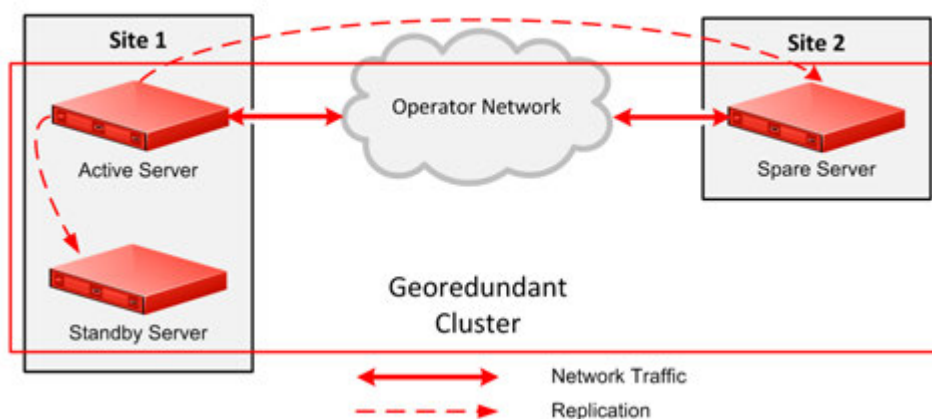


Figure 9: Clusters with Active, Standby, and Spare Servers

Active, standby, and spare servers interoperate as follows:

1. The servers communicate using WAN TCP streams to perform replication, monitor heartbeats, and merge events.
2. The active and standby servers share a common virtual IP (VIP) cluster address to support automatic failover.
3. The spare server has a unique VIP cluster address.
4. The COMCOL state database runtime process constantly monitors the status of all servers.
5. When COMCOL misses the three heartbeats to the spare server, it instructs the spare server to assume the standby role.

The terms active, standby, and spare denote roles, or states, that the servers assume, and these roles can change automatically and at any time based on decisions made by the underlying COMCOL database. If both the active and standby servers become unavailable, the spare server automatically assumes the active role and continues to provide service.

CMP Georedundancy

As shown in [Figure 10: CMP Georedundancy](#), georedundancy is implemented for CMP clusters by pairing a primary site CMP cluster with a secondary site cluster. The active server from the Site 1 CMP cluster will continuously replicate configuration, provisioning, and policy data, using HA, to the active server of the Site 2 cluster.

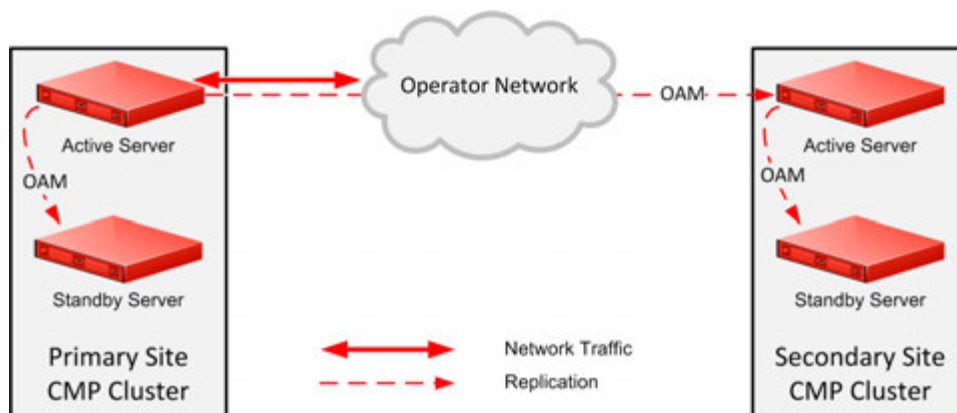


Figure 10: CMP Georedundancy

The secondary cluster does not have to be physically close to the primary cluster. The terms primary and secondary denote roles, or states, that the servers or clusters assume, and you can change these roles manually. If the Site 1 CMP cluster goes offline (as in a disaster scenario), you would log in to the active server of the Site 2 CMP cluster and manually promote this cluster to become the primary (Site 1) CMP cluster to manage the Policy Management network.

Promotion of a CMP cluster is always a manual operation (see [Promoting a Georedundant CMP Cluster](#) for details). The preferred sequence of operation is to first demote the active CMP server at the primary site and then promote the active CMP server at the secondary site, but this is not required. For example, in a disaster-recovery scenario in which the primary site is inaccessible, you can promote the active CMP server at the secondary site immediately. (This may trigger alarms.) The servers record the timestamp when a role is assigned. Policy Management systems recognize the CMP server with the most recent promotion timestamp as the primary cluster (that is, the recognized authority).

In a georedundant topology, c-Class servers (HPE ProLiant BL460c G6/G7/Gen8 servers with a 1x4 mezzanine card) can communicate over a dedicated backup (BKUP) network. This network is set up using the Platform Configuration utility. Refer to *Platform Configuration User's Guide* for detailed information.

Note: CMP servers do not use the replication (REP) network or Differentiated Service Code Point (DSCP) marking.

Georedundancy for Non-CMP Servers

Georedundancy is an optional configuration provided for non-CMP clusters in which the spare server can be located in a separate geographical location, as shown in [Figure 11: Non-CMP Georedundant Configuration](#). The active server replicates state data to the standby and spare servers. If the two servers at one site become unavailable, the third server, located at the other site, automatically becomes the active server and continues to provide service. You can designate sites as primary and secondary.

Georedundancy supports both session-stateful (MPE device) and binding-stateful (MRA device) failover between a pair of geographically separate (or geo-diverse) Policy Management sites. This includes the ability to maintain ongoing sessions and existing bindings that were in progress on the failed site at the time of failure, as well as being able to initiate and handle all new sessions and bindings on the secondary site for the duration of the failure.

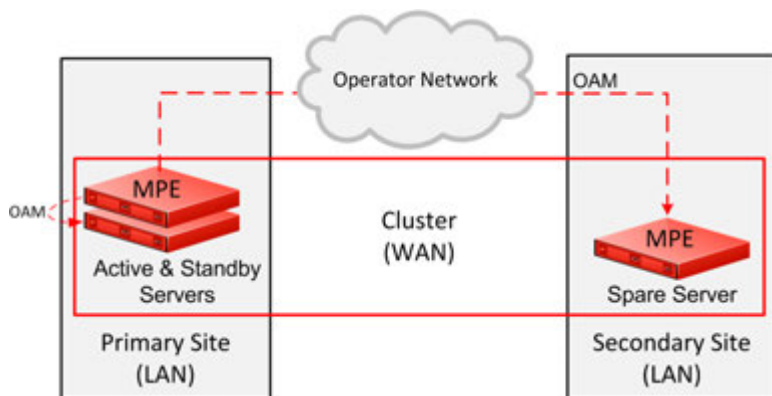


Figure 11: Non-CMP Georedundant Configuration

In a georedundant Policy Management network of two sites, each containing MPE and MRA clusters, client connections are as follows:

- Gateways, content filters, application servers, and other clients are connected to active MRA devices. Each client has a primary connection to the active MRA device at one site and a secondary connection to the active MRA device at the other site. (This is no different than the client connections in a non-georedundant topology.)
- Active MPE devices establish Sh connections, either directly or through Diameter Routing Agents (DRA), to SPRs. The active MPE device at the primary site establishes an Sh connection with a primary IP address, and the spare MPE device at the secondary site establishes an Sh connection with a secondary IP address for use if the spare is promoted to an active role.
- The active MPE devices establish Sy connections, either directly or through DRAs, to online charging servers (OCSs). The active MPE device at the primary site establishes an Sy connection with a primary IP address, and the spare MPE device at the secondary site establishes an Sy connection with a secondary IP address for use if the spare is promoted to an active role.

Using this configuration, if one site fails, clients retain connectivity to the other site, and established sessions remain active. As servers at the failed site recover, they become standby servers, and current state data for the clusters are replicated to them. After the recovered servers are synchronized with the state data of the active servers, they are automatically returned to active roles. This behavior is called revertive which means that if an active server fails and then recovers, it becomes the active server again.

Within a georedundant cluster, the active and standby servers are connected through a local area network (LAN), that uses a single TCP/IP socket connection or stream. The active and spare servers, located at separate sites, are connected through a wide area network (WAN). Since every WAN has distinct bandwidth and packet loss characteristics, the connection can optionally be configured to use up to eight streams to maintain throughput in cases of network congestion or packet loss.

Primary and Secondary Sites

In the Policy Management topology architecture, primary refers to the preferred option for sites, servers, and connections. Under normal conditions, for any cluster, a server at the primary site is the active server that services traffic or manages the Policy Management network. All clients and gateways are connected to this primary site.

MPE and MRA clusters can be dispersed between a primary site and a secondary site. Secondary refers to the georedundant backup site, server, and connection. This dispersal mates the primary and secondary sites together. (In contrast, CMP clusters are paired, not geographically dispersed.) In normal, non-failure conditions, all traffic and active sessions are handled by the active MPE device at the primary site. The standby and spare MPE devices do not receive any live traffic load, but both hold an up-to-date copy of the active session state data at all times (replicated using High Availability).

If for some reason the active server at a primary site can no longer provide service, the cluster fails over to the standby server at the primary site. The server assuming the service becomes the active server.

If and only if no servers are available at an MPE or MRA primary site, the cluster fails over to the secondary site, and a spare server takes over as the active server in the cluster and provides service. When one of the servers at the primary site is able to provide service, then the active status reverts back to the server at the primary site. (In contrast, CMP failover is manual.)

You configure primary and secondary sites as initial states. After MPE and MRA clusters are in operation, failover from a primary site to a secondary site, if necessary, is automatic. (In contrast, CMP failover is manual.)

The spare MPE device at the secondary site does not share the VIP address that is shared between the active and standby MPE devices at the primary site. This means that active MRA devices must support a secondary IP address for each MPE cluster in a georedundant topology. If both the active and standby MPE devices at the primary site become unavailable, and the spare MPE device is promoted to active status, it assumes the Diameter Identity (host name and realm name) of the MPE cluster, and requires active MRA devices to establish Diameter connections using the secondary IP connection to continue sessions.

It is not meaningful to describe a site as primary except in the context of where the active server of a cluster is located. For example, as shown in [Figure 12: Example of Primary and Secondary Sites](#), you could establish a topology with two sites and two MPE clusters, with the spare server of each cluster located at the other site. In this topology, the primary site of Cluster 1 is also the secondary site of Cluster 2, and vice versa.

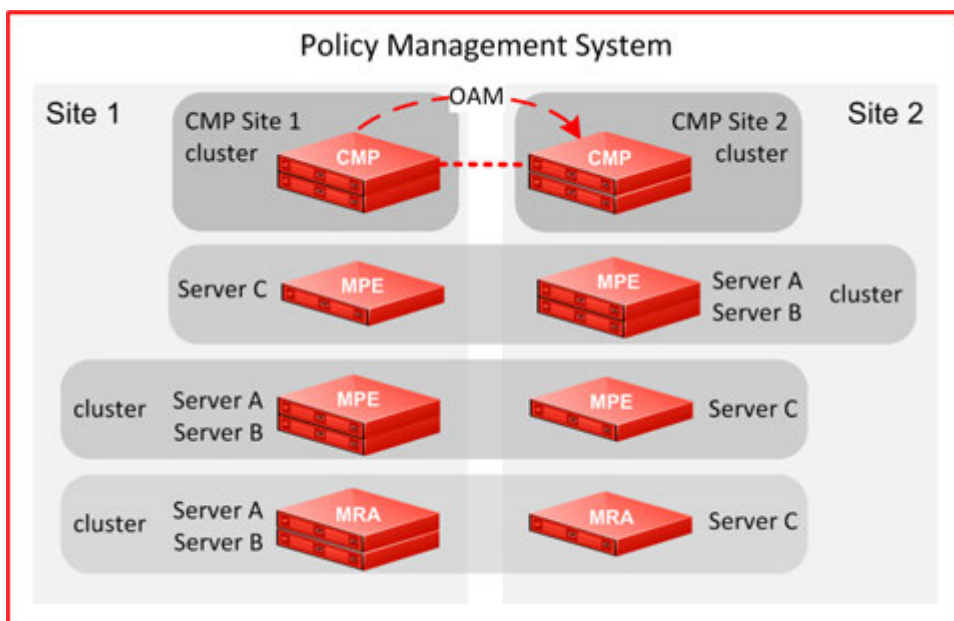


Figure 12: Example of Primary and Secondary Sites

Georedundant Site Preferences

When you configure a georedundant MPE or MRA cluster, you initially set the High Availability site preference to **Normal** to designate that the primary site is preferred. This determines which site contains the active server and initially processes traffic.

After the servers are defined, you can reverse this preference, which designates that the secondary site is preferred. Reversing site preference makes the spare server take over as the active server. The former active and standby servers become the standby and spare servers (which server assumes which role is not determined).

Reversing site preference is useful in situations where you need to troubleshoot, service, upgrade, or replace the active server.

The **Cluster Settings** table on the **Cluster Configuration** page lists information about MPE or MRA cluster preferences under the heading **Site Preference**. A cluster preference is one of the following:

- **Normal**
- **Reverse**
- **N/A** (Not Applicable; CMP clusters cannot be reversed)

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 two servers in the same cluster should ever have the same status.

Note: 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. An active server at the primary site remains active unless it cannot provide service. An active server at the secondary site will remain active as long as no server is available to provide service at the primary site.
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.
Spare	The spare server in an MPE or MRA cluster is the server that is prepared to take over if no server at the primary site is able to provide service. The spare server has the same replicated data as the servers at the primary site. If there is no server available at the primary site, the spare server becomes active and provides service. As soon as a server in the primary site is available to provide service, that server become the active server and the spare server is demoted and reverts to the former status of spare or standby (depending on the availability of the other servers in the cluster).
Out of Service	If a server has failed and is unavailable to assume any of the other roles, then the status is out of service. A server is reported as out of service if the CMP system can reach the server, but the software service on the server is down.
No Data	The CMP system cannot reach the server. This status value provides backward compatibility with previous Policy Management releases. It can be observed during the upgrade process.

Policy Management Network Segmentation

A Policy Management network supports multiple MRA clusters operating as two mated pairs. For larger carrier networks, you can assemble a Policy Management network consisting of multiple independent segments, using Oracle Communications Diameter Signaling Router (DSR) systems to route traffic, both directly and indirectly, between MRA systems. In addition to supporting larger carrier networks, a segmented Policy Management network also isolates faults within one segment.

Figure 13: Segmented Policy Management Network shows an example of a high-capacity, segmented Policy Management network. Each segment is self-contained, including a mated pair of independent MRA clusters, operating in stateful mode, that direct requests to the appropriate MPE device. Each segment can be made fully georedundant. Each segment is served by a mated pair of independent DSR clusters, operating in stateless (static) mode, that direct requests to the appropriate segment. The mated-pair architecture provides redundancy of both systems and connections in the same way as mated MRA pairs. Redundant connections between paired systems allow for both direct and indirect routing.

In a segmented Policy Management network, MPE clients (such as PGWs, HSGWs, and P-CSCFs) are not directly connected to MRA systems, but to DSR systems instead.

The DSR uses a Subscriber Profile Repository (SPR) system to assign subscribers to a specific segment. The DSR system uses the Full Address Based Resolution (FABR) application to use subscriber identification information in initial requests to look up subscriber information in the SPR database and direct the request to the appropriate segment. The DSR system then directly routes subsequent

Configuring the Policy Management Topology

requests associated with a session to the appropriate segment using the destination host information in the request.

The SPR system stores a logical representation of the segment destination in the subscriber record. This allows for changes in the network configuration without requiring changes to the customer provisioning system.

To configure Policy Management network segmentation:

1. Define the DSR systems in the CMP database as network elements. For more information, see [Configuring a DSR Network Element](#).
2. Configure the DSR database to include Policy Management segments, Diameter connections to MRA clusters, DSR pairs, and the appropriate protocols for the FABR application to support. For more information on the DSR product, including configuration and provisioning information, refer to the DSR documentation, available on the Oracle Technology Network site.

For more information on the Oracle Communications Enhanced Subscriber Profile Repository product, including information on configuration and provisioning, refer to the ESPR documentation, available on the Oracle Technology Network site.

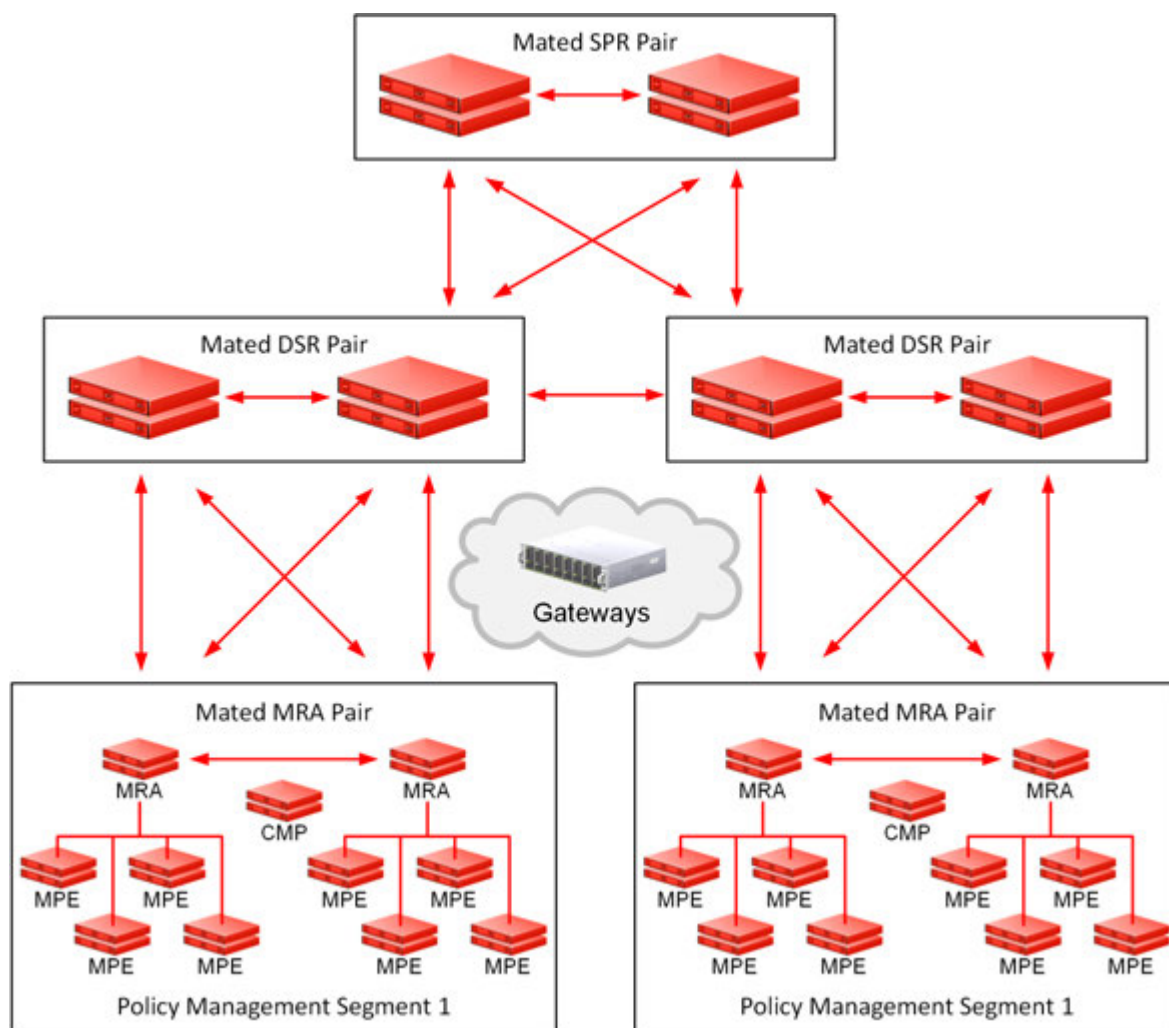


Figure 13: Segmented Policy Management Network

Virtualization

The Policy Management system functions on a range of hardware platforms. Alternatively, you can deploy Policy Management applications in a virtualized hardware environment, as virtual machines (VMs) executing on industry-standard high-volume servers, switches, and storage. VMs are abstracted from host systems (also called compute nodes) and function as if executing alone, although actually multiple VMs execute on a single host system.

The qualified hardware configuration include:

- HP c-Class BL460c Gen8
- Oracle Sun Netra Server X4-2
- Oracle Netra Server X5-2

The qualified VM manager/hypervisor software include:

Oracle Virtual Machine Manager (OVM-M) Oracle Virtual Machine Server (OVM-S)

OpenStack Kernel-based Virtual Machine (KVM)

vSphere VMware ESXi

VMs are deployed within a network functions virtualization (NFV) infrastructure that is hardware independent. The NFV infrastructure includes an environment manager known as a VM manager. The VM manager monitors and manages VMs running on a single host system. The VM manager performs the following management functions:

- Dynamically allocates resources, such as CPU, RAM, and storage among VMs to maximize hardware utilization and balance load
- Instantiates new VMs on demand for increased capacity or in the case of VM failure
- Moves VMs from one host system to another before upgrades or in the case of hardware failure

Figure 14: Virtualization Architecture illustrates the virtualization architecture.

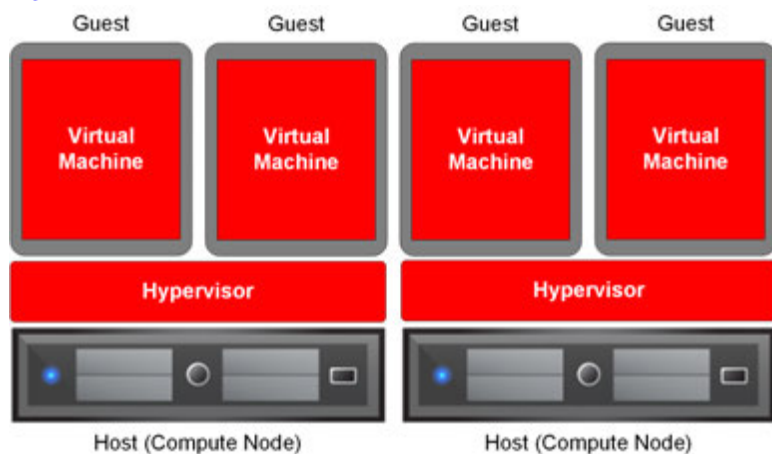


Figure 14: Virtualization Architecture

The virtualized environment supports the multiple network interface connections (OAM, SIG A, SIG B, SIG C, REP, and BKUP) used by Policy Management applications by mapping virtual Ethernet devices as if they were separate physical devices. The virtualized environment supports HA by defining affinity, so that the hypervisor maintains a standby VM on a different host system from the active VM.

Configuring the Policy Management Topology

The virtualized environment calculates key performance indicators (KPI) such as performance, capacity, and load factor by dynamically obtaining the current resources, and the **KPI Dashboard** indicates if a server is running as a virtual machine.

Note: A Policy Management topology can combine both virtual and physical (or bare-metal) machines.

An alternate supported configuration is to include all the Policy Management VMs on a pair of Oracle Netra Server X5-2 RMS host systems or HPE BL380c Gen8 blade host-based systems, executing Oracle Enterprise Linux (OEL) with either the KVM, OVM, or VMware ESXi hypervisor, as a fully functional, high-availability, entry-level, minimal-footprint solution consisting of the following:

- 1 clustered, high-availability (2-server) CMP system
- 2 clustered, high-availability (2-server) MPE systems

Figure 15: Policy Management Minimum Virtualized Topology shows this minimum Policy Management virtualized topology.

Note: The standby VNFC devices reside on separate host systems to ensure proper system function in the event a host system fails.

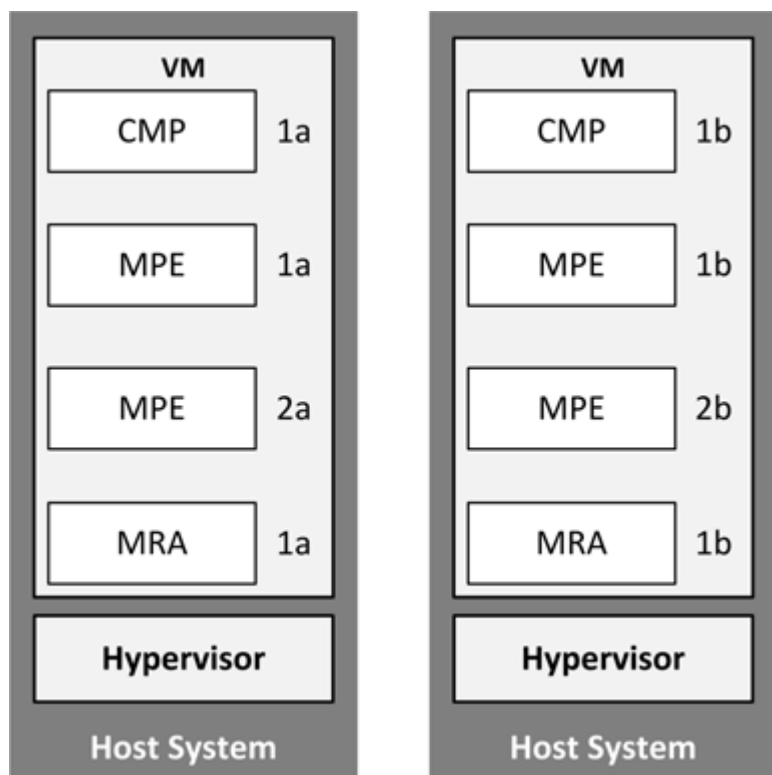


Figure 15: Policy Management Minimum Virtualized Topology

Virtualization is implemented using the Platform Configuration (`platcfg`) utility. Refer to *Platform Configuration User's Guide* for detailed information on creating virtual network function components (VNFC) (for example, CMP, MPE, and MRA devices) on a host system.

Once a virtualized host system is implemented, adding VNFCs to the Policy Management system is as simple as adding a server. See *Setting Up the Topology* for details.

Setting Up the Topology

Topology configuration consists of defining Policy Management sites and clusters, including their addresses and hierarchy. You can add MPE and MRA 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.
 - a. You start to build a topology by logging in to the active CMP server at the primary site.
 - b. Configure the CMP cluster settings. See [Setting Up a CMP Cluster](#) for details.
 - c. The settings are replicated (or pushed) to the standby CMP server. Together, the two servers form a primary, or Site 1, CMP cluster. This is the primary CMP site cluster for the whole topology network.

Note: The primary site cannot be deleted from the topology.

2. (Optional) Use the primary CMP cluster to configure a secondary, or Site 2, CMP cluster.

Note: A secondary CMP cluster can provide georedundancy.

3. Configure non-CMP (MPE and MRA) clusters. See [Setting Up a Non-CMP Cluster](#) for details.

Enter MPE and MRA cluster settings on the active CMP server on the primary site.

Note: You can define the topology before defining the servers themselves.

After defining the topology, the configuration information is replicated as follows:

1. The CMP system replicates the topology configuration, including the cluster settings, to active, standby, and (if present) spare servers using the OAM network. These servers form an MPE or MRA cluster based on the topology configuration.
 2. Active servers communicate with standby servers using LAN connections over the OAM network. Active servers communicate with spare servers using WAN connections over the OAM, SIG-A, SIG-B, or REP network.
 3. Active and standby servers share a virtual IP (VIP) cluster address to support automatic failover. (If present, the spare server has a unique VIP address.)
 4. If present, the spare server has a unique VIP address.
 5. The COMCOL database runtime process constantly monitors the status of the servers in each cluster. If an active server in a cluster fails, the standby server takes over and becomes the active server. In a georedundant topology, if both the active and standby servers in a cluster fail, COMCOL instructs the spare server to take over and become the active server.
4. (Optional) For georedundancy, configure additional sites for MPE and MRA clusters.

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

Note: In a georedundant topology, HP ProLiant BL460 G6 servers (with a 1x4 mezzanine card) can communicate over a dedicated backup (BKUP) network. However, for Policy Management devices, only backup of CMP systems is typical.

Setting Up a CMP Cluster

To set up a CMP cluster:

1. Log in to the CMP server.
2. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens; the initial group is **All Clusters**.

If a primary cluster is not yet defined, you are prompted: Initial Configuration Detected. Please add CMP Site 1 Cluster.
3. From the content tree, select the **All Clusters** group.
The **Cluster Configuration** page opens.
4. Click **Add CMP Site1 Cluster**.
The **Topology Configuration** page opens. The cluster name and application type are fixed.
5. Select the **HW Type** from the list.
Available options are:
 - **C-Class** (default) – HP ProLiant BL460G6/G7/G8 server
 - **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460G6/G7/G8
 - **NETRA** – Sun Netra Server X3-2, Oracle Sun Netra Server X4-2, or Oracle Netra Server X5-2
 - **RMS** (rack-mounted server) – HP ProLiant DL360G6/G8 or HP ProLiant DL380 G6/G8 server
 - **VM** (virtual machine)
6. If you selected **HW Type** of **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**, enter the **General Network - VLAN IDs**.
Enter the **OAM**, **SIG-A**, and (optionally) **SIG-B** virtual LAN (VLAN) IDs.
VLAN IDs are in the range 1–4095. The default values are:
 - **OAM VIP** and server IP – 3
 - **SIG-A VIP** – 5
 - **SIG-B VIP** – 6
7. (Required) To enter up to two **OAM VIP** (one IPv4 and one IPv6) addresses, click **Add New VIP**.
The **New OAM VIP** dialog appears:
 - a) Enter the **OAM VIP** address and the **Mask**.
This is the IP address the CMP server uses to communicate with a Policy Management cluster.

Note: Enter the address in the IPv4 standard dot format and the subnet mask in CIDR notation from 0–32, or IPv6 standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128.
 - b) Click **Save**.
The **OAM VIP** address and **Mask** are saved.
 - c) Repeat this step for a second **OAM VIP** address, if needed.
8. (Optional) To enter up to four **Signaling VIP** addresses, click **Add New VIP**.
The **New Signaling VIP** dialog appears:
 - a) Enter the **Signaling VIP** address and the **Mask**.

Configuring the Policy Management Topology

This is the IP address the CMP server uses to communicate with an external signaling network.

Note: Enter the address in the IPv4 standard dot format and the subnet mask in CIDR notation from 0–32, or IPv6 standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128.

- b) Select the **Interface** from the list.

Available options are:

- **SIG-A**
- **SIG-B**

- c) Click **Save**.

The **Signaling VIP** address and **Mask** are saved.

- d) Repeat this step for any additional **Signaling VIP** addresses, as needed.

The screenshot displays the 'Cluster Settings' page for a 'Wireless CMP Cluster'. It is organized into three main sections: 'Cluster Settings', 'Server-A', and 'Server-B'.

Cluster Settings:

- General Settings:**
 - Name: CMP Site1 Cluster
 - Appl Type: CMP Site1 Cluster
 - HW Type: VM
 - OAM VIP: <OAM VIP1><10.148.235.89/22>
 - Signaling VIPs: (empty field)

Server-A:

- General Settings:**
 - IP: <IP1><10.148.235.90>
 - IP Preference: IPv4
 - HostName: ahatemCMP09
 - Forced Standby: No
 - Status: active

Server-B:

- General Settings:**
 - IP: <IP1><10.148.253.201> (with 'Add New IP', 'Edit', and 'Delete' buttons)
 - IP Preference: ☒ IPv4 ☐ IPv6
 - HostName: sw_reg_2201 (with 'Load' button)
 - Forced Standby: Automatically set

At the bottom of the page, there are 'Save' and 'Cancel' buttons.

Figure 16: Cluster Settings Page for Wireless CMP Cluster

9. To configure **Server-A** (the first server of the cluster which will be the initial active server), click **Add New IP**.

The **New IP** dialog appears:

- a) (Required) Enter the **IP** address for the server.

Up to two IP addresses can be entered (one IPv4 and one IPv6). Use the IPv4 standard dot-formatted IP address string and the IPv6 standard 8-part colon-separated hexadecimal string format.

- b) Select the **IP Preference** to specify the preferred IP address format: **IPv4** or **IPv6**.

The server will preferentially use the IP address of the selected format.

Note: The following restrictions:

- If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 is not available.
- If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 is not available.

- c) Click **Save**.

The **IP** address for Server A is saved.

10. To enter a second **IP** address, repeat the step.

Note: Up to two IP addresses can be entered (one IPv4 and one IPv6).

11. (Required) Enter the **HostName** for the server.

This must exactly match the host name provisioned for this server (that is, the output of the Linux command `uname -n`).

- If the server has a configured server IP address, click **Load** to retrieve the remote server host name. If retrieval fails, you must enter the host name.

12. Select to force the server into **Forced Standby**.

Note: The state 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.

13. Click **Save**.

A confirmation message displays.

14. Click **OK**.

A restart message displays.

15. Click **OK**.

The active server restarts.

16. Log back in to the CMP server.

17. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

The **Cluster Configuration** page opens.

18. From the content tree, select the **CMP Site 1 Cluster**.

The **Topology Configuration** page opens.

19. Select **Modify Server-B**, and enter the appropriate information for the secondary server of the cluster.

20. Click **Save**.

The CMP cluster topology is defined.

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

After you define the primary (Site 1) CMP cluster, you can repeat this procedure to define a georedundant secondary (Site 2) CMP cluster. See [Setting Up a Georedundant Site](#) before adding a secondary CMP cluster.

Note: Backup traffic between CMP sites can be sent between servers over the BKUP network.

Setting Up a Non-CMP Cluster

Before defining a non-CMP cluster, ensure the following:

- The server 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 server IP connection is active.
- The server software is running on at least one server.

To setup a non-CMP cluster:

1. On the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The content tree displays a list of server groups; the initial group is **All Clusters**.
2. Click **Add MPE/MRA Cluster**.
The **Topology Configuration** page opens.
3. In the **Cluster Settings** section of the page:
 - a) (Required) Enter the **Name** for the cluster.
Enter up to 250 characters, excluding quotation marks (") and commas (,).
 - b) Select the **Appl Type** from the list.
Available options are:
 - **MPE** (default)
 - **MRA**
 - c) Select the **HW Type** from the list.
Available options are:
 - **C-Class** (default) – HP ProLiant BL460 G6/G7/G8 server
 - **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 G6/G7/G8
 - **NETRA** – Sun Netra Server X3-2, Oracle Sun Netra Server X4-2, or Oracle Netra Server X5-2
 - **RMS** (rack-mounted server) – HP ProLiant DL360 G6/G8 or HP ProLiant DL380 G6/G8 server
 - **VM** (virtual machine)
 - d) (Required) To enter up to two **OAM VIP** (one IPv4 and one IPv6) addresses, click **Add New VIP**.
The **New OAM VIP** dialog appears.
 1. Enter the **OAM VIP** addresses and the **Mask**.
This is the IP address the CMP server uses to communicate with a Policy Management cluster.

Note: Enter the address in the IPv4 standard dot format and the subnet mask in CIDR notation from 0–32, or IPv6 standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128.

2. Click **Save**.

The **OAM VIP** address and **Mask** are saved.

- e) If needed, repeat the process for the second OAM VIP.
f) (Optional) To enter up to four **Signaling VIPs** addresses, click **Add New VIP**.

The signaling VIP is the IP address a PCEF device uses to communicate with the cluster. A non-CMP cluster supports redundant communication channels, named SIG-A and SIG-B, for carriers who use redundant signaling channels.

The **New Signaling VIP** dialog appears.

1. Enter the **Signaling VIP** address and the **Mask**.

This is the IP address the CMP server uses to communicate with an external signaling network.

Note: Enter the address in the IPv4 standard dot format and the subnet mask in CIDR notation from 0–32, or IPv6 standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128.

2. Select the **Interface** from the list.

Available options are:

- **SIG-A**
- **SIG-B**

3. Click **Save**.

The **Signaling VIP** address and **Mask** are saved.

- g) Repeat the process for any remaining Signaling VIPs.
h) If the hardware type is **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**, configure the **General Network** settings:

1. Enter the **OAM VLAN ID**.

The default value is **3**.

2. Enter the **SIG-A VLAN ID**.

The default value is **5**.

3. (Optional) Enter the **SIG-B VLAN ID**.

The default value is **6**.

Virtual LAN (VLAN) IDs are in the range of 1–4095.

- i) If the hardware type is **C-Class** or **C-Class(Segregated Traffic)**, for the **User Defined Network**, enter the **REP VLAN ID**.

Virtual LAN (VLAN) IDs are in the range of 1–4095.

4. To configure Server-A, in the **Server-A** section of the page:

- a) (Required) To enter the **IP** address, click **Add New IP**.

The **Add New IP** dialog appears.

1. Enter the **IP** address in either IPv4 or IPv6 format.

The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

2. Select the **IP Preference**.

Either **IPv4** or **IPv6**. If **IPv6** is selected, the server will preferentially use the IPv6 address for communication.

Note: If neither an IPv6 OAM IP nor a static IP address is defined, **IPv6** cannot be selected. If neither an IPv4 OAM IP nor a static IP address is defined, **IPv4** cannot be selected.

- b) Enter the **HostName** of the server.

This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

Note: If the server has a configured server IP, you can click **Load** to retrieve the remote server host name. If the retrieve fails, you must enter the host name.

- c) Select **Forced Standby** to put Server-A into forced standby status.

By default, Server-A will be the initial active server of the cluster.

5. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster. Server-B is defined for the cluster.
6. Click **Save**.
A confirmation message displays.
7. Click **OK**.

The cluster is defined. To set up another cluster, repeat the steps.

Figure 17: Sample MRA Cluster Topology Configuration shows the configuration for a georedundant (two-site) MRA cluster, using SIG-B for a replication network and OAM for the backup heartbeat network, with eight WAN replication streams.

Configuring the Policy Management Topology

Topology Settings

- All Clusters
 - CMP Site1 Cluster
 - Doc-Cluster-1
 - Doc-Cluster-2
 - Doc-MRA-Cluster-2
 - MPE09

General Settings

Name: MRA-112
 Appl Type: MRA
 HW Type: C-Class
 OAM VIP:
 Signaling VIPs: <Signaling VIP1><10.113.4.163/22><SIG-A>
 Add New VIP Edit Delete

Network Configuration

General Network

	VLAN ID
OAM	3
SIG-A	5
SIG-B	6

Server-A

Delete Server-A

General Settings

IP: <IP1><10.113.5.133>
 Add New IP Edit Delete

IP Preference: ☒ IPv4 ☐ IPv6

HostName: Host225
 Load

Forced Standby: ☐

Server-B

Delete Server-B

General Settings

IP: <IP1><10.113.8.125>
 Add New IP Edit Delete

IP Preference: ☒ IPv4 ☐ IPv6

HostName: Host299
 Load

Forced Standby: ☐

Save Cancel

Figure 17: Sample MRA Cluster Topology Configuration

Setting Up a Georedundant Site

Note: Sites may only be created when in **Georedundant MPE/MRA/BoD** mode. See [CMP Modes](#) for details.

To set up a georedundant site:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.
2. From the content tree, select the **All Sites** group.
The **Site Configuration** page opens.
3. Click **Create Site**.
The **New Site** page opens.
4. (Required) Enter the **Name** for the site.
Enter up to 35 alphanumeric characters; underscores (_) and hyphens (-) are allowed.
5. Enter the number for **Max Primary Site Failure Threshold**.

If the number of cluster pair failures reaches this threshold, the system generates a trace log entry and a major alarm. A pair failure is recorded when both servers at a primary site are either out of service or in forced standby. The default value is no threshold.

Note: You can optionally enter a number up to the total number of servers provisioned at this site.

6. Select the **HW Type** from the list.

The available options are:

- **C-Class** (default)
- **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
- **NETRA** (for a Netra server)
- **RMS** (for a rack-mounted server)
- **VM** (for a virtual machine)

7. If the hardware type is **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**, configure the **General Network** settings.

Virtual LAN (VLAN) IDs are in the range of 1–4095.

- a) Enter the **OAM VLAN ID**.
- b) Enter the **SIG-A VLAN ID**.
- c) (Optional) Enter the **SIG-B VLAN ID**.

8. If the hardware type is **C-Class** or **C-Class(Segregated Traffic)**, enter the **VLAN ID** for the **User Defined Network**.

Virtual LAN (VLAN) IDs are in the range of 1–4095.

9. Click **Save**.

The CMP database saves the site configuration.

To define multiple sites, repeat the procedure starting at [Step 3](#).

Setting Up a Georedundant Non-CMP Cluster

Note: Georedundancy requires the system to be configured for **Georedundant MPE/MRA/BoD** mode.

Before defining a cluster, ensure the following conditions are met:

- The server 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 server IP connection is active.
- The server application is running on at least one server.

A georedundant non-CMP cluster is one of the following server types:

- MPE
- MRA

Note: If your system is not set up for georedundancy, see [Setting Up a Non-CMP Cluster](#).

To setup a georedundant non-CMP cluster:

1. On the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The content tree displays a list of server groups; the initial group is **All Clusters**.
2. Click **Add MPE/MRA Cluster**.
The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.
3. In the **Cluster Settings** section of the page:

- a) (Required) Enter the **Name** for the site.
Enter up to 35 alphanumeric characters; underscores (_) and hyphens (-) are allowed.

- b) Select an **Appl Type**.

The available options are:

- **MPE** (default)
- **MRA**

- c) Select the **Site Preference**.

Available options are **Normal** (default) or **Reverse**.

- d) Select the type of **DSCP Marking** (Differentiated Services Code Point) for replication traffic.

The valid code points are:

assured forwarding	AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43
class selector	CS1, CS2, CS3, CS4, CS5, CS6, CS7
expedited forwarding	EF
default for no marking	PHB (None)


For information on DSCP marking, see [Setting Up a Non-CMP Cluster](#).

- e) Select the **Replication Stream Count**.

This is the number of redundant TCP/IP socket connections (streams) to carry replication traffic between sites. Up to 8 streams can be configured. The default value is 1 stream.

- f) Select a **Replication & Heartbeat** network to carry inter-site replication and heartbeat traffic.


- **None** (default)
- **OAM**
- **SIG-A**
- **SIG-B**
- **REP**

A warning icon () indicates that you cannot select a network until you define a static IP address on all servers of both sites.

- g) Select a **Backup Heartbeat** network to carry inter-site backup heartbeat traffic.

Available options are:

- **None** (default)
- **OAM**
- **SIG-A**
- **SIG-B**
- **REP**

A warning icon () indicates that you cannot select a network until you define a static IP address on all servers of both sites.

4. In the **Primary Site Settings** section of the page:

- a) Select the **Site Name** from the list.

Configuring the Policy Management Topology

Select **Unspecified** (default) or the **Name** of a previously defined site. You can assign multiple clusters to the same site.

Note: If you select **Unspecified**, you create a non-georedundant site and cannot add a secondary site.

- b) To import the **HW Type** and **VLAN ID** settings from the from the selected site, select **Use Site Configuration**.

When **Use Site Configuration** is selected, the **HW Type** and **VLAN ID** settings become read only.

To edit the fields, uncheck the **Use Site Configuration**.

Note: If **Unspecified** is selected for the site name, the **Use Site Configuration** option becomes unavailable.

- c) Select the **HW Type** from the list.

Available options are:

- **C-Class** (default) – HP ProLiant BL460G6/G7/G8 server
- **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460G6/G7/G8
- **NETRA** – Sun Netra Server X3-2, Oracle Sun Netra Server X4-2, or Oracle Netra Server X5-2
- **RMS** (rack-mounted server) – HP ProLiant DL360G6/G8 or HP ProLiant DL380 G6/G8 server
- **VM** (virtual machine)

- d) (Required) To enter up to two **OAM VIP** (one IPv4 and one IPv6) addresses, click **Add New VIP**.

The **New OAM VIP** dialog appears.

1. Enter the **OAM VIP** address and the **Mask**.

This is the IP address the CMP server uses to communicate with a Policy Management cluster.

Note: Enter the address in the IPv4 standard dot format and the subnet mask in CIDR notation from 0–32, or IPv6 standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128.

2. Click **Save**

The **OAM VIP** address and **Mask** are saved. Repeat the process for the second OAM VIP.

- e) (Optional) To enter up to four **Signaling VIPs** addresses, click **Add New VIP**.

The signaling VIP is the IP address a PCEF device uses to communicate with the cluster. A non-CMP cluster supports redundant communication channels, named SIG-A and SIG-B, for carriers who use redundant signaling channels.

The **New Signaling VIP** dialog appears.

1. Enter the **Signaling VIP** address and the **Mask**.

This is the IP address the CMP server uses to communicate with an external signaling network.

Note: Enter the address in the IPv4 standard dot format and the subnet mask in CIDR notation from 0–32, or IPv6 standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128.

2. Select the **Interface** from the list.

Available options are:

- **SIG-A**
- **SIG-B**

3. Click **Save**.

The **Signaling VIP** address and **Mask** are saved.

- f) If the hardware type is **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**, configure the **General Network** settings:

1. Enter the **OAM VLAN ID**.

The default value is **3**.

2. Enter the **SIG-A VLAN ID**.

The default value is **5**.

3. (Optional) Enter the **SIG-B VLAN ID**.

The default value is **6**.

Note: Virtual LAN (VLAN) IDs are in the range of 1–4095.

- g) If the hardware type is **C-Class** or **C-Class(Segregated Traffic)**, for the **User Defined Network**, enter the **REP VLAN ID**.

Note: Virtual LAN (VLAN) IDs are in the range of 1–4095.

5. To configure Server-A, in the **Server-A** section of the page:

- a) (Required) To enter the **IP** address, click **Add New IP**.

The **Add New IP** dialog appears.

1. Enter the **IP** address in either IPv4 or IPv6 format.

This is the IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

2. Select the **IP Preference: IPv4 or IPV6**.

The server will preferentially use the IP address in the specified format for communication.

- If neither an IPv6 OAM IP nor a static IP address is defined, **IPv6** cannot be selected.
- If neither an IPv4 OAM IP nor a static IP address is defined, **IPv4** cannot be selected.

- b) Enter the **HostName** of the server.

This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

- If the server has a configured server IP, you can click **Load** to retrieve the remote server host name. If the retrieve fails, you must enter the host name.
- c) Select **Forced Standby** to put Server-A into forced standby.
By default, Server-A will be the initial active server of the cluster.
- d) In the **Path Configuration** section, to add a **Static IP**, click **Add New**.
The **New Path** dialog appears.

Note: If an alternate replication path and secondary HA heartbeat path is used, a server **Static IP** address must be entered in this field.

1. Enter a **Static IP** address and **Mask**.
2. Select the **Interface**:

- **SIG-A**
- **SIG-B**
- **REP**
- **BKUP**

Note: If the hardware type is **C-Class(Segregated Traffic)** or **NETRA**, the **BKUP** network is available.

6. (Optional) To configure Server-B, in the **Server-B** section of the page:

- a) (Required) To enter the **IP** address, click **Add New IP**.

The **Add New IP** dialog appears.

1. Enter the **IP** address in either IPv4 or IPv6 format.

The IP address of the server. For an IPv4 address, enter it in the standard IP dot-format. For an IPv6 address, enter it in the standard 8-part colon-separated hexadecimal string format.

2. Select the **IP Preference**: **IPv4** or **IPv6**.

The server will preferentially use the IP address of the specified format for communication.

- If neither an IPv6 OAM IP nor a static IP address is defined, **IPv6** cannot be selected.
- If neither an IPv4 OAM IP nor a static IP address is defined, **IPv4** cannot be selected.

- b) Enter the **HostName** of the server.

This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

- If the server has a configured server IP, you can click **Load** to retrieve the remote server host name. If the retrieve fails, you must enter the host name.
- c) Select **Forced Standby** to put Server-B into forced standby.
By default, Server-A will be the initial active server of the cluster.
- d) In the **Path Configuration** section, to add a **Static IP**, click **Add New**.
The **New Path** dialog appears.

Note: If an alternate replication path and secondary HA heartbeat path is used, a server **Static IP** address must be entered in this field.

Configuring the Policy Management Topology

1. Enter a **Static IP** address and **Mask**.
2. Select the **Interface**:

- **SIG-A**
- **SIG-B**
- **REP**
- **BKUP**

Note: If the hardware type is **C-Class(Segregated Traffic)** or **NETRA**, the **BKUP** network is available.

7. Click **Save**.
A confirmation message displays.
8. Click **OK**.
9. If you are setting up multiple clusters, repeat this procedure.

The cluster is defined.

Figure 18: Sample BoD Cluster Site 1 Configuration shows the configuration for a georedundant (two-site) BoD cluster, using SIG-A for a replication network and OAM for the backup heartbeat network.

Cluster Settings

Name	BOD-56-57-55G7	DSCP Marking	AF11
Appl Type	BoD	Replication Stream Count	1
Site Preference	Normal	Replication & Heartbeat	None
		Backup Heartbeat	OAM

Degrade on failure of: ☐ OAM ☐ SIG-A ☐ SIG-B ☐ Both SIG-A and SIG-B

Primary Site Settings

General Settings

Site Name	BOD-Site1
HW Type	HP ProLiant DL360G6/G7
OAM VIP	
Signaling VIPs	<Signaling VIP1><198.51.100.244/24><SIG-A>

Server-A

General Settings	Path Configuration
IP	Static IP
HostName	
Forced Standby	
Status	

Server-B

General Settings	Path Configuration
IP	Static IP
HostName	
Forced Standby	
Status	

Figure 18: Sample BoD Cluster Site 1 Configuration

Secondary Site Settings

General Settings

Site Name

BOD-Site2

HW Type

HP ProLiant DL360G6/G7

OAM VIP

Signaling VIPs

<Signaling VIP1><198.51.100.247/24><SIG-A>

Server-C

General Settings

IP

198.51.100.248

HostName

BOD55

Forced Standby

No

Status

Spare

Path Configuration

Static IP

Figure 19: Sample BoD Cluster Site 2 Configuration

Example: Setting Up Georedundancy

This topic describes how to add a secondary site, Site-2, to a Policy Management topology, and a third server, located at Site-2, to an existing active/standby MPE cluster located at the primary site, Site-1, to create a two-site (Site-1 and Site-2), three-system (active, standby, and spare, or Server-A, Server-B, and Server-C) mated georedundant MPE cluster. If the primary site were to fail, the spare server would assume the active role. The procedure includes recommended verification steps, and refers to tasks described elsewhere.

Note: Before undertaking this procedure, contact My Oracle Support (MOS) for assistance.

Before creating a georedundant cluster, ensure the following:

- All systems in the topology are running the latest Policy Management software
- The new server (Server-C) is of a supported hardware type, and has been delivered with the latest firmware and TPD software pre-installed

Before beginning the procedure, you will need to collect or provide the following information (to collect information, see [Setting Up a Georedundant Non-CMP Cluster](#)).

Tip: This information can be collected at any time before beginning the procedure without interrupting service.

- The names of existing clusters
- Names for the sites (this procedure uses **Site-1** and **Site-2**)
- The maximum primary site failure threshold, to record site failures (0 is recommended)
- The OAM VIP address of the existing Site-1 CMP system and, if applicable, the georedundant CMP system
- (Optional) a designated network path, either OAM, REP, SIG-A or SIG-B, for backup (secondary) HA heartbeats between Site-1 and Site-2
- (Optional) a designated network path, either OAM, REP, SIG-A or SIG-B, for WAN replication traffic between Site-1 and Site-2

- Initial provisioning information for Server-C:
 - A hostname (this procedure uses **Server-C**)
 - For CMP access, an OAM IPv4 or IPv6 address and subnet mask
 - An OAM IPv4/IPv6 default route
 - A list of network time protocol (NTP) server IP addresses
 - A list of domain name system (DNS) server IP addresses
 - VLAN IDs for OAM, REP, SIG-A, and SIG-B network paths
 - For IPv4-based network elements, an IPv4 VIP address and subnet mask on the SIG-A network
 - For inter-topology communication or any IPv6-based network elements, an IPv6 VIP address and subnet mask on the SIG-A network
 - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, an IPv4/IPv6 static address and subnet mask on the REP network
- For each existing HA cluster:
 - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, a VLAN ID for the REP network path
 - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, an IPv4/IPv6 static address and subnet mask on the REP network for Server-A
 - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, an IPv4/IPv6 static address and subnet mask on the REP network for Server-B
 - Verify that firewall rules are correctly provisioned (for more information, see the *Platform Configuration User's Guide*)
- If DSCP marking for WAN replication traffic is used, the type of DSCP marking
- If multi-stream WAN replication traffic is used, the replication stream count

To create a secondary site and a georedundant MPE cluster, follow these steps.



Caution: This procedure interrupts service.

1. Using the Platform Management & Configuration utility, install the MPE application on Server-C. For more information, refer to the PM&C documentation, or contact MOS for support.
2. Using the Platform Configuration utility, provision Server-C with the following configuration information.
For more information, see the *Platform Configuration User's Guide*.
 - a) HostName
 - b) OAM Real IP Address
 - c) OAM Default Route
 - d) NTP Server
 - e) DNS Server A
 - f) DNS Server B (optional)
 - g) DNS Search
 - h) Device
 - i) OAM VLAN Id
 - j) SIG A VLAN Id
 - k) SIG B VLAN Id (optional)

Configuring the Policy Management Topology

3. Using the Platform Configuration utility, export routing configuration information from Server-A or Server-B and import it into Server-C.

For more information, see the *Platform Configuration User's Guide*.

4. Log in to the CMP system, using its OAM VIP address.

Note: Unless otherwise noted, the remaining steps are performed within the CMP system.

5. If this is the first georedundant cluster in your topology, set the CMP system to manage georedundant MPE/MRA/BoD systems.

See [About Mode Settings](#).

On the content tree of the **Topology Configuration** page, the **All Sites** group becomes available.

6. Define the two sites.

See [Setting Up a Georedundant Site](#).

The sites become visible on the **Site Configuration** page.

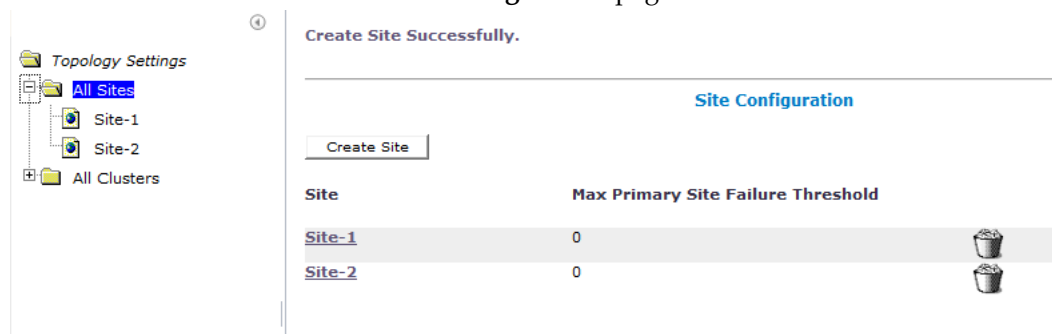


Figure 20: Site Configuration

7. From the content tree, select the **All Clusters** group.
The **Cluster Configuration** page opens, displaying the defined clusters.
8. On the **Cluster Configuration** page, for the MPE cluster you are expanding, click the operation **View**.
The **Topology Configuration** page opens for the MPE cluster.
9. Click **Modify Primary Site**.
The fields in the **Primary Site Settings** section of the page become editable.
10. In the **Primary Site Settings** section of the page:
 - a) In the **Site Name** field, select the primary site name (**Site-1** in this example).
 - b) Confirm the values in the **HW Type** field, **Network Configuration** section, and **Signaling VIPs** field.
 - c) If the REP network is used, in the **User Defined Network** section, enter the VLAN ID for the REP network.
11. In the **Server-A** section of the page:
 - a) Confirm the values in the **General Settings** section.
 - b) In the **Path Configuration** section, click **Add New**, enter the Static IP address and subnet mask for the SIG-A network in the pop-up window, and click **Save**.
 - c) If the REP network is used, repeat [Substep b](#) for the REP network.
12. Repeat [Step 11](#) for Server-B.
The primary site settings are defined; for example:

Primary Site Settings

General Settings

Site Name: Unspecified

HW Type: C-Class

OAM VIP: <OAM VIP1><10.24.252.75/23>

Signaling VIPs: <Signaling VIP1><10.24.252.76/23><SIG-A>

Network Configuration

☐ Use Site Configuration

General Network

OAM: 246

SIG-A: 244

SIG-B: 245

User Defined Network

REP:

Figure 21: Example of Primary Site Settings

13. Click **Save** (at the bottom of the page).
A restart message displays.
 14. Click **OK**.
Server-A restarts. You must now define the Site-2 and Server-C configuration.
 15. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.
 16. From the content tree, select the **All Clusters** group.
The **Cluster Configuration** page opens, displaying the defined clusters.
 17. On the **Cluster Configuration** page, for the MPE cluster you are expanding, click the operation **View**.
The **Topology Configuration** page opens for the MPE cluster.
 18. Click **Modify Secondary Site**.
The fields in the **Secondary Site Settings** section of the page become editable.
 19. In the **Secondary Site Settings** section of the page:
 - a) In the **Site Name** field, select the secondary site name (**Site-2** in this example).
 - b) Confirm the values in the **HW Type** field, **Network Configuration** section, and **Signaling VIPs** field.
 - c) If the REP network is used, in the **User Defined Network** section, enter the VLAN ID for the REP network.
 20. In the **Server-C** section of the page:
 - a) Click **Add Server-C**.
 - b) In the **IP** field, enter the OAM IP address.
 - c) In the **IP Preference** field, enter the preferred IP version, either **IPv4** or **IPv6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an OAM IPv6 IP nor a static IP address defined, the IPv6 radio button cannot be selected here. Similarly, If neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button isn't accessible.
 - d) In the **HostName** field, enter the host name.
 - e) In the **Path Configuration** section, click **Add New**, enter the Static IP address and subnet mask for the SIG-A network in the window, and click **Save**.
 - f) If the REP network is used, repeat [Substep e](#) for the REP network.
- Site-2 and Server-C are defined, and Server-C is placed in Force Standby status; for example:

Configuring the Policy Management Topology

The screenshot displays a configuration window with two main sections: 'Secondary Site Settings' and 'Server-C'.

Secondary Site Settings

- General Settings:**
 - Site Name: Unspecified
 - HW Type: NETRA
 - OAM VIP: <OAM VIP1><10.24.84.15/26>
 - Signaling VIPs: <Signaling VIP1><10.24.84.135/27><SIG-A>
- Network Configuration:**
 - ☐ Use Site Configuration
 - General Network:**

	VLAN ID
OAM	246
SIG-A	244
SIG-B	245

Server-C

- General Settings:**
 - IP: <IP1><10.24.252.90>
 - IP Preference: ☒ IPv4 ☐ IPv6
 - HostName: Server-C
 - Forced Standby: ☐
- Path Configuration:**
 - Static IP: <10.24.248.35/23><SIG-A>

Buttons at the bottom: Save, Cancel.

21. Click **Save** (at the bottom of the page).

A restart message displays.

22. Click **OK**.

Server-A restarts.

Note: The status of Server-C is Out of Service and critical alarm 31283 is raised; this is expected.

23. Click the status of Server-C.

The status changes to **Spare**.

24. Click **Save**.

The configuration is saved.

25. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

The **Cluster Configuration** page opens.

26. From the content tree, select the **All Clusters** group.

The **Cluster Configuration** page opens, displaying the defined clusters.

27. On the **Cluster Configuration** page, for the MPE cluster you are expanding, click the operation **View**.

The **Topology Configuration** page opens for the MPE cluster.

28. Click **Modify Cluster Settings**.

The fields in the **Cluster Settings** section of the page become editable.

29. In the **Cluster Settings** section of the page:

- If DSCP marking is used, in the **DSCP Marking** field, select the type of marking.
- If replication streams are used, in the **Replication Stream Count** field, select the number of streams.
- In the **Replication & Heartbeat** field, select the network used (or **None** to return to the system default).
- If the backup (secondary) heartbeat feature is used, in the **Backup Heartbeat** field, select the network used (or **None** to disable the feature).

30. Click **Save**.

The configuration is saved.

31. Verify the status of Server-C by viewing the cluster.
Server-C is shown as part of the cluster in the Force Standby state with replication on.
32. Use the Alarm History Report and filter in all alarms on the cluster name to verify that no new alarms have been raised.
For more information, see [Viewing the Alarm History Report](#).
Alarm 31102 (DB Replication from a master DB failed) is in the report, but with severity Clear.
33. On Server-C, using the Platform Configuration utility, exchange SSH keys with the other servers of the cluster.
This step is not completed using the CMP software. See the *Platform Configuration User's Guide*.
34. On the CMP system, using the Platform Configuration utility, exchange SSH keys with all other CMP systems in the topology.
This step is not completed using the CMP software. See the *Platform Configuration User's Guide*.
35. Modify the cluster configuration to cancel the Force Standby state of Server-C.
The state of Server-C changes to Spare.
36. Use the **KPI Dashboard** to verify that Server-C is reporting its status as part of the cluster.
For more information, see [KPI Dashboard](#).
Server-C is shown as part of the cluster, in the Spare state.
37. (Optional) Use the **Policy Checkpoint** function to create a policy checkpoint.
Tip: If the function is not available, ensure that the system settings allow policy checkpoints. See [Configuring System Settings](#).
For more information on policy checkpoints, see the *Policy Wizard Reference*.
38. Use the **Data Sources** function to configure routes on Server-C to existing data sources.
For more information, see [Configuring Data Source Interfaces](#).
39. Use the **Topology Settings** function to force Server-A and Server-B to standby status to verify that Server-C is functioning normally:
 - a) Select the MPE cluster and click **Modify Primary Site**.
 - b) In the **Server-A** section of the page, select **Forced Standby**.
 - c) In the **Server-B** section of the page, select **Forced Standby**.
 - d) Click **Save** (at the bottom of the page). You are prompted, `Active server will restart`.
 - e) Click **OK**.
 - f) Use the **System Maintenance** function to verify that Server-C has become the active server.
 - g) Use the **Policy Server Reports** function to verify that Sh connections are active on Server-C.
For more information, see [Data Source Statistics](#).
40. Use the **Topology Settings** function to cancel the Force Standby state of Server-A and Server-B.
On the **System Maintenance** page, the state of Server-C changes to Spare.
Note: Either Server-A or Server-B may assume the Active status. Oracle recommends not attempting to force Server-A back into the Active status, as doing so would interrupt service.

The two sites, and the georedundant MPE cluster, are defined, and the normal function of all servers is verified.

If your topology includes MRA systems, add additional routes on the system to reach Server-C in the case of a cluster restart, and add the georedundant MPE cluster to an MPE pool. For more information, refer to the *Policy Front End Wireless User's Guide*.

Modifying the Topology

After the topology is configured, you can modify the topology to:

- Correct errors
- Add a server to a cluster
- Define new clusters
- Add clusters to an existing site
- Define new sites
- Change which cluster is primary and which secondary
- Put an active server into standby status

Note: You can modify a cluster even if the standby or spare server is offline. However, you cannot modify or delete the active server of a cluster.

Modifying a Georedundant Site

Note: You must enable **Manage Geo-Redundant MPE/MRA/BoD** to create and modify sites within the Policy Management topology. See [CMP Modes](#) for more information.

To modify a georedundant site:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.
2. From the content tree, select the **All Sites** group.
The **Site Configuration** page opens listing all the sites configured in the topology.
3. Select the **Site** you want to modify.
The **Site Configuration** page displays information about the site.
4. Click **Modify**.
The **Modify Site** page opens.
5. Modify site information.

For a description of the fields contained on this page, see [Setting Up a Georedundant Site](#).


6. Click **Save**.

Your changes to the site are saved.

Removing a Site from the Topology

You can only remove a site if the site is not referenced by a Server C-level cluster. When a site is in use by a cluster, you will receive the following message if you try to delete the site: *Site cannot be deleted because it is referred in following clusters: cluster1[, cluster2[, ...]].*

To remove a site from the topology:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.
2. Select the **All Sites** group.
The **Site Configuration** page opens, displaying the configured sites.
3. Delete the site using one of the following methods:
 - From the work area, click  (Delete icon), located to the right of the site.
 - From the content tree, select the site and click **Delete**.

A confirmation message displays.

4. Click **OK**.

The site is removed from the topology.

Modifying a non-CMP Cluster

To modify an non-CMP cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Topology Configuration** page opens.
2. From the content tree, select the **All Cluster** group.
The **Cluster Configuration** page opens, listing the clusters.
3. From the **Cluster Settings** table, click the **View** operation for the cluster you want to modify.
The **Topology Configuration** page opens, displaying information about the cluster.
4. Click the button for the changes you want to make:
 - To modify cluster settings, click **Modify Cluster Settings**.
 - To modify server A, click **Modify Server-A**.
 - To modify server B, click **Modify Server-B**.
 - To delete a server configuration, click the appropriate button to modify the server and then click **Delete**.

See [Removing a Cluster from the Topology](#) for details.

The appropriate section on the **Topology Configuration** page becomes editable.

5. Make changes as required.

You must make changes to each section individually.

- You can remove all servers from a cluster.
- You can select **Forced Standby** on one or more servers in the 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.

6. Click **Save**.
A warning message displays.

7. Click **OK**.

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

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 **All Cluster** group.
The **Cluster Configuration** page opens, listing the clusters.
3. From the **Cluster Settings** table, click the **View** operation for the CMP cluster you want to modify.
The **Topology Configuration** page opens, displaying information about the cluster.
4. Click the button for the changes you want to make:
 - To modify cluster settings, click **Modify Cluster Settings**.
 - To modify server A, click **Modify Server-A**.
 - To modify server B, click **Modify Server-B**.

The appropriate section on the **Topology Configuration** page becomes editable. For information on configurable settings, see [Setting Up a CMP Cluster](#).

5. Make the changes as required.
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.

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

The changes to the CMP cluster are saved. 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 a non-CMP or Secondary Site (Site 2) CMP cluster from the topology.

Note: You cannot remove the (primary) Site 1 CMP cluster from the topology.

Before removing an MPE or MRA cluster from a fully configured system:

- Remove it from the MPE pool on an MRA device, or remove it as a backup MRA device, as appropriate.
- 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 Settings**.

The **Topology Configuration** page opens.

2. From the content tree, select the **All Clusters** group.
The **Cluster Configuration** page opens, displaying the **Cluster Settings** table listing information about the clusters defined in the topology.
3. In the **Cluster Settings**, 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**.
You are prompted: The cluster `cluster_name` was successfully deleted. Go to each server and `su - platcfg -> Policy Configuration -> Cluster Configuration Removal -> Cluster information cleanup`

The cluster is removed from the topology.

After the cluster is removed, use the Platform Configuration (`platcfg`) utility to remove cluster information. For more information, refer to *Platform Configuration User's Guide*.

Reversing Georedundant Cluster Preference

If your system has been configured for georedundancy (that is, **Geo-Redundancy MPE/MRA/BoD** mode is enabled), there can be situations, when you need to change the preference of the servers in a cluster to be active or spare.

To reverse a georedundant cluster preference:

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 **All Cluster** group.
The **Cluster Configuration** page opens, listing the clusters.
3. From the **Cluster Settings** table, click the **View** operation for the cluster you want to modify.
The **Topology Configuration** page opens, displaying information about the cluster.
4. Click **Modify Cluster Settings** to edit the settings.
5. In the **Cluster Settings** section of the page:
 - To set the preference to reverse (where the active Site 1 becomes the inactive site and Site 2 becomes the active site), toggle from **Normal** to **Reverse**.
 - To set the preference to normal (where the active Site 2 becomes the inactive site and Site 1 becomes the active site), toggle from **Reverse** to **Normal**.
6. Click **Save**.

The cluster preferences are reversed.

Demoting a Georedundant CMP Cluster

In a two-cluster CMP topology, you can demote the primary cluster (which is typically the Site 1 cluster) to secondary status. You would do this, for example, prior to performing site-wide maintenance that affects service (such as replacing a server), or if the primary cluster has failed completely and is unreachable.

Note: This is a manual process.

When you demote a CMP cluster, the secondary site (which is typically the Site 2 cluster) can be promoted to the primary site (see [Promoting a Georedundant CMP Cluster](#) for details). This promoted status will persist until you manually demote the new primary site or the primary site fails over for some reason.



Caution: Perform cluster demotion before cluster promotion to avoid having both georedundant clusters active at the same time. Continuous and rapid failovers (flopping back and forth) between georedundant clusters is not recommended and should be avoided. Improper cluster failover can result in loss of data or interruption of network services on the CMP cluster.

To demote a georedundant CMP cluster:

1. Log in to the currently active georedundant CMP cluster:
 - a) From the **Platform Setting** section of the navigation pane, select **Topology Settings**. The **Topology Configuration** page opens.
 - b) From the content tree, select the **All Cluster** group. The **Cluster Configuration** page opens, displaying the **Cluster Settings** table listing information about the clusters defined in the topology.

Note: The name of the primary CMP cluster is marked with (P), and the name of the secondary cluster is marked with (S).

You should see **Operations to View and Demote**.

2. Open a second browser window and log in to the secondary CMP cluster. The page displays the message: This server you signed in is the Secondary Active Server.

Note: The state of the servers of the primary cluster is not available to the secondary active server and appears as **Out-of-Service**.

3. To verify the status of the secondary cluster, on the secondary CMP cluster:
 - a) From the **Platform Setting** section of the navigation pane, select **Topology Settings**. The **Topology Configuration** page opens.
 - b) From the content tree, select the **All Cluster** group. The **Cluster Configuration** page opens, displaying the **Cluster Settings** table listing information about the clusters defined in the topology. You should see **Operations to View and Promote**.



Caution: If you do not see the same information in this step as you did in [Step 2](#), stop this procedure and do not try to change the current active georedundant cluster. Contact My Oracle Support before proceeding.

4. Return to the browser window showing the primary CMP cluster. You should still be on the **Cluster Configuration** page.
5. In the **Cluster Settings** table, in the row listing the primary CMP cluster, click the **Demote** operation. You are prompted: Are you sure you want to demote this Cluster?
6. Click **OK**. The page displays the message: Demote cluster successfully.
7. Log out of the primary CMP system for the cluster you have just demoted. The primary CMP cluster is demoted to secondary status.

After demoting a primary cluster, you must promote the secondary cluster for it to become active. See [Promoting a Georedundant CMP Cluster](#) for detailed information.

Promoting a Georedundant CMP Cluster

Prior to performing this procedure, you must demote the primary active cluster. See [Demoting a Georedundant CMP Cluster](#) for detailed information.

In a two-cluster CMP topology and after demoting the primary cluster, you can promote the secondary cluster (which is typically the Site 2 cluster) to primary active status. You would do this, for example, prior to performing site-wide maintenance that affects service (such as replacing a server) or if the primary cluster has failed completely and is unreachable.

Note: This is a manual process.

When you promote a CMP cluster, the secondary site (which is typically the Site 2 cluster) becomes the primary site. This status will persist until you manually demote the new primary site or the primary site fails over for some reason.



Caution: Perform cluster demotion before cluster promotion to avoid having both georedundant clusters active at the same time. Continuous and rapid failovers (flopping back and forth) between georedundant clusters is not recommended and should be avoided. Improper cluster failover can result in loss of data or interruption of network services on the CMP cluster.

To promote a georedundant CMP cluster:

1. Log in to the secondary CMP cluster:

- a) From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The page displays the message: This server you signed in is the Secondary Active Server.

Note: The state of the servers of the primary cluster is not available to the secondary active server and appears as **Out-of-Service**.

- b) From the content tree, select the **All Cluster** group.
The **Cluster Configuration** page opens, displaying the **Cluster Settings** table listing information about the clusters defined in the topology.

Note: The name of the primary CMP cluster is marked with (S), and the name of the secondary cluster is marked with (S).

For the secondary cluster, you should see **Operations to View and Promote**.



Caution: If you do not see the same information in this step as you did in [Step 2](#), stop this procedure and do not try to change the current active georedundant cluster. Contact My Oracle Support before proceeding.

2. If you have just demoted a primary cluster, wait two minutes.
3. In the **Cluster Settings** table, in the row listing the secondary CMP cluster, click **Promote**.
You are prompted: Are you sure you want to promote this Cluster?
4. Click **OK**.
The page displays the message: Promote cluster successfully.

5. Log out of the CMP system for the cluster you have just promoted.
6. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
7. From the content tree, select the **All Cluster** group.
The **Cluster Configuration** page opens, displaying the **Cluster Settings** table listing information about the clusters defined in the topology.

The newly promoted primary cluster is marked with (P), and the name of the demoted secondary cluster is marked with (S). The old primary cluster may briefly display as off-line.

Note: For the new primary cluster, you should see options to **View** and **Demote**. All functions available for the primary CMP cluster should now appear and be accessible.
8. Wait ten minutes.
9. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
10. From the content tree, select the **All Cluster** group.
The **Cluster Configuration** page opens, displaying the **Cluster Settings** table listing information about the clusters defined in the topology.
11. Verify that both the primary and secondary CMP clusters are available and have the correct status.
The secondary CMP cluster is promoted to primary status.

Changing Server Status to Forced Standby

You can change the status of a server in a cluster to forced standby. A server placed into forced standby status cannot become active. You would do this, for example, to an active server prior to performing maintenance on it.

When you place a server into forced standby, the following actions occur:

- If the server is active, the server is demoted.
- The server will not assume the active role, regardless of its status or the roles of the other servers in the cluster.
- The server continues as part of its cluster and reports its status as **Forced Standby**.
- The server coordinates with the other servers in the cluster to take the role **Standby** or **Spare**.



Caution: If you set all servers in a cluster into forced standby status, you can trigger a site outage.

To change a server into a forced standby status:

1. On the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Topology Configuration** page opens.
2. From the content tree, select the **All Cluster** group.
The **Cluster Configuration** page opens, listing the clusters.
3. From the **Cluster Settings** table, click the **View** operation for the cluster you want to change.
The **Topology Configuration** page opens, displaying information about the cluster.
4. Click **Modify Server-A** or **Modify Server-B** (whichever server needs the status change).
5. Select **Forced Standby**.
6. Click **Save**.

The server status is changed to forced standby.

Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network. You can configure the Policy Management network such that the CMP system collects and forwards all traps, or such that each server generates and delivers its own traps.

Note: SNMP settings configuration must be done on the active CMP server in the primary cluster. A warning displays if the login is not on the active primary CMP system.

To configure SNMP settings:

1. Log in to the CMP system using a **Username** 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. For each **Manager 1-5**, enter a valid host name or an IPv4/IPv6 address.
This field is required for an SNMP Manager to receive traps and send SNMP requests. These fields have the following restrictions:
 - A host name should include only alphanumeric characters.
 - Maximum length is 20 characters.
 - Case insensitive (uppercase and lowercase are treated as the same).
 - This field can contain an IPv4/IPv6 IP address.
 - Port configuration is optional for each manager and it can have a value between 1 and 65535. If this field is left blank, the port defaults to 162.

By default, these fields are blank.
5. Select the **Enabled Versions** from the list:
 - **SNMPv2c**
 - **SNMPv3**
 - **SNMPv2c and SNMPv3 [default]**
6. Select **Traps Enabled** to enable sending SNMPv2 traps.
The default is enabled. Uncheck the check box to disable sending SNMPv2 traps.
Note: To use the **SNMP Trap Forwarding** feature, enable this option.
7. Select **Traps from individual Servers** to enable sending traps from each individual server.
The default is disabled. Uncheck the check box to send traps from the active CMP system only.
Note: To use the **SNMP Trap Forwarding** feature, disable this option.
8. Enter the **SNMPv2c Community Name**.
This is the SNMP read-write community string. This field has the following restrictions:
 - The field is required if SNMPv2c is enabled.

- The name can contain alphanumeric characters and cannot exceed 31 characters in length.
- The name cannot be either **private** or **public**.

The default value is **snmppublic**.

9. Enter the SNMPv3 Engine ID.

This is the configured Engine ID for SNMPv3. This field has the following restrictions:

- The field is required if SNMPv3 is enabled.
- The Engine ID uses only hexadecimal digits (0-9 and a-f).
- The length can be from 10 to 64 digits.

The default value is no value (null).

10. Select the SNMPv3 Security Level (SNMPv3 Authentication and Privacy) from the list:

- **No Auth No Priv** — Authenticate using the **Username**. No Privacy.
- **Auth No Priv** — Authenticate using MD5 or SHA1 protocol.
- **Auth Priv** — [default] Authenticate using MD5 or SHA1 protocol. Encrypt using the AES or DES protocol.

11. Select the SNMPv3 Authentication Type (Authentication protocol for SNMPv3) from the list:

- **SHA-1** — Use Secure Hash Algorithm authentication.
- **MD5** — [default] Use Message Digest authentication.

12. Select the SNMPv3 Privacy Type (Privacy Protocol for SNMPv3) from the list:

- **AES** — [default] Use Advanced Encryption Standard privacy.
- **DES** — Use Data Encryption Standard privacy.

13. Enter the SNMPv3 Username.

This field has the following restrictions:

- The field is required if SNMPv3 is enabled.
- The name must contain alphanumeric characters and cannot exceed 32 characters in length.

The default value is **TekSNMPUser**.

14. Enter the SNMPv3 Password.

This value is the Authentication password for SNMPv3 and is also used for `msgPrivacyParameters`. This field has the following restrictions:

- The field is required if SNMPv3 is enabled.
- The length of the password must be between 8 and 64 characters and can include any character.

The default value is **snmpv3password**.

15. Click Save.

The SNMP settings for the network are configured.

Platform Configuration Settings

The **Platform Configuration Settings** page sets global options that are applicable for all other components that have the same georedundant arrangement.

Configuring the Upsync Log Alarm Threshold

You can configure the threshold of outstanding updates to a secondary server that triggers an alarm. When the outstanding updates reaches a configured percent of the upsync log capacity, an event is issued and the current condition of the connection (volume of outstanding data, current throughput, time of the event, and so forth) is logged.

The events are tracked in the MPE/MRA replication report. See [Viewing the MPE/MRA Replication Statistics Report](#) for more information.

To configure the upsync log alarm threshold:

1. From the **Platform Setting** section of the navigation pane, select **Platform Configuration Setting**.
The **Platform Configuration** page opens.
2. Click **Modify**.
3. Enter the **Upsync Log Alarm Threshold** (5).
The percent must be in the range of 50% – 95%.
4. Click **Save**.

Configuring Concurrent Bulk Transfers

Concurrent Bulk Transfers can occur over the WAN. Under normal operations setting the number of concurrent bulk audits between two sites to **1** is sufficient because bulk audits are relatively uncommon. However in case of a site/WAN outage this limit can result in long recovery times.

Configuring the **Concurrent Bulk Transfers** setting specifies the number of servers that simultaneously perform a bulk transfer across the WAN. A bulk transfer can happen when a server starts COMCOL or is demoted from active status. A bulk transfer copies one or more database tables to the secondary site database because the record of database updates is not available. Unlike steady state replication which is limited by the rate of updates applied to the database, bulk transfer sends the table as fast as possible.

The recommended number is based on the available bandwidth within the WAN. For example, if the WAN transfer speed is 1GB/s, it is best to set the **Concurrent Bulk Transfers** **1**.

1. From the **Platform Setting** section of the navigation pane, select **Platform Configuration Setting**.
The **Platform Configuration** page opens.
2. Click **Modify**.
The **Platform Configuration** page becomes editable.
3. Enter the allowed number of **Concurrent Bulk Transfers**.
Valid values are **1** to **8**. The default value is **1**.

4. Click **Save**.

The number of allowed concurrent bulk transfers are set.

Chapter 4

Managing Multimedia Policy Engine Devices

Topics:

- *Managing Policy Server Profiles.....86*
- *Managing Configuration and Virtual Templates.....89*
- *Configuring MPE Protocol Options.....92*
- *Configuring Data Source Interfaces.....104*
- *Policy Server Groups.....115*
- *About Reapplying a Configuration.....118*
- *Resetting Counters.....119*
- *Enabling or Disabling All Sh Connections.....120*
- *Checking the Status of an MPE Server.....120*
- *Policy Server Reports.....121*
- *Viewing Policy Server Logs.....132*
- *Analytics Data Stream.....137*

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

Note: The MPE device is also called the Policy Server.

Managing Policy Server Profiles

A policy server profile contains the configuration information for an MPE device (which can be a single server, a two-server cluster, or a three-server cluster). The CMP system stores policy server profiles in a configuration database. After you create and configure policy profiles, you deploy them to MPE devices across the network.

The following sections describe how to manage policy server profiles:

- [Creating a Policy Server Profile](#)
- [Configuring a Policy Server Profile](#)
- [Modifying a Policy Server Profile](#)
- [Deleting a Policy Server Profile](#)

For information on deploying defined policies to an MPE device, see *Policy Wizard Reference*.

Creating a Policy Server Profile

Note: 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. (Required) Select the **Associated Cluster** with which to associate this MPE device.
See [Configuring the Policy Management Topology](#) for details on adding cluster's to the topology.
5. (Required) Enter the **Name** for this 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 (,)
6. (Optional) Enter **Description / Location**
Information that defines the function or location of this MPE device.
7. (Optional) Select to enable **Secure Connection**.
This setting determines whether or not to use the HTTPS protocol for communication between Policy Management devices. If selected, devices communicate over port 8443.

Note: In Policy Management release 9.3, secure connections used port 443. Before upgrading from release 9.3 to release 11.5, disable **Secure Connection** until all devices are upgraded.
8. Select the **Type** from the list.

This setting defines the policy server type:

- **Oracle** (default) — The policy server is an MPE device and can be fully managed by the CMP system.
 - **Unmanaged** — The policy server is not an MPE device and therefore cannot be actively managed by the CMP system. This selection is useful when an MPE device is routing traffic to a third-party policy server.
9. (Optional) **Associate Templates.** See [Managing Configuration and Virtual Templates](#) for information about configuration and virtual templates.
10. Click **Save**.

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

Proceed with configuring the policy server. See [Configuring a Policy Server Profile](#).

About Policy Server Administration

After creating and saving a policy server profile, you can proceed with configuring the device using the **Policy Server Administration** page.

The **Policy Server Administration** 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 or IPv6 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 system). See [Creating a Policy Server Profile](#) for details.
- **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. See [Policy Server Reports](#) for details.
- **Logs** – Displays the Trace Log, Syslog, SMS, SMTP, and HTTP log configurations. See [Viewing Policy Server Logs](#) for details.
- **Policy Server** – Lets you associate applications and network elements with an MPE device and configure protocol information. See [Configuring MPE Protocol Options](#) for details.
- **Diameter Routing** – Lets you configure the Diameter peer and route tables. See [Configuring Protocol Routing](#) for details.
- **Policies** – Lets you manage policies that are deployed on the policy server. Refer to *Policy Wizard Reference* for details.
- **Data Sources** – Lets you configure interfaces to LDAP (Lightweight Directory Access Protocol), Diameter Sh, or SPR (Subscriber Profile Repository) systems. See for details.
- **Session Viewer** (read only) – Displays static session and binding data for a specific subscriber from the Policy Management device that is managing the session. See [Displaying Static Session and Binding Data for a Subscriber](#) for details.

Configuring a Policy Server Profile

To configure 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 policy server.

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

3. Select the tab that contains the information you want to configure or modify and click **Modify**.
4. Edit the information:

- **Logs** – See [Configuring Log Settings](#) for details.
- **Policy Server** – See [Configuring MPE Protocol Options](#) for details.

Note: You must configure attribute information on the **Policy Server** tab for most protocols to function correctly.

- **Diameter Routing** – See [Configuring Protocol Routing](#) for details.
- **Policies** – Refer to *Policy Wizard Reference* for details.
- **Data Sources** – See [Configuring Data Source Interfaces](#) for details.

5. Click **Save**.

After you have configured a policy server profile for an MPE device in your Policy Management network, you can associate network elements with it (see [Managing Network Elements](#)).

Modifying a Policy Server Profile

To modify 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 policy server.
The **Policy Server Administration** page opens in the work area.
3. Select the tab that contains the information you want to configure or modify and click **Modify**.
4. Edit the information:

- **System** – See [Creating a Policy Server Profile](#) for details.
- **Logs** – See [Configuring Log Settings](#) for details.
- **Policy Server** – See [Configuring MPE Protocol Options](#) for details.

Note: You must configure attribute information on the **Policy Server** tab for most protocols to function correctly.

- **Diameter Routing** – See [Configuring Protocol Routing](#) for details.
- **Policies** – Refer to *Policy Wizard Reference* for details.
- **Data Sources** – See [Configuring Data Source Interfaces](#) for details.


5. 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.

Note: You cannot delete a policy server profile if the profile is configured in an MPE pool. Refer to *Policy Front End Wireless User's Guide* for more information.

To delete 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. 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:
 1. Select the MPE device.
The **Policy Server Administration** page opens.
 2. Select the **System** tab and click **Delete**.

A confirmation message appears.

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

The policy server profile is deleted.

Managing Configuration and Virtual Templates

Configuration and Virtual Templates provide a more efficient means of normalizing common configurations between multiple MPE or MRA instances. Any given device can be associated with no template, one, or many templates. In addition, users can add, remove, clone, and prioritize templates.

Virtual Templates are similar to symbolic links in Linux. Virtual Templates are particularly efficient when users want to replace a template that has been associated to multiple MPE or MRA devices with another template.

Creating a Configuration Template

Note: You must create a configuration template before creating a virtual template because a virtual template references, and is dependent on, a configuration template.

Use this procedure if you want to make a template that you will use many times.

To create a configuration template:

1. From the **Policy Server** section of the navigation pane, select **Configuration Template**.
The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates**.
2. From the content tree, select **Configuration Templates**.
The **Configuration Template Administration** page opens.
3. Click **Create Template**.
The **New Configuration Template** page opens.
4. Enter the **Name** of the template.

Note: This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, space, comma, and backslash characters are not valid.

5. (Optional) To use an existing template as a base for the new template, select an existing template from the **Copy From** list.
6. (Optional) Enter a **Description / Location**.
The text box is limited to 255 characters.
7. Click **Save**.

The new template appears in the list in the content pane.

After creating the template, proceed with configuring the template.

Creating a Configuration Template

Note: This procedure applies to both MPE and MRA devices.

Note: You must create a configuration template before creating a virtual template because a virtual template references, and is dependent on, a configuration template.

Use this procedure if you want to make a template that you will use many times.

To create a configuration template:

1. From the **MRA** section of the navigation pane, select **Configuration Template**.
The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates**.
2. From the content tree, select **Configuration Templates**.
The **Configuration Template Administration** page opens.
3. Click **Create Template**.
The **New Configuration Template** page opens.
4. Enter the **Name** of the template.
Note: This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, space, comma, and backslash characters are not valid.
5. (Optional) To use an existing template as a base for the new template, select an existing template from the **Copy From** list.
6. (Optional) Enter a **Description / Location**.
The text box is limited to 255 characters.
7. Click **Save**.

The new template appears in the list in the content pane.

After creating the template, proceed with configuring the template.

Modifying a Template

Note: This procedure applies to both MPE and MRA devices.

Use this procedure if you need to modify an existing template to comply with new requirements or conditions.

To modify a configuration template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.
The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates**.
2. From the content tree, select the **Configuration Template** for modification.
The **Configuration Template Administration** page opens with the template configuration settings.
3. Select the tab that contains the information you want to configure or modify and click **Modify**.
4. For a policy server, edit the information:
 - **Template**
 - **Logs** – See [Configuring Log Settings](#) for details.
 - **Policy Server** – See [Configuring MPE Protocol Options](#) for details.

Note: You must configure attribute information on the **Policy Server** tab for most protocols to function correctly.

 - **Diameter Routing** – See [Configuring Protocol Routing](#) for details.
 - **Policies** – See *Policy Wizard Reference* for details.
 - **Data Sources** – See [Configuring Data Source Interfaces](#) for details.
5. Click **Save**.

The settings are saved for the template and applied to all associated MRA or MPE devices.

Changing the Template Priority

You would reorder templates in a list to prioritize templates according to configuration values applied to a given MRA or MPE instance. For example, different configurations will provide different prioritizations depending on the order (the lower the number the higher the prioritization) as it is listed in the **Associated Templates** section of the **Modify System Settings** screen.

Note: This procedure applies to both MPE and MRA devices.

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration**.
The content tree displays a list of **All Policy Servers** or **MRA** devices.
2. From the content tree, select the device.
The Administration page opens with the device configuration.
3. Select the **System** tab.
The device's system configuration settings display on the page.
4. Click **Modify**.
The administration page becomes enabled for editing.
5. In the **Associated Templates** section, edit the **Priority** value to change the number to a higher or lower value.
6. Click **Update Order**.
The priority order of the **Associated Templates** is changed.

Creating a Virtual Template

Because an MPE or an MRA device can exist independently of one another, you can create both virtual and configuration templates in two locations in the CMP interface. Depending on your needs, the CMP interface enables you to create templates either in the Policy Server or MRA section.

Because virtual templates are based on configuration templates, modifying a configuration template associated with a virtual template automatically modifies the virtual template. After the template is created, the template has the functionality that is specific to that instance (that is, either MPE or MRA). After templates are created and associated, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

Note: You must create a configuration template before creating a virtual template because a virtual template references, and is dependent on, a configuration template.

Note: This procedure applies to both MPE and MRA devices.

Use this procedure if you have virtual template capability.

To create a virtual template:

1. From the **Policy Server** section of the navigation pane, select **Configuration Template**.
The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates**.
2. From the content tree, select **Virtual Templates**.
The **Virtual Template Administration** page opens.
3. Click **Create Virtual Template**.
The **New Virtual Template** page opens.
4. Enter the **Name** of the template.

Note: This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, space, comma, and backslash characters are not valid.
5. Select a template from the **Associated Configuration Template** list.
6. (Optional) Enter a **Description**.
7. Click **Save**.

The settings are saved for the template, and applied to all associated MPE devices.

Configuring MPE Protocol Options

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 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.

Selecting or choosing **undefined** signifies that the value comes from a configuration profile. If there is not a configuration profile, then the default value is used.

The following sections define the available options. (The options you see vary depending on the mode configuration of your system.)

- [Associations Configuration Options](#)
- [Subscriber Indexing Configuration Options](#)
- [General Configuration Options](#)
- [RADIUS-S Configuration Options](#)
- [Diameter Configuration Options](#)
- [S9 Configuration Options](#)
- [User Profile Lookup Retry and Session Updates Configuration Options](#)
- [Diameter AF Default Profiles Configuration Options](#)
- [Default Charging Servers Configuration Options](#)
- [SMS Relay Configuration Options](#)
- [SMPP Configuration Options](#)
- [Primary SMSC Host Configuration Options](#)
- [Secondary SMSC Host Configuration Options](#)
- [SMTP Configuration Options](#)
- [Generic Notification Configuration Options](#)
- [RADIUS Configuration Options](#)
- [Analytics Configuration Options](#)

5. Click **Save**.

You have defined the protocol options for this MPE device.

Associations Configuration Options

Attribute	Description
Applications	The application profiles associated with this MPE device. To modify this list, click Manage . For more information on application profiles, see <i>Policy Wizard Reference</i> .
Network Elements	The network elements associated with this MPE device. To modify this list, click Manage . For more information on network elements, see Managing Network Elements .
Network Element Groups	The network element groups associated with this MPE device. To modify this list, select or deselect groups. For more information on network element groups, see Managing Network Elements .
Notification Servers	The notification servers associated with this MPE device. To modify this list, click Manage .

Subscriber Indexing Configuration Options

Attribute	Description
Index by IPv4	Select if the associated Subscriber Profile Repository is indexed by IPv4 address.
Index by IP-Domain-ID	Select if the associated Subscriber Profile Repository is indexed by IP domain ID. The combination of framed IPv4 address and IP domain ID ensures a globally unique binding, even if the same IPv4 address is locally assigned in multiple networks.
Index by IPv6	Select if the associated Subscriber Profile Repository is indexed by IPv6 address.
Index by Username	Select if the associated Subscriber Profile Repository is indexed by account ID.
Index by NAI	Select if the associated Subscriber Profile Repository is indexed by network access ID.
Index by E.164 (MSISDN)	Select if the associated Subscriber Profile Repository is indexed by E.164 phone number.
Index by IMSI	Select if the associated Subscriber Profile Repository is indexed by International Mobile Subscriber Identity (IMSI) number.
Overrides by APN	Select to configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN). In the Overrides by APN section, click Add . Enter the APN and click Save to enable Index by IPv4, Index by IPv6, or both. You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

General Configuration Options

Time of Day Triggering	Select Enable or Disable (default) from the list. If you select Enable , this MPE device supports time-of-day triggering when evaluating policy rules. For more information on time-of-day triggering, refer to <i>Policy Wizard Reference</i> .
Billing Day	If true , you can configure a global monthly billing day for subscribers who do not have a specific day configured in their profiles in a back-end database.
Billing Day of Month	If Billing Day is enabled, enter the day of the month on which subscriber usage counters are reset. This date is the default billing date for all subscribers handled by this MPE device; billing dates can be changed on a per-subscriber basis.
Billing Time Zone	Select the time zone used for billing cycle calculations. If this feature is configured, the user equipment time zone, even if reported, is irrelevant for billing cycle calculations.
Observe Daylight Saving Changes	If true , the MPE device observes Daylight Saving Time for the configured Billing Time Zone.

Default Local Time Mode	<p>Select the time used within a user's session from the list: System Local Time to use the local time of the MPE device (default) or User Local Time to use the user's local time.</p> <p>Note: If the time zone was never provided for the user equipment, system local time is applied.</p>
Enable Pro Rate	<p>If false or undefined, the full monthly quota for subscribers is granted for the billing cycle following a quota reset.</p> <p>If true, the monthly quota for subscribers is prorated, on a per-quota basis (for up to 30 quotas), for the billing cycle following a quota reset, based on the value of the Billing Date Effective field in the profile for the subscriber profile. This is a global setting affecting all subscribers. (If the field value is null, usage will not be prorated.)</p>
Billing Date Effective Name	<p>Enter the name of the custom field in subscriber profiles to use for the SPR variable <i>NewBillingDateEffective</i>. The default is null. This is a global setting affecting all subscribers.</p> <ul style="list-style-type: none"> To specify a local time in the SPR, the field must be in the format: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <code>yyyy-mm-ddThh:mm:ss</code> </div> To specify a time zone (UTC offset), the field must be in the format: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <code>yyyy-mm-ddThh:mm:ssZ</code> </div> <p>For example: 2011-10-30T00:00:00-5:00</p>
Track Usage for Unknown Users	<p>If true, the MPE device tracks usage and state per subscriber ID, even if the subscriber is not registered in the SPR. If tracking was enabled and is now disabled, usage and state is no longer tracked for unknown users, but existing usage and state data is retained.</p>
Subscribe For Unknown Users	<p>If Validate user is false (at the MPE device), then unknown users are allowed to create sessions. In this case, if Subscribe for Unknown Users is true, then the MPE device will subscribe for those users.</p> <p>Note: This setting is only for the MPE device and does not have any effect on the SPR. There are settings in the SPR that must be set to allow auto-enrolling.</p>
Use Single Lookup	<p>If true, the MPE device reads multiple Sh user data blocks (subscriber, quota usage, and entity state) with a single read request. If you enable this feature, you must also configure the Sh data source with the option Notif-Eff (see Configuring an Sh Data Source).</p> <p>If false, separate lookups are used.</p>
Use Combined Writes	<p>If true, the MPE device will combine the updates (PUR messages) resulting from a single user request into a single PUR update to the SPR. The PUR will contain both the quota usage and state updates for the user. This reduces the number of transactions between the MPE and SPR.</p>
Cache Quota Usage	<p>If true, the MPE device caches the quota usage objects locally for as long as the user session exists.</p>

	If false , objects are cached for a default of 60 seconds.
Cache Entity State	If true , the MPE device caches the entity state objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.
Subscribe Quota Usage	If true , the MPE device subscribes to receive notifications from the SPR for any changes to the quota.
Subscribe Entity State	If true , the MPE device subscribes to receive notifications from the SPR for any changes to the entity state.

RADIUS-S Configuration Options

Attribute	Description
RADIUS Shared Secret	Authenticates RADIUS messages received from external gateways (that is, PDSN or HA). This field must be configured with a value or the RADIUS-S protocol will not work. Also, each gateway must be configured to use this value when sending messages to the MPE device, or the messages received from that gateway will be dropped.
Untiered Plan Name	When the MPE device is set to RADIUS-S mode, this attribute indicates that a matching plan name does not participate in any tiered service plan. On a successful lookup for a given subscriber, the plan name returned by LDAP is compared to the Untiered Plan Name configured for the MPE device via the Policy Server tab. If they match, no default QoS values are sent to the gateway for the subscriber. If the Untiered Plan Name is null, this only matches if the subscriber has an entry in LDAP with no value for the associated attribute. The default value is null.
Default Downstream Profile / Default Upstream Profile	Define the upstream and downstream bandwidth parameters that are used when establishing a default traffic profile using RADIUS-S. You can override these parameters by configuring policy rules that apply different profiles. If a default profile is not configured, and the policy rules do not set the bandwidth parameters, a default traffic profile is sent to the Gateway to disable policing.
Index by Username	Select if the RADIUS database is indexed by subscriber account ID.
Index by NAI	Select if the RADIUS database is indexed by subscriber network address ID.
Index by Calling Station ID	Select if the RADIUS database is indexed by subscriber calling station ID.
Index by IP Address	Select if the RADIUS database is indexed by subscriber IP address.

Diameter Configuration Options

Attribute	Description
Diameter Realm	The domain of responsibility (for example, galactel.com) for the MPE device.

Attribute	Description
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, mpe3.galactel.com).
Default Resource Id	The bearer used if a GGSN does not send any bearer information in a Credit-Control Request (CCR). Enter an alphanumeric string of up to 100 characters. The default is no resource ID (that is, no bearer).
Correlate PCEF sessions	If true , the primary PCEF Gx session will share information with all secondary sessions that share an IP address within the same IP-CAN session. Up to 10 different Gx sessions can be correlated to one subscriber. By default, PCEF sessions are not correlated and do not share information.
Validate user	If true , sessions for unknown users are rejected.
Diameter PCEF Default Profile	Select the default traffic profile from the list that will be applied during PCEF session establishment using the Gx or Ty protocols, or if no other SCE traffic profile is applied as a result of a policy being triggered. Refer to <i>Policy Wizard Reference</i> for details on creating a traffic profile.
Use Synchronous Sd	If true , the MPE device establishes an Sd session before sending a Gx CCA message to a traffic detection function (TDF).
Identify Duplicate sessions based on APN	If true , the MPE device will detect duplicate sessions. This makes it possible to remove duplicate sessions if their number becomes excessive.
Subscriber ID to detect duplicate sessions	This option is available only if Identify Duplicate sessions based on APN is true . Select the subscriber index type to use from the list: <ul style="list-style-type: none"> • Username • NAI • E.164 (MSISDN) • IMSI
Protocol Timer Profile	The timer profile to use. See Creating a Protocol Timer Profile for details.
Prevent Overlapping Rule Names	If selected, rule names that are dynamically generated on the primary and spare MPE devices in the same Gx session are unique.
Allow Multiple Rx Connections with the same Origin-host Id	When enabled, the MPE device accepts multiple Rx connections with the same Origin-Host Attribute Value Pair (AVP) and source IP address.
Timers	Rx-to-PCMM gate timers. Enter values in seconds for T1 (authorized, default 1 second), T2 (reserved, default 300 seconds), and T3 (committed, default 300 seconds).

S9 Configuration Options

Attribute	Description
Initiate S9 Requests	<p>If true, the MPE device can initiate S9 requests. In addition, you must specify Initiate Connection when you define the Diameter peer. For more information, see Configuring Diameter Peers.</p> <p>Note: If an MRA device is deployed in the Policy Management network, the MPE device will not initiate S9 connections regardless of how you configure S9 options.</p>
Accept S9 Requests	<p>If true, the MPE device can accept S9 requests. If not enabled, when the MPE device receives an S9 request, an error code is generated at the device.</p>
Primary DEA	<p>If one or more Diameter Edge Agents is defined, you can select the primary agent from the list. For information on defining a DEA, see Configuring Diameter Peers.</p>
Secondary DEA	<p>If multiple Diameter Edge Agents are defined, you can select the secondary agent from the list. If you select both primary and secondary DEAs (and there is not a deployed MRA device in the Policy Management network), the MPE device establishes a connection to both DEAs. If the primary connection is down, the MPE device sends messages over the secondary connection. After the primary connection is back up, communication reverts back to the primary.</p>

User Profile Lookup Retry and Session Updates Configuration Options

Attribute	Description
Enforcement	<p>If true, enables user profile lookup retry on session updates for Gx and Gxx updates.</p>
Application	<p>If true, enables user profile lookup retry on session updates for Rx.</p>

Diameter AF Default Profiles Configuration Options

Note: To select a profile of any of the attributes, you must first create a Diameter profile in the general profile configuration.

Attribute	Description
Default	<p>Define the bandwidth parameters that are used when a request from an Application Function (AF) does not contain sufficient information for the MPE device to derive QoS parameters. These profiles are defined per media type: The Default profile is used when a profile for a media type is not defined.</p>
Audio	<p>The profile for the audio.</p>
Video	<p>The profile for the video.</p>
Data	<p>The profile for data.</p>
Application	<p>The profile for application.</p>

Attribute	Description
Control	The profile for control. Note: To select a profile, first create a Diameter profile in the general profile configuration.
Text	The profile for text.
Message	The profile for messages.
Other	The profile for all other media types.

Default Charging Servers Configuration Options

Attribute	Description
Primary Online Server	FQDN of the primary online charging server (used, for example, for prepaid accounts).
Primary Offline Server	FQDN of the primary offline charging server (used, for example, for billed accounts).
Secondary Online Server	FQDN of the secondary (backup) online charging server.
Secondary Offline Server	FQDN of the secondary (backup) offline charging server.

SMS Relay Configuration Options

Attribute	Description
SMS Enabled	Select true to enable SMS messaging to subscribers.
Relay Host	Enter the FQDN or IP address of the relay server.
Relay Port	Enter the port number on which the relay server is listening for SMS messages. The default port is 8080.
Throttle Value	Enter the time interval, in milliseconds, at which SMS messages are sent from the MPE device. If set to 1000 ms, the MPE device sends one SMS message per second; if set to 500 ms, the MPE device sends two messages per second. The recommend throttle value is 0 ms which means that the device sends the SMS message as soon as it receives the message.

SMPP Configuration Options

Attribute	Description
SMPP Enabled	Select true to enable Short Message Peer to Peer (SMPP) messaging to subscribers. To send an SMS message to a subscriber, a Mobile Station International Subscriber Directory Number (MSISDN) must be present in the subscriber's profile. Messages can be up to 254 characters long.
Validate Message Length	Select true to validate message length.

Attribute	Description
SMPP Long Message Support	If true , SMS messages longer than 160 characters are split into segments and reassembled by the receiving device. Messages of up to 1000 characters are supported.
Delivery Method for Long Message	Select the message delivery method for long messages from the list: <ul style="list-style-type: none"> • Segmentation and Reassembly (SAR) (default) • Message Payload

SMS/XML Configuration Options

Note: This function is restricted. See [About Mode Settings](#) for more information.

Attribute	Description
Service Name	The name of the SMS service. For example, <code>sendMessage</code> .
Service URL	The URL for the service. For example, <code>http://192.0.2.0/example/sms</code>
SMS Source Address	The address to use in the From element in the <code>sendMessageRequest</code> . If left empty, the From element is not included in the <code>sendMessageRequest</code> .
Alert URL	The URL for message alerts. For example, <code>http://192.0.2.0/example/alertsms</code>

Primary SMSC Host Configuration Options

Attribute	Description
SMSC Host	Enter the FQDN or IP address of the primary Short Messaging Service Center (SMSC) store-and-forward server that accepts SMS messages from the relay server.
SMSC Port	Enter the port number on which the primary Short Messaging Service Center store-and-forward server is listening for SMS messages. The default port is 2775.
ESME System ID	Enter the system ID of the primary External Short Messaging Entity (ESME). Sending the ID and password values authenticates the relay server as a trusted source. Note: This value must be configured on the primary SMPP server.
ESME Password	Enter the password of the primary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source. Note: This value must be configured on the SMPP server.
Confirm ESME Password	Re-enter the primary ESME password for verification. Note: This setting is only available from the Modify page.

Secondary SMSC Host Configuration Options

Attribute	Description
SMSC Host	<p>Enter the FQDN or IP address of the secondary Short Messaging Service Center (SMSC) store-and-forward server, which accepts SMS messages from the relay server.</p> <p>Note: The secondary SMSC server is used if the secondary server fails.</p>
SMSC Port	<p>Enter the port number on which the secondary Short Messaging Service Center store-and-forward server is listening for SMS messages. The default port is 2775.</p>
ESME System ID	<p>Enter the system ID of the secondary External Short Messaging Entity (ESME). Sending the ID and password values authenticates the relay server as a trusted source.</p> <p>Note: This value must be configured on the secondary SMPP server.</p>
ESME Password	<p>Enter the password of the secondary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source.</p> <p>Note: This value must be configured on the SMPP server.</p>
Confirm ESME Password	<p>Re-enter the secondary ESME password for verification.</p>
ESME Source Address	<p>Enter the source address for a SUBMIT_SM operation in SMPP Protocol V3.4. The default is none.</p>
ESME Source Address TON	<p>Select the source address Type of Number (TON) from the list:</p> <ul style="list-style-type: none"> • UNKNOWN (default) • INTERNATIONAL • NATIONAL • NETWORK SPECIFIC • SUBSCRIBER NUMBER • ALPHANUMERIC • ABBREVIATED
ESME Source Address NPI	<p>Select the source address Number Plan Indicator (NPI) from the list:</p> <ul style="list-style-type: none"> • UNKNOWN (default) • ISDN (E163/E164) • DATA (X.121) • TELEX (F.69) • LAND MOBILE (E.212) • NATIONAL • PRIVATE • ERMES • INTERNET (IP) • WAP CLIENT ID

Attribute	Description
Character Encoding Scheme	Select the character-set encoding for SMS messages from the list: <ul style="list-style-type: none"> • SMSC Default Alphabet • IA5 (CCITT T.50)/ASCII (ANSI X3.4) • Latin 1 (ISO-8859-1) • Cyrillic (ISO-8859-5) • Latin/Hebrew (ISO-8859-8) • UCS2 (ISO/IEC-10646) • ISO-2022-JP (Music Codes) • JIS (X 0208-1990) • Extended Kanji JIS(X 212-1990)
SMSC Default Encoding Scheme	Select the SMSC default encoding from the list: UTF-8 or GSM7 .
Request Delivery Receipt	Select the global default behavior when evaluating the policy action send SMS from the list: <ul style="list-style-type: none"> • No Delivery Receipt • Delivery Receipt on success and failure • Delivery Receipt on failure

SMTP Configuration Options

Attribute	Description
SMTP Enabled	Select true to enable Simple Mail Transport Protocol (SMTP) messaging (email) to subscribers. SMTP notifications are triggered from policy action and sent through an SMS Relay (SMSR) function to an external mail transfer agent (MTA). <p>Note: There is no delivery receipt for the SMTP messages sent from the SMSR, only confirmation that it reached the configured MTA.</p>
MTA Host	Enter the FQDN or IP address of the Mail Transfer Agent server, which accepts SMTP messages from the SMSR function.
MTA Port	Enter the port number on which the MTA server is listening for SMTP messages. The default port is 25.
MTA Username	Enter the system ID of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. <p>Note: This value must be configured on the MTA.</p>
MTA Password	Enter the password of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. <p>Note: This value must be configured on the MTA.</p>
Confirm MTA Password	Re-enter the password for verification. <p>Note: This is a new configuration setting for the SMTP connection.</p>

Attribute	Description
Default From Address(es)	<p>Enter the source address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none.</p> <p>Note: The total number of To, CC, and BCC addresses is limited to five.</p>
SMTP Connections	<p>The number of SMTP connections. Enter a number from 1–10.</p> <p>Note: SMTP connections can be increased to support a higher throughput. Contact My Oracle Support (MOS) for more information.</p>
Default Reply-To Address(es)	<p>Enter the email address automatically inserted into the To field when a user replies to an email message. For most email messages, the From and Reply-To fields are the same, but this is not necessarily so. If no Default Reply-To is specified here, the From address is used. Optionally, enter a static email address to use for Reply-To.</p> <p>The default is none.</p>
Default CC Address(es)	<p>Enter the copy address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none.</p> <p>Note: The total number of To, CC, and BCC addresses is limited to five.</p>
Default BCC Address(es)	<p>Enter the blind copy recipient address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none.</p> <p>Note: The total number of To, CC, and BCC addresses is limited to five.</p>
Default Signature	<p>Enter the text that should appear as the signature in an SMTP message.</p> <p>The default is none.</p>

Generic Notification Configuration Options

Attribute	Description
Notification Enabled	<p>If SMPP/XML mode is enabled, select true to enable notifications using notification servers. For more information about notification servers, refer to <i>Policy Wizard Reference</i>.</p>

RADIUS Configuration Options

Attribute	Description
RADIUS Enabled	<p>When selected, the MPE device processes RADIUS messages.</p> <p>When not selected, RADIUS messages are ignored.</p> <p>The default is enabled.</p>
RADIUS Ports (Listening)	<p>Enter a comma-separated list of UDP port numbers that the MPE device listens on for RADIUS messages.</p> <p>The default is 1813,3799.</p>

Attribute	Description
Concatenate Multiply Occurring VSA's	<p>When selected, if a string VSA appears multiple times in a RADIUS message, the values are concatenated to form one large value.</p> <p>When not selected, if a string VSA appears multiple times in a RADIUS message, the value of the last TLV or VSA is used, and the earlier values are ignored. The default is disabled (earlier values are ignored).</p>
Validate User	<p>When selected, if an SPR lookup fails for a subscriber, the MPE device rejects the request.</p> <p>When not selected, if an SPR lookup fails for a subscriber, the MPE device creates a dummy subscriber instance to store necessary information for later use. The default is disabled (requests are processed).</p>
Default Passphrase	<p>Enter the default passphrase (a text string). This shared secret value is used when no shared secret is defined for a specific RADIUS network element. The same shared secret is used for decrypting accounting requests and CoA responses and encoding accounting and CoA responses.</p> <p>If you enter no passphrase and either of the fields in the associated network elements are not set, then the MPE device ignores RADIUS requests and responses.</p> <p>The default is radius.</p>







Analytics Configuration Options

Attribute	Description
Policy Analytics Enabled	<p>If the Oracle Communications Policy Management Analytics feature is enabled, select true to generate an analytics data stream from the MPE device. For more information, see Analytics Data Stream.</p>

Configuring Data Source Interfaces

Before the MPE device can communicate with any external data sources, you must configure the interface. To configure a data source interface:

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.
3. Select the **Data Sources** tab.
The current data sources are displayed, listing the following information:
 - Administrative state
 - Name
 - Role
 - Type
 - Primary host
 - Secondary host

- Tertiary host
4. To modify the list of data sources, click **Modify**.
The **Modify Data Sources** page opens. The functions available from this table are as follows:
 - To add a data source:
 1. Click  **Add**.
 2. Select the data source type from the **Add** list.
The appropriate **Add Data Source** window opens.
 3. Configure values:
 - For LDAP data sources, see [Configuring an LDAP Data Source](#).
 - For an Sh data source, see [Configuring an Sh Data Source](#).
 - For an Sy data source, see [Configuring an Sy Data Source](#).
 - Cloning a data source in the table
 1. Select an existing data source in the table.
 2. Click  **Clone**. The **Clone Data Source** window opens with the information for the data source.
 3. Make changes as required.
 4. Click **Save**. The data source is added to the table
 - Editing a data source in the table
 1. Select the data source in the table.
 2. Click  **Edit**. The **Edit Data Source** window opens, displaying the information for the data source.
 3. Make changes as required.
 4. Click **Save**. The data source is updated in the table.
 - Deleting a data source from the table
 1. Select the data source in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the data source entry. The data source is removed from the table.
 - Ordering the list.
If you define multiple entries, they are searched in the order displayed in this list. To change the order:
 1. Select an entry.
 2. Click  **Up** or  **Down**. The search order is changed.
- Click **Save**.
5. The following general settings are available:
 - **Merge Search Results** — If you define multiple data sources and a search returns results from more than one source, the results are displayed in source order. To display one sorted list instead, select this option.

- **Subscription Enabled Via Policy Only** — For detailed information, see the SPR documentation.
6. The following Sh general settings are available:
- **Notification Re-auth Via Policy** — If selected, every notification is processed by the policy engine of the MPE device to determine whether it should generate a re-authorization. If selected, you must write policy rules to specifically generate the re-authorizations. See the *Policy Wizard Reference* for more information on policy rules. If this setting is not selected (default), only notifications related to provisioning, such as user profile, pool profile, dynamic quota, or pool dynamic quota notifications, generate re-authorizations.
 - **Combine Lookup And Subscription** — If selected, lookup and subscription requests are combined.
7. The following Sy general setting is available:
- **Notification Re-auth Via Policy** — If selected, every notification is processed by the policy engine of the MPE device to determine whether it should generate a re-authorization. If selected, you must write policy rules to specifically generate the re-authorizations. See the *Policy Wizard Reference* for more information on policy rules. If this setting is not selected (default), only notifications related to provisioning, such as user profile, pool profile, dynamic quota, or pool dynamic quota notifications, generate re-authorizations.
8. Click **Save**.

Configuring an LDAP Data Source

For LDAP, you can configure connections to up to three servers.

The **Add Data Source** window contains the following tabs:

- [Server Info Tab](#)
- [Search Criteria Tab](#)
- [Search Filters Tab](#)
- [Associated Data Sources Tab](#)
- [External Fields Tab](#)

Server Info Tab

On the **Server Info** tab, enter the following:

Role	Data source attribute:	
	Primary	The data source which performs the initial level of lookups.
	Secondary	Indicates a dependency on the results of the prior lookup. It must initially be associated with the primary data source and configured to be used in a subscriber lookup.
Unique Name	Name given to associate with the created LDAP.	
Admin State	Select to enable this data source. Selected by default.	
Read Enabled	Select to enable read access to this data source. Selected by default.	

Write Enabled	Select to enable write access to this data source.
Primary Host	FQDN or IP address in IPv4 or IPv6 format of primary LDAP server.
Primary Port	Port number of primary server. The default port number is 389.
Secondary Host	FQDN or IP address in IPv4 or IPv6 format of secondary LDAP server.
Secondary Port	Port number of secondary server. The default port number is 389.
Tertiary Host	FQDN or IP address in IPv4 or IPv6 format of tertiary LDAP server.
Tertiary Port	Port number of tertiary server. The default port number is 389.
Authentication DN	The Distinguished Name (DN) used for binding to the LDAP server. The DN can refer to an entry in the directory or to a relative distinguished name (RDN). RDN attributes include cn (common name), uid (user ID), ou (organizational unit), and o (domain name). For example: cn=PolicyServer,ou=galactel,o=galactel.com
LDAP Password	Provides read-only access to the LDAP directory. The MPE device must bind to the LDAP server with the DN and password to access the database. Example: LDAPpassword .
Read Connections	Enabled for data sources set in the Secondary role. Select up to 10 connections.
Write Connections	Disabled for data sources set in the Secondary role. Select up to 10 connections.

If merged results are enabled, multiple primary data sources are searched asynchronously. Secondary searches are dependent on the results of the primary they are associated with, and will run as soon as the results are returned from that primary. The secondary searches will not wait for the results of other primary data sources before initiating.

Search Criteria Tab

On the **Search Criteria** tab, enter the following:

1. Select how the LDAP database is indexed:
 - **Alternate Key** — The Alternate Key has an LDAP data source role of primary.
Note: If you select Alternate Key indexing, there are no options, so the rest of the tab becomes blank.
 - **Username** — The database is indexed by user name (account ID).
 - **NAI** — The database is indexed by NAI (network access ID).
 - **E.164 (MSISDN)** — The database is indexed by E.164 (E.164 phone number).
 - **IMSI** — The database is indexed by International Mobile Subscriber Identity.
 - **IP Address** — The database is indexed by IP address.
2. **Root DN** — The root distinguished name for the LDAP search.
3. **Scope** — Scope of the LDAP search:
 - **Object** — Restrict the scope of the LDAP search to the specified object.

- **One-Level** (default) — Extend the scope of the LDAP search one level under the given search base.
 - **Sub-Tree** — Extend the scope of the LDAP search to the whole subtree under the given search base.
4. **Key Attribute** — The attribute whose value is checked to match the key value; used to construct a search filter of the format *KeyAttribute=KeyValue*.
 5. **Base DN Attribute** — This attribute will be prefixed to the root distinguished name when building the DN for a search.
 6. **Key Transform Pattern** — Regular expression (regex) pattern to use to transform a key.
 7. **Key Replace Pattern** — Replacement string to use to transform the key.
For example, **17\$2** means the new string starts with 17 and is followed by the group 2 (\$2) pattern.
 8. **Attributes** — Comma-separated list of entries defining how to save attributes in the object returned from the LDAP search.
The default is null, meaning that all values are saved using the attribute name used in LDAP. Otherwise, each entry should be one of the following:
 - *attr* — A field is saved with the same name and value as the specified attribute.
 - *field=attr* — A field with the specified name is saved with the value of the specified attribute.
 - *field=attr[from:to]* — A field with the specified name is saved with a substring of the value of the specified attribute.

The substring is determined by the *from* and *to* values. A value of 0 in *from* indicates the beginning of the value, and a value of 0 in *to* indicates the end of the value.
 9. Click **Save**.

Search Filters Tab

You can configure any number of filters per search type per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters. It is best to order filtered data sources higher than unfiltered ones.

To define filters, on the **Search Filters** tab, enter the following:

1. **Key Type** — Select from the list:
 - **User Name** (default) — User name (account ID)
 - **NAI** — Network address ID
 - **E.164 (MSISDN)** — E.164 phone number
 - **IMSI** — International Mobile Subscriber Identity
 - **IP Address** — IP address
2. **Expression** — Enter a regular expression.
For example:
 - **508.*** — Matches numbers beginning with 508.
 - ***@galactel.com** — Matches strings ending with @galactel.com
 - **.*** — Matches any input string

To add the expression to the list, click **Add**. To remove an expression from the list, select it in the list and click **Delete**.

3. Click **Save**.

The LDAP data source filters are defined.

Associated Data Sources Tab

On the **Associated Data Sources** tab, enter the following:

Associated Data Sources A list of associated secondary data sources. The list is displayed on the priority order of the secondary data sources. For example:





```
LDAP1.AssociatedLDAPs=1234567890111111,
123456789022222
```

Note: Select **Deselect All** if you want to deselect your choices.

External Fields Tab

The **External Fields** tab lets you define external fields and map them to specific LDAP attributes and distinguished names (DNs). This enables you to use the same external field name when writing a policy that will be deployed across multiple MPE devices. You can define up to 50 attributes per data source.

The functions available from the **External Fields** tab are as follows:

1. Click  **Add**.
The **Add External Field** window opens.
2. Enter the external field name, the LDAP attribute name, and a distinguished name (DN).
3. Click **Save**.
4. (Optional) Add, modify, or delete external fields using the following functions:
 - Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is added to the table
 - Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
 - Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.

Configuring an Sh Data Source

For an Sh data source, you can define two active primary connections and two standby backup connections. An incoming message can be handled from either active connection. You can subscribe through the MPE device (via the Sh interface) to receive notifications on changes to the Quota and Entity State objects.

The Sh interface is not session stateful—each new request is independent of any other requests. A Diameter Subscription for Notification Request (SNR) message causes a subscription to be registered until it is explicitly canceled. To minimize traffic, a Profile Read (UDR) message can be combined with an SNR message. The MPE device reads a subscriber's profile when the subscriber's first session is established, and caches the profile until the subscriber's last session is terminated. If the MPE device receives a Profile Change Notification (PNR) message, the cached profile is updated, and policies for all sessions using the profile are re-evaluated.

If an Sh request originated by the MPE device fails, the error code returned is compared against a set of error codes, and if the code matches the request is retried, one time. An Sh request is sent to the primary connections first, and to the secondary connection only so long as no primary connection is available.

You can specify settings that apply to all Sh data sources. See [Configuring Data Source Interfaces](#) for more information.

Server Info Tab

On the **Server Info** tab, enter the following:

1. **Admin State** — Select to enable this data source.
Selected by default.
2. **Realm** — Enter the server realm; for example, **galactel.com**
 - **Enable Subscription** — Select to allow the MPE device to receive subscription notifications as changes are implemented to the Quota and Entity state. This function manages dynamic profile changes. The data is returned in one XML response. If this option is disabled, separate look ups are used.
3. **Unique Name** — Enter a specific name for the MPE device for organizational purposes.
 - **Use Notif-Eff** — Select to enable reads of multiple user data blocks (subscriber, quota, and entity state).
4. Select a **Sh Profile**:
 - **ProfileV1** (default) — third-party HSS
 - **ProfileV2** — HSS/Sh (7.5 or earlier version)
 - **ProfileV3** — SPR (8.0 or later version)
 - **ProfileV4** — Oracle Communications User Data Repository-Base
5. **Version** — Identifies the version of the data source in the format *x.x*.
This number identifies the data source as either SDM or UDR:
 - A version number of 9.x specifies an SDM data source.
 - A version number of 10.x specifies a UDR data source.

6. **Protocol Timer Profile** — Select a protocol timer profile. For information on creating Protocol Timers, see [Managing the Protocol Timer Profiles Function](#).
7. **Transport** — Select the transport mode for the MPE device.
 - a) **TCP** — Indicates whether the Sh data source can support TCP protocol. If selected, an MPE device can communicate with the Sh data source in TCP. Select a value in the range 1 to 8. The default is 1.
 - b) **SCTP** — Indicates whether the Sh data source can support SCTP protocol. If selected, an MPE device can communicate with the Sh data source in SCTP. Select a value in the range 1 to 8. The default is 8 for both **Max Incoming Streams** and **Max Outgoing Streams**.
8. **Primary Servers:**
 - a) **Primary Identity** — Enter the primary server host name.
 - b) **Primary Address** — Enter the IP address, in IPv4 or IPv6 format, of the primary server.
 - c) **Primary Port** — Enter the primary server port number.
The default port number is 3868.
 - d) **Secondary Identity** — Enter the secondary server host name.
 - e) **Secondary Address** — Enter the IP address, in IPv4 or IPv6 format, of the secondary server.
 - f) **Secondary Port** — Enter the secondary server port number.
The default port number is 3868.
9. **Backup Servers:**
 - a) **Primary Identity** — Enter the primary backup server name.
 - b) **Primary Address** — Enter the IP address, in IPv4 or IPv6 format, of the primary backup server.
 - c) **Primary Port** — Enter the primary backup server port number.
The default port number is 3868.
 - d) **Secondary Identity** — Enter the secondary backup server name.
 - e) **Secondary Address** — Enter the IP address, in IPv4 or IPv6 format, of the secondary backup server.
 - f) **Secondary Port** — Enter the secondary backup server port number.
The default port number is 3868.
 - g) **OAM IP** — SPR feature queries and edits data from the Sh data source via RESTful API.
10. Click **Save**.
The Sh data source is configured.

Search Criteria Tab

Define the search criteria by entering the following:

1. Select the **Search Criteria** tab.
2. Select how the database is indexed:
 - **NAI** — The database is indexed by NAI (network access ID).
 - **E.164 (MSISDN)** — The database is indexed by E.164 (E.164 phone number).
 - **IMSI** — The database is indexed by International Mobile Subscriber Identity.
3. **Key Transform Pattern** — Regular expression (regex) pattern to use to transform a key.
4. **Key Replace Pattern** — Replacement string to use to transform the key.

For example, **17\$2** means the new string starts with 17 and is followed by the group 2 (\$2) pattern.

5. Click **Save**.

Search Filters Tab

You can configure any number of filters per search type per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters. It is best to order filtered data sources higher than unfiltered ones.

To define filters, on the **Search Filters** tab, enter the following:

1. **Key Type** — Select from the list:

- **NAI** — Network address ID
- **E.164 (MSISDN)** — E.164 phone number
- **IMSI** (default) — International Mobile Subscriber Identity

2. **Expression** — Enter a regular expression. For example:

- **508.*** — Matches numbers beginning with 508
- ***@galactel.com** — Matches strings ending with @galactel.com
- **.*** — Matches any input string

To add the expression to the list, click **Add**. To remove an expression from the list, select it in the list and click **Delete**.

3. Click **Save**.

The Sh data source filters are defined.

Associated Data Sources Tab

If you have defined multiple data sources, you can select which one is associated with this Sh data source on the **Associated Data Sources** tab.

To associate a data source, on the **Associated Data Sources** tab, enter the following:

1. **Associated Data Sources** — Displays a list of defined secondary data sources. Select the data sources to associate with this Sh data source.

Select **Deselect All** if you want to deselect your choices.

2. Click **Save**.

The associated data sources are defined.

Configuring an Sy Data Source

Sy is a Diameter interface between a PCRF and an online charging server (OCS). It provides spending information using policy counter identifiers for a particular subscriber. An MPE device can use this data to drive policy decisions for the subscriber. For information on defining policy counter IDs, see *Policy Wizard Reference*.

The Sy interface is session stateful—a session is normally established when the Gx session for the first PDN is established for a subscriber. A Diameter Subscription for Notification Request (SLR) message causes a subscription to be registered until it is explicitly canceled or the Sy session is lost. A policy

counter read is included with the SLR message. The subscriber's profile indicates whether the subscriber requires the use of policy counters. The MPE device reads a subscriber's policy counters when the subscriber's first session is established, and caches the profile until the subscriber's last session is terminated. If the MPE device receives a Policy Counter Change Notification (SNR) message, the cached policy counters are updated, and policies for all sessions using the policy counters are re-evaluated.

For an Sy data source, you can define a primary, secondary, and tertiary server. An Sy request is sent to the primary connections first. If the primary server is not available, the request is sent to the secondary connection. If the primary and secondary connections are unavailable, the request is sent to the tertiary server. Connections are used in order, always defaulting to the highest server available. As soon as a higher connection is available, requests resume on that connection.

When an Sy data source is defined with an automatic role, that data source is available as an associated data source for the primary data source. Associated data sources are available as secondary and tertiary server data sources on all primary Sy, HSS, or LDAP data sources. You must select the secondary or tertiary Sy data source and associate it with the primary data source to create the connection. Connections are used in order, always defaulting to the highest connection available. As soon as a higher connection is available, calls resume on that connection.

You can specify settings that apply to all Sy data sources. See [Configuring Data Source Interfaces](#) for more information.

Server Info Tab

On the **Server Info** tab, enter the following:

1. **Common** (information common to all configured Sy servers):

- a) **Admin State** — Select to enable this data source.
- b) **Role** — Determines how and when the data sources are used to look up information on the OCS.
 - 1. Select **Automatic** to automatically access a data source, or **On Demand** to use a policy to access a data source.
 - 2. Select **Primary** (default) if this group of data sources will be queried directly when Sy data is needed, or **Secondary** if this group of data sources will be queried only after a successful query to another primary data source.
- c) **Realm** (required) — Defines the Diameter realm of the primary and optional secondary servers; for example, **galactel.com**.
- d) **Unique Name** (required) — Name to identify this group of servers in the CMP database.
- e) **Protocol Timer Profile**—select a protocol timer profile.
- f) Select the **Transport** protocol either **TCP** or **SCTP**.

Indicates whether the Sy data sources support the SCTP protocol. If checked, an MPE device can communicate with the Sy data sources using SCTP. The default is to use the TCP protocol.

- g) Select the number of **Connections** for either transport protocol.

For TCP, select 1 thru 8 connections. (Default is 1.) For SCTP select 8 thru 1 Max Incoming or Outgoing Streams. (Default is 8 for both Incoming and Outgoing Streams.)

2. **Primary Servers:**

- a) **Identity** (required) — Fully qualified domain name (FQDN) of the primary server.

- b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary server. If omitted, the primary identity is used to look up the server address.
- c) **Primary Port** — Primary server port number. The default port number is 3868.

3. Secondary Server:

- a) **Identity** — FQDN of the secondary server.
- b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the backup server. If omitted, the secondary server primary identity is used to look up the server address.
- c) **Primary Port** — Secondary server port number. The default port number is 3868.

4. Tertiary Server:

- a) **Identity** — FQDN of the tertiary server.
- b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the tertiary server. If omitted, the tertiary server primary identity is used to look up the server address.
- c) **Primary Port** — Backup server port number. The default port number is 3868.

5. Click **Save**.

The Sy data source is configured.

Search Criteria Tab

On the **Search Criteria** tab, enter the following:

1. Using the tabs on the left, select how the database is indexed:
 - **Alternate Key** (default) — If the data source role is defined as primary, the window is blank. If the data source role is defined as secondary, the **Alternate Key** fields are available. If the fields are present, enter the **Alternative Key Name**.
 - **NAI** — The database is indexed by NAI (network access ID).
 - **E.164 (MSISDN)** — The database is indexed by E.164 (E.164 phone number).
 - **IMSI** — The database is indexed by International Mobile Subscriber Identity.
2. **Key Transform Pattern** — When searching the database, this is a regular expression (regex) pattern to use to transform a key.
3. **Key Replace Pattern** — When searching the database, this is a replacement string to use to transform the key.
For example, **17\$2** means the new string starts with 17 and is followed by the group 2 (\$2) pattern.
4. Click **Save**.

You have defined the search criteria.

Search Filters Tab

By defining search filters you can configure the MPE device to direct subscriber lookups to particular data sources. If there are multiple Sy data sources, you must define search filters. You can configure any number of filters per search type per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters. Oracle recommends ordering filtered data sources before unfiltered ones.

To define filters, on the **Search Filters** tab, enter the following:

1. Click **Add**.

The **Add Search Key Value** window opens.

2. In the **Key Type** field, select the type:
 - **NAI** (default) — Network address ID
 - **E.164 (MSISDN)** — E.164 phone number
 - **IMSI** — International Mobile Subscriber Identity
 - **Alternate Filter** (if the data source is defined with the role of Secondary) — Specifies a subscriber profile attribute retrieved from the primary data source lookup. For example, if the primary Sh data source returned a subscriber profile attribute named PaymentPlan with a value of either Prepaid or Postpaid, you could set up an alternate filter on the alternate field PaymentPlan to direct Sy lookups for Prepaid subscribers to one data source and lookups for Postpaid to a different data source.
3. In the **Expression** field, enter a regular expression. For example:
 - **508.*** — Matches numbers beginning with 508
 - ***@galactel.com** — Matches strings ending with @galactel.com
 - **.*** — Matches any input string
4. Click **Save**.
The filter is added to the filters list. To remove an expression from the list, select it and click **Delete**.

The Sy data source filters are defined.

Associated Data Sources Tab

If you have defined multiple automatic data sources, you can select which one is associated with this Sy data source on the **Associated Data Sources** tab.

Note: For an Sy data source that has a secondary or tertiary role, or has a role of on-demand, this tab is blank.

To associate a data source:

1. Select the **Associated Data Sources** tab.
2. **Associated Data Sources** — Displays a list of defined data sources. Select the data sources to associate with this Sy data source.

Note: Select **Deselect All** if you want to deselect your choices.

3. Click **Save**.

The associated data sources are defined.

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.

About Reapplying a Configuration

You can reapply the configuration to an individual Policy Management device (server), or to all Policy Management devices in a group. When you reapply the configuration, the CMP system completely reconfigures the servers with topology information, ensuring that the configuration matches the data in the CMP system. 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 server field by field. You should also use the Rediscover Cluster operation to clear the failed status in the Cluster Information Report. See [Rediscovering a Cluster](#) for more information.
- After upgrading the software on a server, it is recommended that you reapply the configuration from the CMP system to ensure that the upgraded server and the CMP system are synchronized.
- The server configuration may 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 server). If such a condition occurs, the CMP system displays the server status on its **System** tab with the notation **Config Mismatch**. You can click the notice to display a report comparing the server configuration with the CMP database information. Reapplying the configuration brings the server back into synchronization with the CMP database.

CMP provides the following methods for reapplying a configuration:

- [Reapplying the Configuration to a Single Device](#)
- [Reapplying the Configuration to a Group of Devices](#)

Reapplying the Configuration to a Single Device

To reapply the configuration associated with an MPE or MRA device:

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.
The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. From the content tree, select the device.
The **Policy Server Administration** page opens to the **System** tab, displaying information for that device.

The device is synchronized with the CMP system.

Reapplying the Configuration to a Group of Devices

To reapply the configuration associated with a group of MPE or MRA devices:

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.
The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. From the content tree, select the group.
The appropriate **Administration** page opens in the work area.
3. From the **Operations** menu, select **Reapply Config**.
The **Bulk Reapply Config** dialog displays stating the number of agents affected.
4. Specify the delay time (in seconds) for applying the operation to each server in the group.
The number of seconds is 0 to 60. 0 is the default.
5. Click **Reapply Config** to reapply the configuration.
An in-progress message appears. After the action completes, the page indicates Reapply Config of MRAs: 2 successful, 0 failed. Successful: <list of devices successfully reconfigured>.

All of the servers in a group are synchronized with the CMP system.

Rediscovering a Cluster

After reapplying a configuration or deleting a failed server, use the Rediscover Cluster operation to refresh the Cluster Information Report. The Rediscover Cluster operation rediscovers the cluster, deleting any failed servers that have been removed from service or refreshing the status of any failed servers after reapplying the configuration.

To rediscover a cluster:

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.
The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. From the content tree, select the a server or cluster.
The appropriate administration page opens in the work area.
3. Click **Rediscover Cluster**.
The Cluster Information Report is updated.

The cluster is rediscovered.

Resetting Counters

The **Reset Counters** option is included in the **Operations** list when the **Stats Reset Configuration** option is set to **Interval**. The **Reset All Counters** option is included in the **Operations** list when the **Stats Reset Configuration** option is set to **Manual**. See [Setting Stats Settings](#) for more information.

To reset the counters associated with a group of MPE or MRA servers:

1. From the **Policy Server** or **MRA** 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 group that contains the servers of interest.
The **Policy Server Administration** page opens in the work area.
3. From the **Operations** list, select **Reset Counters** or **Reset All Counters**.
The **Bulk Reset All Counters** or **Bulk Reset Counters** dialog displays showing the number of servers affected.
4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60.
The default value is 0.

The counters are reset.

Enabling or Disabling All Sh Connections

You can manually enable or disable all Sh connections for all MPE devices in a group. Operations are recorded in the audit log. An alarm is raised if either operation fails.

Note: If the enable or disable operation encounters an exception, the operation is not retried.

To manually disable or enable all Sh connections:

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 group that contains the servers.
The **Policy Server Administration** page opens in the work area.
3. From the **Operations** menu, select **Enable Sh** or **Disable Sh**.
The **Bulk Enable Sh** or **Bulk Disable Sh** dialog displays stating the number of servers affected.
4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60.
0 is the default.
5. Click **Enable Sh** or **Disable Sh** to perform the action.

Sh connections for all of the MPE devices in the group are disabled or enabled.

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 View Select **ALL** from the policy server content tree to view all the defined MPE servers, or 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 22: Group View shows an example of a Group View in which one of the servers is degraded.

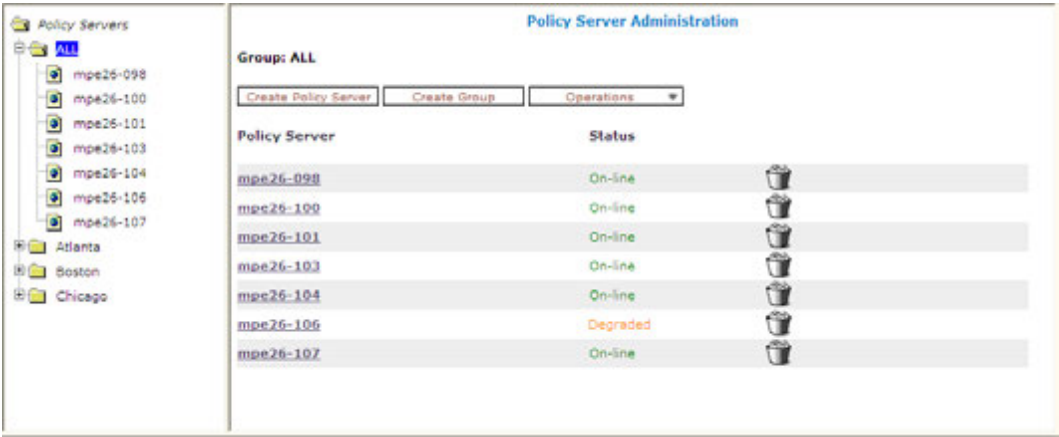


Figure 22: Group View

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	Rediscover the cluster, deleting any failed servers that have been removed from service or refreshing the status of the failed server after reapplying the configuration.
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.
Blades	Information about the individual physical components in the cluster.
Time Period	Information about the current time period and transition status.
Policy Statistics	Information about the execution of policy rules.
Quota Profile Statistics	Information about quota profiles.
Traffic Profile Statistics	Information about traffic profiles.
Session Cleanup Statistics	Information about removal of stranded subscriber sessions.
Sy Reconciliation Statistics	Information about the activity of reconciling Sy sessions after a split-brain event between georedundant MPE devices.
Protocol Statistics	Information about the active network protocols.
Latency Statistics	Information about protocol latency.
Event Trigger Statistics	Information about triggered events.
Error Statistics	Information about any errors, arranged by protocol.
Data Source Statistics	Information about LDAP, Sh, Sy, and SPR activity.
KPI Interval Statistics	Information about the configured reporting interval for key performance indicator (KPI) statistics.

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 following:

- **Cluster Status** — The status of the cluster:
 - **On-line:** If one server, it is active; if two servers, one is active and one is standby; if three servers, one is active, one is standby, one is spare.
 - **Degraded:** One server is active, but at least one other server is not available.
 - **Out-Of-Service:** No server is active.
 - **No Data:** The CMP system cannot reach the server.
- **Site Preference** — The preference of the cluster (Normal or Reversed). Default status is Normal.

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 (the active server). The report also lists the following server-specific information:

- **Overall** — Displays the current topology state (Active, Standby, Forced-Standby, or Spare), 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 file system), average value for the CPU utilization, and memory.

The **Actions** links let you restart the Policy Management software on the server or reboot the server.

Time Period

The Time Period section shows the current time period for the cluster (none indicates that the cluster is not in any time period) and the status of its last transition:

N/A	No time periods are defined, or the cluster has not yet made the transition to any time periods.
Transitioning	The cluster is updating sessions based on the transition of the time period.
Completed	The cluster has updated all affected sessions (either successfully or not) after a time period transition.
Aborted	The transition was stopped by a CMP user.
Incomplete	The transition has not completed, due to a communication failure with an enforcement device.
Cancel	Cancels a transition that is in progress.

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.

To see statistics per policy, click **(details...)**. All existing policies are displayed in a statistics table, with Evaluated, Executed, and Ignored counter values listed for each.

To see details for a specific policy with the distribution of execution time, click the policy name. In addition to Evaluated, Executed, and Ignored, the following details are displayed:

Total Execution Time (ms)	The summary of all execution durations, where execution duration is measured starting at the beginning of the policy conditions evaluation until the execution completion.
Maximum Execution time (ms)	The longest execution duration of the policy.
Average Execution time (ms)	The average of all execution durations of the policy.
Processing Time Statistics	The number of policies processed per time range, in milliseconds. Ranges include <ul style="list-style-type: none"> • 0–20 • 20–40 • 40–60 • 60–80 • 80–100 • 100–150 • 150–200 • 200–250 • >250

Quota Profile Statistics

The Quota Profile Statistics section summarizes quota profile activity within the MPE device. This is presented as a summary table of statistics for all quota profiles executing on the MPE device. For more information on quota profiles, see the *Policy Wizard Reference*.

The following statistics are included:

- **Name** — Name of the quota profiles.
- **Activated** — Number of times the quota profile was activated.
- **Volume Threshold Reached** — Number of times the quota profile reached its volume threshold.
- **Time Threshold Reached** — Number of times the quota profile reached its time threshold.
- **Event Threshold Reached** — Number of times the quota profile reached its event threshold.

To see statistics per quota profile, click **(details...)**. All quota profiles in the MPE device are displayed in a statistics table. To see details for a specific quota profile, click its name.

Traffic Profile Statistics

The Traffic Profile Statistics section summarizes traffic profile activity within the MPE device. This is presented as a table of statistics for each traffic profile that is configured for the MPE device. For more information on traffic profiles, see the *Policy Wizard Reference*.

The following statistics are included:

- **Name** — Name of the traffic profile.
- **Install Attempts** — Number of times the MPE device attempted to install the traffic profile.
- **Removed by PCRF** — Number of times the MPE device removed a traffic profile.
- **Failed or Removed by Gateway** — Number of times the traffic profile failed or was removed by a gateway.
- **Total Retry Attempts** — The total number of retry attempts taken for a successful installation of the PCC or ADC rule.
- **Retry Cycle Attempts** — The number of retry cycles taken before a successful installation of the PCC or ADC rule.
- **Failed after max Retry Cycles** — The number of times a PCC or ADC rule failed to be installed after trying for the maximum retry cycles.

To see statistics per traffic profile, click (**details...**). All traffic profiles in the MPE device are displayed in a statistics table. To see details for a specific traffic profile, click the name of the traffic profile.

Session Cleanup Statistics

The Session Cleanup Statistics section summarizes the activity of removing stale or stranded subscriber sessions within the MPE device.

For information on configuring session cleanup, see [Configuring Expert Settings](#).

The following statistics are included:

- **Ready for Cleanup** — Number of sessions that are stale.
- **Removed on unknown session id** — Number of sessions removed because the session ID is no longer valid.
- **Reauthorized** — Number of sessions reauthorized.
- **Reauthorization Timeout** — Number of sessions for which the reauthorization request timed out.
- **Removed for Expiration** — Number of sessions removed.

Sy Reconciliation Statistics

The Sy Reconciliation Statistics section summarizes the activity of reconciling Sy sessions after a split-brain event between geo-redundant MPE devices.

For information on configuring Sy Reconciliation, see [Configuring Expert Settings](#).

The following statistics are included:

- **Total Run** — The total number of Sy Reconciliation Audits that have been started since the last reset.
- **Total Sessions Audited** — The cumulative number of Sy sessions that have been audited since the last reset.

- **Total Sessions Reconciled** — The cumulative number of Sy sessions that have been reconciled since the last reset.
- **Percentage of Sessions Reconciled** — The percentage of Sy sessions reconciled since the last reset.

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.

Figure 23: Sample Protocol Statistics shows a sample.

Protocol Statistics			
Name	Connections	Total client messages in / out	Total messages timeout
Diameter			
Diameter AF Statistics	3	1733 / 1677	4
Diameter PCEF Statistics	2	2691 / 2691	22
Diameter CTF Statistics	1	0 / 0	N/A
Diameter BBERF Statistics	1	536 / 536	2
Diameter TDF Statistics	1	0 / 0	0
Diameter Sh Statistics	2	1334 / 1334	0
Diameter DRMA Statistics	1	841 / 841	0
Diameter Sv Statistics	0	0 / 0	0
RADIUS			
RADIUS Stats		0 / 0	N/A

Figure 23: Sample Protocol Statistics

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 [Policy and Protocol Specifications](#)).

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 online, 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.

For example, the DRMA statistics include the following:

RUR_SEND_COUNT	The number of RUR messages sent.
RUR_RECV_COUNT	The number of RUR messages received.
RUA_SEND_SUCCESS_COUNT	The number of RUA success messages sent.
RUA_RECV_SUCCESS_COUNT	The number of RUA success messages received.
RUA_SEND_FAILURE_COUNT	The number of RUA failure messages sent.
RUA_RECV_FAILURE_COUNT	The number of RUA failure messages received.
LNR_SEND_COUNT	The number of LNR messages sent.
LNR_RECV_COUNT	The number of LNR messages received.
LNA_SEND_SUCCESS_COUNT	The number of LNA success messages sent.
LNA_RECV_SUCCESS_COUNT	The number of LNA success messages received.
LNA_SEND_FAILURE_COUNT	The number of LNA failure messages sent.
LNA_RECV_FAILURE_COUNT	The number of LNA failure messages received.
LSR_SEND_COUNT	The number of LSR messages sent.
LSR_RECV_COUNT	The number of LSR messages received.
LSA_SEND_SUCCESS_COUNT	The number of LSA success messages sent.
LSA_RECV_SUCCESS_COUNT	The number of LSA success messages received.
LSA_SEND_FAILURE_COUNT	The number of LSA failure messages sent.
LSA_RECV_FAILURE_COUNT	The number of LSA failure messages received.

Latency Statistics

The Latency Statistics section summarizes latency information, for Diameter protocols, within the MPE device. This is presented as a table of statistics for each configured protocol. Each protocol lists the number of connections.

To see details for a specific protocol, click the protocol name. Statistics are displayed for the maximum and average transaction time for messages sent and received, as well as the distribution of execution times.

You can control the information displayed within the detailed report using the following buttons:

Reset Counters	Resets all latency counters.
Show Absolute/Show Deltas	Switches between absolute mode (statistics between last reset) and delta mode (statistics since last display).

Pause/Resume	Stops or restarts automatic refreshing of displayed information. The refresh period is ten seconds.
Cancel	Returns to the previous page.

Event Trigger Statistics

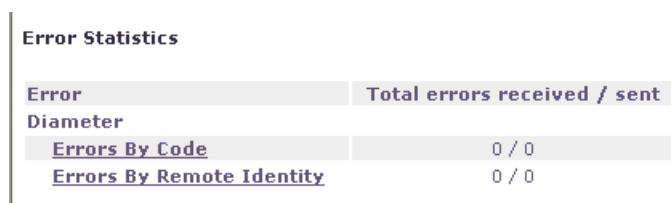
The Event Trigger Statistics section summarizes any event triggers reported by the MPE device. This is presented as a table of overall statistics for event triggers by code and event triggers by application.

You can click the name of each entry in the Event Trigger table to display a detailed report page listing activity by specific event triggers.

Error Statistics

The Error Statistics section summarizes any protocol-related errors reported by the MPE device. This is presented as a table of overall statistics for each protocol that is configured for the MPE device.

[Figure 24: Sample Error Statistics](#) shows a sample.



Error Statistics	
Error	Total errors received / sent
Diameter	
Errors By Code	0 / 0
Errors By Remote Identity	0 / 0

Figure 24: Sample Error Statistics

The following summary statistics are displayed:

Error	List of protocols configured on this MPE device.
Total errors received/sent	Total number of errors received or sent in this protocol.

You can click the name of each entry in the Error Statistics table to display a detailed report page. For most protocols, this report page displays a set of counters that break down the errors by error code and the remote identity of each client or server with which the MPE device is communicating through that protocol.

Data Source Statistics

The Data Source Statistics section summarizes the data source activity within the MPE device. Information is available for each data source. You can click the name of each entry in the Data Source Statistics table to display a detailed report page.

LDAP Statistics

For an LDAP data source, the **Data Source Statistics** page displays the following statistics:

- Number of successful searches
- Number of unsuccessful searches

- Number of searches that failed because of errors
- Max Time spent on successful searches (ms)
- Max Time spent on unsuccessful searches (ms)
- Average time spent on successful searches (ms)
- Average time spent on unsuccessful searches (ms)
- Number of successful updates
- Number of unsuccessful updates
- Number of updates that failed because of errors
- Time spent on successful updates (ms)
- Time spent on unsuccessful updates (ms)
- Max Time spent on successful update (ms)
- Max Time spent on unsuccessful update (ms)
- Average time spent on successful updates (ms)
- Average time spent on unsuccessful updates (ms)

Sh Statistics

For an Sh data source, the **Data Source Statistics** page displays the following statistics:

- Number of successful searches
- Number of unsuccessful searches
- Number of searches that failed because of errors
- Number of search errors that triggered the retry
- Number of search timeouts that triggered the retry
- Max Time spent on successful search (ms)
- Max Time spent on unsuccessful search (ms)
- Average time spent on successful searches (ms)
- Average time spent on unsuccessful searches (ms)
- Number of successful updates
- Number of unsuccessful updates
- Number of updates that failed because of errors
- Number of update errors that triggered the retry
- Number of update timeouts that triggered the retry
- Time spent on successful updates (ms)
- Time spent on unsuccessful updates (ms)
- Max Time spent on successful update (ms)
- Max Time spent on unsuccessful update (ms)
- Average time spent on successful updates (ms)
- Average time spent on unsuccessful updates (ms)
- Number of successful subscriptions
- Number of unsuccessful subscriptions
- Number of subscriptions that failed because of errors
- Number of subscription errors that triggered the retry
- Number of subscription timeouts that triggered the retry
- Time spent on successful subscriptions (ms)
- Time spent on unsuccessful subscriptions (ms)

- Max Time spent on successful subscription (ms)
- Max Time spent on unsuccessful subscription (ms)
- Average time spent on successful subscriptions (ms)
- Average time spent on unsuccessful subscriptions (ms)
- Number of successful unsubscriptions
- Number of unsuccessful unsubscriptions
- Number of unsubscriptions that failed because of errors
- Number of unsubscription errors that triggered the retry
- Number of unsubscriptions timeouts that triggered the retry
- Number of searches from session updates
- Time spent on successful unsubscriptions (ms)
- Time spent on unsuccessful unsubscriptions (ms)
- Max Time spent on successful unsubscription (ms)
- Max Time spent on unsuccessful unsubscription (ms)
- Average time spent on successful unsubscriptions (ms)
- Average time spent on unsuccessful unsubscriptions (ms)

Sy Statistics

For an Sy data source, the **Data Source Statistics** page displays the following statistics:

- Number of successful searches
- Number of unsuccessful searches
- Number of searches that failed because of errors
- Max Time spent on successful search (ms)
- Max Time spent on unsuccessful search (ms)
- Average time spent on successful searches (ms)
- Average time spent on unsuccessful searches (ms)

SPR Statistics

For an SPR system, the **Data Source Statistics** page displays the following statistics:

- Number of successful searches
- Number of unsuccessful searches
- Number of searches that failed because of errors
- Max Time spent on successful search (ms)
- Max Time spent on unsuccessful search (ms)
- Average time spent on successful searches (ms)
- Average time spent on unsuccessful searches (ms)
- Number of successful updates
- Number of unsuccessful updates
- Number of updates that failed because of errors
- Time spent on successful updates (ms)
- Time spent on unsuccessful updates (ms)
- Max Time spent on successful update (ms)
- Max Time spent on unsuccessful update (ms)

- Average time spent on successful updates (ms)
- Average time spent on unsuccessful updates (ms)
- Number of successful subscriptions
- Number of unsuccessful subscriptions
- Number of subscriptions that failed because of errors
- Number of successful unsubscriptions
- Number of unsuccessful unsubscriptions
- Max Time spent on successful unsubscription (ms)
- Max Time spent on unsuccessful unsubscription (ms)
- Average time spent on successful unsubscriptions (ms)
- Average time spent on unsuccessful subscriptions (ms)

Database Statistics

The Database Statistics section summarizes the read/write activity for the MPE device database. Click **Database Status Statistics** to display the last reset time (that is, the last time that you clicked **Reset All Counters**), the last collection time, and cumulative read/write activity. Data is collected every 10 seconds.

KPI Interval Statistics

The KPI Interval Statistics section summarizes the maximum key performance indicator (KPI) values recorded by the Policy Management cluster during the previous recording interval. Intervals are recorded on the quarter hour.

The following interval statistics are displayed:

Interval StartTime	Timestamp of when the current interval started.
Configured Length (Seconds)	Configured interval length. The value of 900 seconds (15 minutes) is fixed.
Actual Length (Seconds)	Actual interval length. When data is collected over a full interval, this value matches the Configured Length value.
Is Complete	Displays 0 or 1, where 1 indicates that data was collected for a full interval.
Interval MaxTransactionsPerSecond	The highest value of the counter MaxTransactionsPerSecond during the previous interval.
Interval MaxMRABindingCount	The highest value of the counter MaxMRABindingCount during the previous interval. (This value is 0 on MPE clusters.)
Interval MaxSessionCount	The highest value of the counter MaxSessionCount during the previous interval.
Interval MaxPDNConnectionCount	The highest value of the counter MaxPDNConnectionCount during the previous interval.

You can control the information displayed within the detailed report using the following buttons:

Pause/Resume	Stops or restarts automatic refreshing of displayed information.
---------------------	--

Cancel

Returns to the previous page.

Note: If a cluster has just started up and no data is available, the Interval StartTime is displayed as Undefined and the maximum values are displayed as 0. If a cluster has started up and a recording interval has completed but it is less than 15 minutes, the value of Actual Length will not match Configured Length, and the maximum values are displayed as 0.

Viewing Policy Server Logs

The log files trace the activity of a Policy Management device. 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 Log Settings** — Records the policy-level messages.
- **Policy Syslog Forwarding** — Records policy-processing activity. Supports the standard UNIX logging system, in conformance with RFC 3164.
- **SMS log** — Contains all Short Messaging Service messages sent by the MPE device as well as any ACK messages received from an SMS Center (SMSC) server or its equivalent
- **SMPP log** — Contains all Short Message Peer-to-Peer Protocol (SMPP) notifications sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server.
- **SMTP log** — Contains all Simple Mail Transfer Protocol (SMTP) messages sent by the MPE device.
- **HTTP log** — Contains all Hypertext Transfer Protocol (HTTP) messages sent by the MPE device.

Viewing the Trace Log

The trace log records Policy Management application notifications, such as protocol messages, policy 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.

The activity of the Policy Rules Engine is recorded in a trace log at eight levels: Emergency (ID 4560), Alert (ID 4561), Critical (ID 4562), Error (ID 4563), Warning (ID 4564), Notice (ID 4565) Info (ID 4566), and Debug (ID 4567). You can configure the severity level of messages that are recorded in the trace log.

To view the Trace log:

1. Select the device to view:

- To view an MPE device, from the **Policy Server** section of the navigation pane, select **Configuration**.
- To view an MRA device, from the **MRA** 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 , select the starting date and time, then click **Enter**.
- **End Date/Time** — Click , 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** display.

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 in events last month and this month, only results from this month are listed.

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** — When 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** — When 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. 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. For information on policy actions, see the *Policy Wizard Reference*.

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

You can define multiple destinations for notifications and filter notifications by severity level. For more information, see [Configuring Log Settings](#).

The SMS Log

The SMS log, `/var/Camiant/log/smsr.log`, contains all Short Message Service (SMS) messages sent by the MPE device as well as any ACK messages received from an SMS Center (SMSC) server or its equivalent. You can configure the severity level as well as the destination IP addresses of messages that are written to the SMS log. The default severity level is WARN. See [Configuring Log Settings](#) for more information.

The SMPP Log

The SMPP log is a policy action-generated notification that contains all Short Message Peer-to-Peer Protocol notifications sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server. In SMPP or XML mode, SMPP information appears on the **Logs** tab of the **Policy Server Administration** page. You can modify the severity of messages that are written to the SMPP log on the MPE configuration page. The default severity is WARN. See [Configuring Log Settings](#) to modify the settings.

The SMTP Log

The SMTP log contains all Simple Mail Transfer Protocol (SMTP) messages sent by the MPE device, as well as any ACK messages received from a Mail Transfer Agent (MTA). In SMPP or XML mode, the SMTP log information appears on the **Logs** tab of the **Policy Server Administration** page. You can modify the severity level of messages that are written to the SMTP log on the MPE configuration page. The default severity is WARN. See [Configuring Log Settings](#) to modify the settings.

The HTTP Log

The HTTP log contains all Hypertext Transfer Protocol (HTTP) messages sent by the MPE device. In SMPP or XML mode, the HTTP log information appears on the **Logs** tab of the **Policy Server Administration** page. You can modify the severity level of messages that are written to the HTTP log on the server configuration page. The default severity is WARN. See [Configuring Log Settings](#) for more information.

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** (default) — 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 log level setting from its default value (for example, from **Warn** to **Info**) causes more notifications to be recorded in the log and can adversely affect performance. Similarly, raising the log level setting (for example, from **Warn** to **Alert**) causes fewer notifications to be recorded in the log and may cause you to miss important notifications.

7. In the **Modify Policy Log Settings** section of the page, configure the **Policy Log Level**.

This setting indicates the minimum severity of messages that are recorded in the policy log for all policies. The levels are:

- **OFF** — No messages are recorded.
- **DEBUG** — All messages are recorded.
- **INFO** — Only informational messages are recorded.
- **WARN** (default) — Only messages designating potentially harmful situations are recorded.

8. To configure the **Modify Policy Syslog Forwarding Settings**, for each system, enter the following:

- a) **Hostname/IP Addresses** — Remote system host name or IP address (either IPv4 or IPv6 format).



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) **Facility** — Select from **Local0** (default) to **Local7**.

- c) **Severity** — Filters the severity of notifications that are written to syslog:

- **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** (default) — 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.

9. In the **Modify SMPP Log Settings** section of the page, configure the following:

- a) **SMPP Log Level** — Indicates the severity of messages that are written to the file `SMPP.log`.

Adjusting this setting allows any new events, at or above the configured severity, to be written to the SMPP log.

Note: You can optionally enable the syslog forwarding address for new logs.

Valid levels are:

- **OFF** — Turns off logging.
- **ERROR** — Designates error events which may or may not be fatal.
- **WARN** (default) — Designates potentially harmful situations.
- **INFO** — Designates informational messages highlighting overall progress.
- **DEBUG** — Designates information events of lower importance.
- **TRACE** — Designates informational events of very low importance.
- **ALL** — Records all logging levels.

- b) **SMPP Log Forwarding IP Addresses** — You can forward SMPP log entries to multiple syslog servers.

10. In the **Modify SMTP Log Settings** section of the page, configure the **SMTP Log Level**.

This setting indicates the minimum severity of messages that are recorded in the SMTP 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 SMTP log. The levels are:

- **OFF** — Turns off logging.
- **ERROR** — Designates error events which may or may not be fatal.
- **WARN** (default) — Designates potentially harmful situations.
- **INFO** — Designates informational messages highlighting overall progress.
- **DEBUG** — Designates information events of lower importance.
- **TRACE** — Designates informational events of very low importance.
- **ALL** — Records all logging levels.

11. In the *Modify HTTP Log Settings* section of the page, configure the **HTTP Log Level.**

This setting indicates the minimum severity of messages that are recorded in the HTTP log. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the HTTP log. The levels are:

- **OFF** — Turns off logging.
- **ERROR** — Designates error events which may or may not be fatal.
- **WARN** (default) — Designates potentially harmful situations.
- **INFO** — Designates informational messages highlighting overall progress.
- **DEBUG** — Designates information events of lower importance.
- **TRACE** — Designates informational events of very low importance.
- **ALL** — Records all logging levels.

12. Click *Save*.

The log settings are configured.

Analytics Data Stream

You can obtain a data feed with real-time analytics data from one or more MPE devices. This feature is referred to as Oracle Communications Policy Management Analytics and is generated by events that occur in the system. The analytics data stream (ADS) contains data about message processing in the MPE device and specific details about the policies that are triggered by those messages. The policy-related messages in the ADS are known as Policy Event Records (PERs).

Data contained in ADS messages can be analyzed by a third-party analytics system. The MPE device supports load-balancing of ADS messages across multiple connections for efficient transmission to a single analytics client.

Data is sent as a byte-encoded set of type length values (TLV) over a client-initiated TCP connection. The analytics client implements a customized interface to read and process the data sent from the MPE device over the connection. TLVs represent different pieces of information about an event, which when pieced together make up an ADS message.

The Oracle Communications Policy Management Analytics feature is implemented using a defined set of TLVs so that the data sent from the MPE device can be targeted at any third-party analytics client. Refer to *Analytics Data Stream Reference* for a list of supported TLVs for the feature.

The ADS feature is configured from the **Mode Settings** page. See [CMP Modes](#) for information on configuring the ADS feature.



Caution: CMP operating modes should only be set in consultation with My Oracle Support. Setting modes inappropriately can result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

After the feature is configured, ADS can be enabled for specified MPE devices (see [Configuring MPE Protocol Options](#)) or policies or policy groups (see *Policy Wizard Reference*).

Chapter 5

Configuring Protocol Routing

Topics:

- [*Configuring Diameter Peers.....140*](#)
- [*Configuring Diameter Realm Based Peer Routes.....142*](#)

Routing enables a Policy Management device to forward requests to other Policy Management devices for further processing. The following routing messages and protocols are supported:

- Diameter applications: Rx, Gq, Ty, Gxx, Gx, Gy, and Sd

Configuring Diameter Peers

The MPE and MRA devices support Diameter Rx, Gq, Ty, Gxx, Gx, Gy, S9, and Sd applications. For example, traffic control is supported using the Diameter Gx application. When a subscriber attaches to the network (for example, using a phone) via a GGSN (Gateway GPRS Support Node), the GGSN can establish a session with both the MPE and MRA devices using a Diameter Gx CCR (Credit Control Request) message. The MPE and MRA devices respond to the request with a Gx CCA (Credit Control Answer) message.

Use this procedure if you need to configure system devices (peers) to a diameter-based network.

To configure Diameter peers for either an MPE or MRA device:

1. Either in the **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server or MRA groups.
2. From the content tree, select the MPE or MRA device.
The **Administration** page for that device opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings appear.
4. Click **Modify Peers** which opens the **Modify the Diameter Peer Table**.
5. Add a peer to the table using these steps.
 - a) Click **Add**.

The **Add Diameter Peer** window opens.




Figure 25: Add Diameter Peer

- b) Enter the following:
 - **Configured MRAs/MPes (optional)** — If you are defining an existing Policy Management cluster as a Diameter peer, select it from this list; the other fields are populated.

- **Name** (required) — Name of the peer device (which must be unique within the CMP database).
- **IP Address** (required) — IP address in IPv4 or IPv6 format of the peer device.
If not specified, the MPE device uses a DNS lookup to resolve the value in the Diameter Identity field into an IP address and try to connect.
- **Diameter Realm** (required) — The peer's domain of responsibility (for example, **Example.com**).
- **Diameter Identity** (required) — Fully qualified domain name (FQDN) of the peer device (for example, **mpe33.Example.com**).
- **Protocol Timer Profile** — Select from the list.
- **Initiate Connection** — Select to initiate an S9 connection for this Diameter peer.
- **Transport** — Select either **TCP** or **SCTP** (shown as Transport Info in the Diameter peer table). For TCP select **Connections** (range 1-8, default 1). For SCTP select **Max Incoming Streams** and **Max Outgoing Streams**(1-8 connections, default is 8) which will be shown as Connection Info in the Diameter peer table.
- **IP Port** — Enter the IP Port number.
- **Watchdog Interval** — Enter the watchdog interval in seconds. The default is 30 seconds.
- **Reconnect Delay** — Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout** — Enter the response timeout interval in seconds. The default is 5 seconds.

c) Click **Save**.

6. Complete these steps to add, edit or delete additional Diameter Peers.

- Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is added to the table
- Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
- Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.

7. Click **Save**.

Configuring Diameter Realm Based Peer Routes

By default, Diameter messages are processed locally. In a network with multiple Policy Management devices, messages can be routed, by realm, application, or user ID, for processing by peers or other realms.




Note: Diameter messages can be routed in either an MPE or MRA the steps listed below can be used for either device.

Use this procedure if you have an extensive peer network or a network that includes multiple realms, user IDs or applications.



To configure the Diameter realm based peer routes:

1. From the Policy Management device (either **Policy Server** or **MRA** 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 Server** or **MRA** that needs diameter routing.
The **Policy Server Administration** or **MRA Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings display.
4. Click **Modify Routes**.
The **Modify the Diameter Route Table** page opens.
5. Add a route to the table
 - a) Click **Add**.
The **Add Diameter Route** window opens.
 - b) Configure the route using the following fields.
 - **Diameter Realm** — For example, **Example.com**.
 - **Application ID** — Select **Rx** (default), **Gq**, **Ty**, **Gx**, **Gxx**, **Sd**, **Sh**, **Sy**, **Gy**, **S9**, or **All**.
Note: You can include only one application per route rule. For multiple applications, create multiple rules.
 - **User ID type** — Select **ANY** (default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
 - **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use a period followed by an asterisk (.) as a wildcard character. To add the user ID to the list, click **Add**; to remove one or more user IDs from the list, select them and click **Delete**.
 - **Evaluate as Regular Expression** — The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards.
Note: Regular expressions are specifically JAVA expressions and using any other language expression will result in a failed status. See [Examples of JAVA Regular Expressions for MRA Routes](#) for more information about using regular expressions for MRA routes.
 - **Action** — Select **PROXY** (stateful route, default), **RELAY** (stateless route), or **LOCAL** (process on this device).
 - **Server ID** — Select a destination peer from the list.

Note: You can define a server with a Diameter identity.

- c) Click **Save**.
6. (Optional) Add, delete, modify, or order entries.
 - Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is added to the table
 - Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
 - Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.
 - Ordering the list.

If you define multiple entries, they are searched in the order displayed in this list. To change the order:

 1. Select an entry.
 2. Click  **Up** or  **Down**. The search order is changed.
7. Define the default route:
 - a) Click **Edit** in the **Default Route** section.
 - b) Select the default action: **PROXY**, **RELAY**, or **LOCAL**.
 - c) Select the peer server ID.
 - d) Click **Save**.
8. To delete the default route, click **Delete**.
9. Click **Save**.

The Diameter realm based peer routes are configured.

Chapter 6

Configuring Advanced Device Settings

Topics:

- [*Configuring Expert Settings.....145*](#)
- [*Configuring Service Overrides.....151*](#)
- [*About Overload Controls.....153*](#)
- [*Resetting Configuration Keys to Defaults.....157*](#)
- [*Filtering the Configuration Keys.....158*](#)
- [*Exporting the Configuration Keys.....159*](#)

This chapter describes how to configure and manage expert settings, service overrides, and load shedding options.

Configuring Expert Settings

Expert settings control global settings that are not used regularly. For example, session cleanup options and timers. These settings are set for a specific MPE or MRA device.

1. View the device list.

- For an MPE device, go to the **Policy Server** section of the navigation pane and select **Configuration**.
- For an MRA device, go to the **MRA** section of the navigation pane and select **Configuration**.

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

2. From the content tree, select the device.

- For an MPE device, select the **Policy Server** tab.
- For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

3. Click **Advanced**.

The advanced settings for the device display.

4. Click **Modify**.

The advanced configuration settings can be edited.

5. Select a configuration key in the **Expert Settings** table and click **Edit**.

The **Edit Expert Setting Value** dialog opens.

6. Modify the settings and click **OK** to save.

See [Table 2: Expert Settings for MPE](#) and [Table 3: Expert Settings for MRA](#) for information about the configurations keys.

Table 2: Expert Settings for MPE

Category	Configuration Key	Description	Default
Admission	ADMISSION.DIAMETER.RequestProcessingLimit	The maximum amount of time a request can be processed before being dropped, if no answer has been sent. Specified in milliseconds.	5000
Diameter	DIAMETER.AF.AuditForAuthLifetime	Enables the configuration of a minimum and maximum lifetime for an AF session.	False
Diameter	DIAMETER.AF.AuthLifetime	The maximum lifetime of an AF session. Otherwise the corresponding AF session would be purged subject to the configured grace period. Specified in seconds. Valid range is 300–58060800.	86400 (1 day)
Diameter	DIAMETER.AF.EnableGracePeriodForSubscriptionExpiry	Enables the configuration of a grace period for an AF session.	False
Diameter	DIAMETER.AF.GracePeriodForSubscriptionExpiry	Indicates the maximum configured grace period for an AF session, which is added to the negotiated AuthLifeTime	86400 (1 day)

Configuring Advanced Device Settings

Category	Configuration Key	Description	Default
		to determine if a given AF session can be considered stale and purged. Specified in seconds. Valid range is 0–86400.	
Diameter	DIAMETER.AF.MinAuthLifetime	The minimum lifetime of an AF session. Otherwise the corresponding AF session would be purged subject to the configured grace period. Specified in seconds.	300
Diameter	DIAMETER.AF.SignallingSessionAuthLifetime	Indicates the maximum configured period for an Rx sessions containing signaling flow past which the session is considered stale. Specified in seconds. Valid range is 300–58060800.	259200 (3 days)
Diameter	DIAMETER.Cleanup.AuditRxSessions	If enabled, an RAR message is sent for auditing. Note: This is for future releases and has not been implemented yet.	False
Diameter	DIAMETER.Cleanup.AuditSySendEmptyPolicyCounterList	If enabled, the Policy Counter Identifier subscription list is not sent as part of an SLR (INTERMEDIATE) message to audit stale Sy sessions. If disabled, the current Policy Counter Identifier subscription list is sent as part of an SLR (INTERMEDIATE) message to audit stale Sy sessions.	True
Diameter	DIAMETER.Cleanup.AuditSySessions	If enabled, an SLR (INTERMEDIATE) message is sent for auditing. If disabled, the Sy session is checked for an association with an IP-CAN session. If there are no IP-CAN associations, the Sy session is considered active; otherwise, the session is deleted. Note: This is for future releases and has not been implemented yet.	False
Diameter	DIAMETER.Cleanup.CleanupStaleRxSessions	Determines if the MPE device should consider AF sessions in the regular cleanup cycles. If enabled, AF sessions are considered expired if they have lived longer than the specified AFSessionValidityTime. Note: At that point, in future releases, if AuditAFSessions is set to True, an RAR will be sent for auditing the session.	True
Diameter	DIAMETER.Cleanup.MaxDurationForSessionIteration	The maximum duration in seconds to iterate through the sessions. Valid range is 1–86400.	7200 (2 hours)

Configuring Advanced Device Settings

Category	Configuration Key	Description	Default
Diameter	DIAMETER.Cleanup.MaxSessionCleanupRate	The rate (in sessions/sec) at which the cleanup task attempts to clean stale sessions. Valid range is 1–5000.	50
Diameter	DIAMETER.Cleanup.MaxSessionIterationRate	The rate (in sessions/sec) at which the cleanup task iterates through the sessions database. Valid range is 1–100000.	1000
Diameter	DIAMETER.Cleanup.MaxSySessionValidityTime	The maximum amount of time in seconds after which the Sy session is cleaned up on any error. Valid range is 1–8640000.	172800 (2 days)
Diameter	DIAMETER.Cleanup.OverrideCleanupAudit	This specifies if the regular audit processing for cleaning up a stale session is overridden. When enabled, the cleanup task bypasses the audit process and deletes all sessions that are stale for the session validity time.	False
Diameter	DIAMETER.Cleanup.RXSessionValidityTime	The amount of time in seconds after which the session is expired and is purged if EnabledAFSessionCleanup is enabled.	86400 (1 day)
Diameter	DIAMETER.Cleanup.SessionCleanupInterval	The amount of time in seconds after which the cleanup task will run to look for stale sessions.	21600 (5 hours)
Diameter	DIAMETER.Cleanup.SessionCleanupStartTime	Schedules the cleanup task once a day at a specified time. If the start time is specified, then it is scheduled to run once a day at the given time. The value can be specified in either a 24-hr format (<i>HH:mm</i>) or an exact date and time (<i>YYYY-MM-ddThh:mm:ss</i>) of when it will first run and then repeat at the interval specified.	undefined
Diameter	DIAMETER.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Valid range is 1–8640000.	432000 (5 days)
Diameter	DIAMETER.Cleanup.SySessionValidityTime	The amount of time in seconds after which the session is declared stale and deemed a candidate for cleanup.	36000 (10 hours)
Diameter	DIAMETER.EnableSessionCleanUp	Enables the DiameterSessionCleanUp Task.	True
Diameter	DIAMETER.ENF.MaxTimeForAnGwFailure	The maximum time allowed after getting indication for SGW failure in which the MPE device does not send any new or updated policies to the P-GW except rules to be removed. Specified in seconds.	3600

Configuring Advanced Device Settings

Category	Configuration Key	Description	Default
Diameter	DIAMETER.ENF. ReevaluateGeneratedDefaultRule	If set to True, on receipt of a session update request the MPE device evaluates the flow which contains the generated default rule even when there is no new default-EPS-Bearer-QoS information in the request.	False
Diameter	DIAMETER.ENF. RegisterForAnGwChangeWithSGWRest	If the SGW-Rest supported feature was negotiated and the value of this parameter is false, the MPE device checks if AN_GW_CHANGED event trigger is one of the armed event triggers to be installed and removes it. As a result, the MPE device will not register for AN_GW_CHANGE.	False
Diameter	DIAMETER.PCEF.NetLocSupportedAccesses	<p>A combination of values used for network location (NetLoc) support. The format is <i>IPCanType:RATType:AN-Trusted</i>. If not set, any types or values are applicable. For example:</p> <p>THREEGPP_GPRS means to support NetLoc as if <i>IPCanType=THREEGPP_GPRS</i>.</p> <p>NON_THREEGPP_EPS:WLAN:TRUSTED means to support NetLoc when <i>IPCanType=NON_THREEGPP_EPS</i>, <i>RATType=WLAN</i>, and <i>ANTrusted=TRUSTED</i>.</p> <p>NON_THREEGPP_EPS::TRUSTED means to support NetLoc when <i>IPCanType=NON_THREEGPP_EPS</i> and <i>ANTrusted=TRUSTED</i>.</p> <p>:: means all accesses support NetLoc.</p>	THREEGPP_GPRS, THREEGPP_EPS, NONTHREEGPP_EPS:WLAN:TRUSTED
Diameter	DIAMETER.SessionUniquenessControl	If enabled (True), the MPE cluster will maintain session uniqueness and avoid stale session processing.	False
Diameter	DIAMETER. SessionUniquenessControlWaitTime	If enabled (True), the Max-Wait-Time AVP is used in conjunction with the message origination time stamp to determine staleness of message.	False
PCMM	PCMM.Cleanup.CleanupStalePcmmSessions	Enables the inclusion of PCMM sessions in regular cleanup cycles. If enabled (True), PCMM sessions are considered expired if they have lived longer than the specified <i>PcmmSessionValidityTime</i> or license timeout duration configured in the application.	

Configuring Advanced Device Settings

Category	Configuration Key	Description	Default
PCMM	PCMM.Cleanup.PcmmSessionValidityTime	The amount of time in seconds after which the session is deemed expired and is purged if the setting EnabledAFSessionCleanup is enabled.	86400 (1 day)
SH	SH.Retry.Enabled	If enabled, indicates that the MPE device retries the Sh Requests for UDR, PUR, and SNR to the backup server when the primary server returns one of the defined error codes. PNA messages are not retried. If the backup server returns an error, then retry is not performed on the primary server.	False
SH	SH.Retry.EnabledOnTimeout	If enabled with the SH.Retry.Enabled setting, allows the MPE to retry an Sh Request to a backup datasource server when there is a response timeout. If the request to backup server times out, then a retry is not performed on the primary server. This setting depends on the configuration of the SH.Retry.Enabled and SH.ResponseTimeout settings. You can configure the SH.ResponseTimeout in the Service Overrides section of the Advanced Settings page.	False
SMPP	SMPP.SendSMSNowWhenDeliveryDateInPast	In SMS:SMPP mode, determines if SMS notifications scheduled to be delivered in the past will be dropped or delivered. If false, SMS notifications scheduled to be delivered on a date in the past will be dropped. If true, SMS notifications scheduled to be delivered on a date in the past will be delivered immediately.	False
SMSXML	SMSXML.SendSMSNowWhenDeliveryDateInPast	In SMS:XML mode, determines if SMS notifications scheduled to be delivered in the past will be dropped or delivered. If false, SMS notifications scheduled to be delivered on a date in the past will be dropped. If true, SMS notifications scheduled to be delivered on a date in the past will be delivered immediately.	False
SY	SY.Reconciliation.Enabled	Determines whether the Sy Reconciliation is activated and an audit of Sy sessions will be executed on a recovery from a split-brain scenario.	False
SY	SY.Reconciliation.HoldTimer	The time in seconds after receipt of a notification of recovery from a split-brain scenario the Sy Reconciliation task will wait before starting.	180
SY	SY.Reconciliation.MaxSessionReconcileRate	The rate (in sessions/sec) at which the tasks will attempt to send Sy SLR Messages to reconcile Sy sessions.	50

Category	Configuration Key	Description	Default
SY	SY.SendOriginationTimestamp	If enabled (True), the message origination timestamp will be included as part of the initial SLR Sy message.	False

Table 3: Expert Settings for MRA

Category	Configuration Key	Description	Default
Admission	ADMISSION.DIAMETER.RequestProcessingLimit	The maximum amount of time in milliseconds a request can be processed before being dropped, if no answer has been sent.	5000
Diameter	DIAMETERDRA.Cleanup.BindingCleanupInterval	The interval in seconds at which the cleanup task that looks for stale bindings occurs. Valid range is 1-8640000.	86400 (1 day)
Diameter	DIAMETERDRA.Cleanup.BindingValidityTime	The amount of time in seconds elapsed until a binding is deemed stale. Valid range is 1-8640000.	864000 (10 days)
Diameter	DIAMETERDRA.Cleanup.CheckForStaleBindings	Check for stale bindings during the cleanup cycle, which is determined by the current time being greater than the DIAMETERDRA.Cleanup.BindingValidityTime. If this is set to false, the cleanup task will not check if the entire binding is stale.	False
Diameter	DIAMETERDRA.Cleanup.CheckForStaleSessionsInBinding	Check for stale sessions in binding determined by the current time being greater than the SessionValidityTime. If this is disabled, the cleanup task checks the entire binding only.	True
Diameter	DIAMETERDRA.Cleanup.CheckForSuspectBindings	Check for suspect bindings during the cleanup cycle. If this is set to false, the cleanup task checks that an entire binding is stale.	True
Diameter	DIAMETERDRA.Cleanup.CleanupStartTime	Schedules the cleanup task once a day at a specified time. If a time is specified, then it is scheduled to run once a day at the given time. The value can be specified in either a 24-hr format (<i>HH:mm</i>) or an exact date and time (<i>YYYY-MM-ddThh:mm:ss</i>) of when it will first run and then repeat at the interval specified.	
Diameter	DIAMETERDRA.Cleanup.MaxBindingCleanupRate	The rate (in bindings/sec) at which the cleanup task attempts to clean stale bindings. Valid range is 1-40000.	250

Configuring Advanced Device Settings

Category	Configuration Key	Description	Default
Diameter	DIAMETERDRA.Cleanup.MaxBindingIterationRate	The rate (in bindings/sec) at which the cleanup task iterates through the binding database. Valid range is 1–100000.	1000
Diameter	DIAMETERDRA.Cleanup.MaxDurationForBindingIteration	The maximum duration in seconds to iterate through the bindings. Valid range is 1-2147483647.	21600 (5 hours)
Diameter	DIAMETERDRA.Cleanup.MaxSessionValidityTime	The maximum amount of time in seconds after which the session is cleaned up on any error. Valid range is 1–8640000.	864000 (10 days)
Diameter	DIAMETERDRA.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Valid range is 1–8640000.	432000 (5 days)
Diameter	DIAMETERDRA.StaticMigrationModeEnabled	Enables the static to stateful MRA migration mode. While in this mode, static routes are used for MPE selection only.	False
Diameter	DIAMETERDRA.Routing.RemoteDiversion	If enabled, the MRA will divert messages remotely when necessary.	False
Diameter	DIAMETERDRA.Routing.LocalDiversion	If enabled, the MRA will divert messages locally when necessary.	True
Diameter	DIAMETERDRA.Routing.FailedDiversionResult	Determines the Result Code to use when the MRA can not perform local or remote diversion. The format is <i>VendorID:Code</i> . If the <i>VendorID</i> is not needed, use a value of 0 (zero). The default is DIAMETER_TOO_BUSY.	0:3004

7. Click **Save**.

The settings are applied to the selected device.

Configuring Service Overrides



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

Configuration key changes are made using the **Service Overrides** section of the Advanced configuration page.

Make service override changes as follows:

1. View the device list.

- For an MPE device, go to the **Policy Server** section of the navigation pane and select **Configuration**.
- For an MRA device, go to the **MRA** section of the navigation pane and select **Configuration**.

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

2. From the content tree, select the device.
 - For an MPE device, select the **Policy Server** tab.
 - For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

3. Click **Advanced**.
The advanced settings for the device display.
4. Click **Modify**.
The advanced configuration settings can be edited.
5. Select a configuration key in the **Service Overrides** table and click **Edit**.
 - Adding a key to the table:

1. Click **Add**.

The **Add Configuration Key Value** window opens.



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.

2. Enter the following values:
 - **Configuration Key** — The attribute to set
 - **Value** — The attribute value (up to 255 characters)
 - **Comments** — Information about the key.

3. Click **OK**.

The key is displayed in the table with its defined and default values.

- Cloning a key in the table:
 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 as required.
4. 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 as required.
4. Click **Save**.

- Deleting a key from the table:
 1. Select an existing key in the table.
 2. Click **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the key.
 - 6. Click **Save**.
- The settings are applied to the selected device.

About Overload Controls

Load Shedding occurs when a Diameter node (an MPE or MRA device) has insufficient resources to successfully process all of the Diameter requests that it receives. You can access **Load Shedding Configuration** controls from the MRA and MPE **Advanced Configuration** pages where you can configure rules for handling messages during overload conditions. Multiple congestion levels can be configured to accept, reject or drop selected messages at each level.

An MRA attempts to successfully process a message whenever possible using either Local or Remote Diversion:

Local Diversion	Selects an MPE device in the MPE pool to handle a new connection for a subscriber who is bound to a busy MPE device.
Remote Diversion	Selects an MRA device to handle a new connection for a subscriber who is bound to a busy MPE device. That MRA device creates a binding for the subscriber pointing to one of the MPE devices in the MPE pool.

Both MPE and MRA devices have configurable levels of congestion (busyness) for handling message overload. An MRA device has two congestion levels (Level 1 and 2) and an MPE device has four congestion levels (Levels 1–4). At each level you can define a default action for the level and create rules to handle specific message types. A level action is an action that is taken if none of the rules configured for the level match a message type. For example, for MRA and MPE Level 1, the default level action is **Accept**, which means to bypass load shedding rules instead of rejecting messages.

Note: When Local or Remote Diversion is not possible, the default result code is `DIAMETER_TOO_BUSY`. The `NO_CAPACITY` result code indicates an MRA device has a binding, but the MPE it points to is currently overloaded, and the MRA cannot perform local diversion to handle the request. The default result code is configurable.

An MRA device proactively rejects all messages destined for an overloaded MPE at all congestion levels. For example, if an MPE is configured to reject CCR-U messages at Level 2, the MRA device rejects the CCR-U message with `DIAMETER_UNABLE_TO_COMPLY` instead of forwarding it to the MPE device.

An MRA device subscribes to its pool of MPE devices for load notifications by issuing an LSR message after connection is established. It also subscribes to MPE devices in the backup MRA pool and to all other MRA devices in its association. MRA devices communicate their status using Load Notification (LNR) messages that include a Diversion-Status AVP to indicate whether that MRA device is available.

The Diversion-Status AVP indicates whether an MRA is available for diverting traffic to its MPEs (Remote Diversion). The diversion status is set to `DIVERTABLE` if none of the MPE devices in an MPE

pool are overloaded. The status is set to NOT_DIVERTABLE if at least one MPE device in the MPE pool is overloaded.

The CMP system supports configuration of MPE load shedding rules on the MRA **Advanced Configuration** page. When you configure the admission rules for an MRA device to reject messages on behalf of an overloaded MPE, there may still be times when the MPE device responds to a message with DIAMETER_TOO_BUSY. In these cases, before forwarding the answer message, the MRA runs the original request through the MPE admission rules and updates the result code with the result code found in the MPE rules.

Configuring MPE and MRA Load Shedding Rules

Use the **Load Shedding Configuration** section of the **Advanced Configuration** page to edit, reorder, or add new rules at each level of busyness for a device based on the amount of backlog. To reach a configured level of busyness:

- The backlog of outstanding messages in a node crosses a predefined threshold for the level.
- The backlog has been above the busyness level threshold for a minimum amount of time.

At each level, the device can be configured to take one of the following actions (referred to as rules) until the busyness level clears:

- Accept the message.
- Drop the message.
- Reject new messages with a specific result code (the default is DIAMETER_TOO_BUSY).

Refer to MPE Default Load Shedding Rules and MRA Default Load Shedding Rules for more information on default rules.

Note: Configuration keys must also be used in configuring load shedding options. Contact My Oracle Support for assistance.

Configure the load shedding rules as follows:

1. View the device list.
 - For an MPE device, go to the **Policy Server** section of the navigation pane and select **Configuration**.
 - For an MRA device, go to the **MRA** section of the navigation pane and select **Configuration**.

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

2. From the content tree, select the device.
 - For an MPE device, select the **Policy Server** tab.
 - For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

3. Click **Advanced**.
The advanced settings for the device display.
4. Click **Modify**.
The advanced configuration settings can be edited.
5. In the **Load Shedding Configuration** section of the page, select the enabled state.
 - **true** (default)—Enables load shedding.
 - **false**—Disables load shedding.

- **undefined**— The value for this field is taken from the associated Configuration Template. If there is not a configuration template associated, then the default value is used.
6. Set the Level Action for a busyness level.
This step is optional. The default Level Action of Accept applies to all levels except MRA Level 2 and MPE Level 4, which has a default Level Action of Drop.
 - a) Click ► (right arrow) next to the level to expand the level.
 - b) Select one of the following default Level Actions:
 - **Accept** all messages.
 - **Drop** all messages.
 - Reject all messages and **Answer with** (select a code from the drop-down list).
 - Reject all messages and **Answer With Code** (enter a code) and **Vendor ID** (enter a vendor ID).
 7. Configure the rules for the busyness levels:
 - a) Click ► (right arrow) next to the level to expand the level.
 - b) Click **Add** and select the category.
The **Add Load Shedding Rule** dialog appears.
 - c) Enter the values for the load shedding rule:
 - **Name** — Name of the rule.
 - **Application** — Select the application the rule applies to. You can select **Drma**, **Gx**, **Gxx**, **S9**, **Rx**, **Sh**, or **Sy**.
 - **Message** — Type of message the rule applies to (which depends on the application chosen).
 - **Request Types** (available only when the CCR message type is selected) — Select the Request-Type attribute-value pairs (AVPs) that the message must contain. You can select **Initial**, **Update**, and/or **Terminate**.
 - **APNs** — Enter a CSV list of one or more access point names that the message must contain.
 - d) Click **OK**.
The rule is displayed in the table.
 8. After a rule is defined, you can clone, edit, or delete it by selecting the rule and clicking the appropriate button.
- The settings are applied to the selected device.

MPE Default Load Shedding Rules

You can configure load shedding rules to determine how a device reacts to a processing backlog. This state is called busyness. Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MPE has four busyness levels. With each successive level, the device becomes more aggressive in rejecting or discarding messages in an attempt to prevent the main queue from becoming full. At any level of busyness, requests that have been queued longer than a configurable time are discarded without further processing, since the originator would have abandoned that request.

On the MPE **Advanced Configuration** page, there is a default action for each Busyness Level. The default level action for levels 1, 2, and 3 is Accept, which means to process the message by bypassing load shedding rules. Level actions are configurable.

The following tables show the default load-shedding rules for an MPE. For configuration information, see the task [Configuring MPE and MRA Load Shedding Rules](#).

Note: The default rules shown in your system may differ than those listed here depending on how your system is configured.

Table 4: MPE Busyness Level 1

The default action for Level 1 is Accept.

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule4	Reject Gxx CCR messages with DIAMETER_TOO_BUSY

Table 5: MPE Busyness Level 2

The default action for Level 2 is Accept.

Rule Name	Actions
DefaultRule2	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule5	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule7	Reject Rx AAR messages with DIAMETER_TOO_BUSY

Table 6: MPE Busyness Level 3

The default action for Level 3 is Accept.

Rule Name	Actions
DefaultRule3	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule6	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule8	Reject Rx AAR messages with DIAMETER_TOO_BUSY
DefaultRule9	Reject Sh PNR messages with DIAMETER_TOO_BUSY
DefaultRule10	Reject Sy SNR messages with DIAMETER_TOO_BUSY

Table 7: MPE Busyness Level 4

The default action for Level 4 is Drop, which applies to all messages other than the DRMA messages that are accepted by default.

Note: The DRMA rule configuration is only displayed in Diameter 3GPP mode as the functionality requires DRMA messaging which is a Diameter-based protocol.

Rule Name	Actions
DefaultRule11	Accept Drma LNR with ACCEPT
DefaultRule12	Accept Drma LSR with ACCEPT
DefaultRule13	Accept Drma RUR with ACCEPT

MRA Default Load Shedding Rules

You can configure load shedding rules to determine how a device reacts to a processing backlog. This state is called busyness. Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MRA has two busyness levels. At each level of busyness, requests that have been queued longer than a configurable time are discarded without further processing, since the originator would have abandoned that request.

On the MRA **Advanced Configuration** page, there is a default action for each Busyness Level. The default level action is Accept for Level 1, which means to process the message by bypassing load shedding rules. Level actions are configurable.

The following tables show the default load-shedding rules for an MRA. For configuration information, see the task [Configuring MPE and MRA Load Shedding Rules](#).

Note: The default rules shown in your system may differ than those listed here depending on how your system is configured.

Table 8: MRA Busyness Level 1

The default action for Level 1 is Accept.

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule2	Reject Gxx CCR messages with DIAMETER_TOO_BUSY

Table 9: MRA Busyness Level 2

The default action for Level 2 is Drop, which applies to all messages other than the DRMA messages that are accepted by default.

Note: The DRMA rule configuration is only displayed in Diameter 3GPP mode as the functionality requires DRMA messaging which is a Diameter-based protocol.

Rule Name	Actions
DefaultRule3	Accept Drma LNR with ACCEPT
DefaultRule4	Accept Drma LSR with ACCEPT
DefaultRule5	Accept Drma RUR with ACCEPT

Resetting Configuration Keys to Defaults

All the configuration keys in the Expert Settings table can be reset to the defaults. The configuration keys in the Service Overrides table cannot be reset.

To reset the configuration keys in the Expert Settings table:


1. View the device list.

- For an MPE device, go to the **Policy Server** section of the navigation pane and select **Configuration**.
- For an MRA device, go to the **MRA** section of the navigation pane and select **Configuration**.

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

2. From the content tree, select the device.
 - For an MPE device, select the **Policy Server** tab.
 - For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

3. Click **Advanced**.
The advanced settings for the device display.
4. Click **Modify**.
The advanced configuration settings can be edited.
5. Click  **Set to Default**.
A confirmation message displays.
6. Click **OK**.

All the configuration keys for Expert Settings are set to default values.

Filtering the Configuration Keys

To limit the number of configuration keys in the Expert Settings or Service Overrides tables, use the filter option.


To filter the configuration key table:

1. View the device list.
 - For an MPE device, go to the **Policy Server** section of the navigation pane and select **Configuration**.
 - For an MRA device, go to the **MRA** section of the navigation pane and select **Configuration**.

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

2. From the content tree, select the device.
 - For an MPE device, select the **Policy Server** tab.
 - For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

3. Click **Advanced**.
The advanced settings for the device display.
4. (Optional) Click **Modify**.
The advanced configuration settings can be edited.
5. Click  **Filters** to open the filtering popup.
The filtering popup opens.
6. Specify the filtering parameters using any of the following fields.

Option	Description
Change Status	The change status of the configuration key. <ul style="list-style-type: none"> • All (default)—All keys are listed. • Changed—Lists the configuration keys that have been modified from the default setting. • Unchanged—Lists the configuration keys that have not been modified from the default setting.
Category	The category for the configuration key.
Configuration Key	Enter all or part of a configuration key name.

7. Click **Filter Result**.
The filtered list of configuration keys displays.

Exporting the Configuration Keys

The Expert Settings or Service Overrides configuration keys can be exported to a comma separated values (CSV) file or to a printable format in a new browser window.

To export the configuration key table:

1. View the device list.
 - For an MPE device, go to the **Policy Server** section of the navigation pane and select **Configuration**.
 - For an MRA device, go to the **MRA** section of the navigation pane and select **Configuration**.

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

2. From the content tree, select the device.
 - For an MPE device, select the **Policy Server** tab.
 - For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

3. Click **Advanced**.
The advanced settings for the device display.

4. Click  **Export**.
The export list opens.

5. Select the export type.

Option	Description
Save as CSV	A comma-separated value (CSV) file named <code>CSV_report.csv</code> is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
Printable Format	The configuration key list displays in a separate window for printing.

Chapter 7

Managing Network Elements

Topics:

- [*About Network Elements.....161*](#)
- [*Configuring Options for Network Elements....164*](#)
- [*Associating a Network Element with an MPE Device.....170*](#)
- [*Working with Network Element Groups.....171*](#)

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:

- Gateway GPRS support node (GGSN)
- 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 **Network Elements**.
The **Network Element Administration** page opens.
3. Click **Create Network Element**.
The **New Network Element** page opens.
4. Enter information for the network element:
 - a) **Name** (required) — The name you assign to the network element.
Enter up to 250 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 or IPv6 format, assigned to the network element.
 - c) **Backup Host Name** — Alternate address that is used if communication between the MPE device and the primary address for the network element fails.
 - d) **Description/Location** — Free-form text.
Enter up to 250 characters.
 - e) **Type** (required) — Select the type of network element.
The supported types are:

- **PDSN** — Packet Data Serving Node (with the sub-types **Generic PDSN** or **Starent**)
 - **HomeAgent** — Customer equipment Home Agent (with the sub-types **Generic HomeAgent** or **Starent**)
 - **GGSN** — Gateway GPRS Support Node
 - **HSGW** — HRPD Serving Gateway
 - **PGW** — Packet Data Network Gateway
 - **SGW** — Serving Gateway
 - **DPI** — Deep Packet Inspection device
 - **NAS** — Network Access Server device
- f) **Capacity** — The bandwidth allocated to this network element.
- g) **Network Element Groups which contain this Network Element** — Specifies the links to other network elements.
5. In **Policy Servers associated with this Network Element**, select one or more policy servers (MPE devices) to associate with this network element.
 6. In **Network Element Groups which contain this Network Element** select the group (see [Adding a Network Element to a Network Element Group](#)).
 7. Click **Save**.

You have created the definition for a network element and the network element is listed on the **Network Element Administration** page.

Modifying a Network Element

To modify 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 network element.
The **Network Element Administration** page opens in the work area.
3. Click **Modify**.
The **Modify Network Element** page opens.
4. Modify the network element information.
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**.
2. From the content tree, select the **ALL** group.

The **Network Element Administration** page opens in the work area, displaying all defined network elements.

3. From the work area, click  (trash can icon) located to the right of the network element.
A confirmation message displays.
4. Click **OK**.

You have deleted the network element definition.

Deleting Multiple Network Elements

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. Click **Bulk Delete**.
The **Bulk Delete Network Elements** page opens.
4. Select the network elements or network element groups to delete.
5. (Optional) Filter the search by entering a search pattern (for example, **cmts***) and click **Filter**.
By default, the **Search Pattern** entry box contains an asterisk (*) to match all network elements.
6. Click **Bulk Delete**.
A confirmation message displays.
7. Click **OK**.

The selected network element or group definitions 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. You can also use the function to locate all of the Cable Modem Termination Systems (CMTS) and MPE devices associated with a specified subscriber IP address or subnets. To use the network element search function:

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. Click **Search**.
The **Network Element Search Criteria** window opens.
4. Enter the search criteria:
 - **Name** — The name assigned to the network element.
 - **Host Name/IP Address** — The domain name or IP address in IPv4 or IPv6 format of the network element.

- **Description** — The information pertaining to the network element that helps identify it within the network. Enter up to 250 characters.

Note: Searches are not case sensitive. You can use the wildcard characters * and ?.

If a subscriber IP address is entered with a mask code (up to 32 for IPv4, or up to 128 for IPv6), then the associated CMTS and MPE device is displayed. If the mask is left blank, then the input IP subnet is treated as an IP address, and the mask code is set automatically to 32 for IPv4 or 128 for IPv6.

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.

Note: Configuration changes made in the CMP system could potentially be reverted on an MPE device if the scheduled run time of the OSSI Distributor task on the Management Agent is before the scheduled run time for the CMP system. The discrepancy is resolved when the OSSI Distributor Task runs on the CMP system. See [Managing Scheduled Tasks](#) for more information.

Configuring the PDSN Network Element

To configure the packet-switched data network (PDSN) 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **PDSN** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the RADIUS-S features:
 - a) **RADIUS Enabled**— Select to enable/disable RADIUS-S support for this network element.
 - b) **RADIUS Shared Secret**— Enter the value that is used by the network element to authenticate RADIUS messages sent from the MPE device. This field must be configured with the same value that is provisioned on the network element or the MPE device will not be able to send messages to the network element.
5. Configure the Diameter features:
 - a) **Diameter Realm**— Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

6. Click **Save**.

The PDSN device is defined.

Configuring the Home Agent Network Element

To configure the Home Agent 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **Home Agent** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the RADIUS-S features:
 - a) **RADIUS Enabled**— Select to enable/disable RADIUS-S support for this network element.
 - b) **RADIUS Shared Secret**— Enter the value that is used by the network element to authenticate RADIUS messages sent from the MPE device. This field must be configured with the same value that is provisioned on the network element or the MPE device will not be able to send messages to the network element.
5. Configure the Diameter features:
 - a) **Diameter Realm**— Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

6. Click **Save**.

The Home Agent network element is defined.

Configuring a GGSN Network Element

To configure a gateway GPRS support node (GGSN) 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **GGSN** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the following information:
 - a) **IP Domain ID** — Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.
Enter a string of 0–100 characters, using only letters, digits, periods (.) or hyphens (-). If left empty, IP domain mapping is disabled for this network element.
 - b) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - c) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.
5. Click **Save**.

The GGSN network element is configured.

Configuring the HSGW Network Element

To configure the HRPD Serving Gateway (HSGW) 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **HSGW** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the following information:
 - a) **IP Domain ID** — This field is reserved for future use.
 - b) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - c) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

5. Click **Save**.

The HSGW network element is configured.

Configuring the PGW Network Element

To configure the packet data network gateway (PGW) 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **PGW** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the following information:
 - a) **IP Domain ID** — Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.
Enter a string of 0–100 characters, using only letters, digits, periods (.) or hyphens (-). If left empty, IP domain mapping is disabled for this network element.
 - b) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - c) **MIPv6 Host Identity**—Specifies the Mobile IPv6 (MIPv6) host.
 - d) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

5. Click **Save**.

The PGW network element is configured.

Configuring the SGW Network Element

To configure the serving gateway (SGW) 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **SGW** tab and then click **Modify**.

The **Modify Network Element** page opens.

4. Configure the following information:
 - a) **IP Domain ID** — This field is reserved for future use.
 - b) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - c) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

5. Click **Save**.

The SGW network element is configured.

Configuring a DPI Network Element

To configure deep packet inspection (DPI) 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**.
2. From the content tree, select a network element with a type of DPI.

Note: If the list does not contain an element with the appropriate type, you must first define the network element of that type. See [Defining a Network Element](#).

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

3. On the **Network Element Administration** page, select the **DPI** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the following information:
 - a) **IP Domain ID** — This field is reserved for future use.
 - b) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - c) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

5. (TDF-Solicit fields) Configure the following traffic detection function fields.

Note: Traffic detection function fields are only available when the network capacity is **TDF-Solicit**. See [Defining a Network Element](#) for more information.

- a) **SCTP Enabled** (available if DPI capability is **TDF-Solicit**) — By selecting the check box, you connect to the traffic detection function (TDF) using the SCTP protocol. TCP is the default connection protocol.
- b) **Allow direct connection from MPE** (available if DPI capability is **TDF-Solicit**) — By selecting the check box, TDF connects directly to Sd with the MPE device (bypassing the MRA device).
- c) **TDF Port** (available if DPI capability is **TDF-Solicit**) — Enter the port number used to communicate with the TDF device. The default port is 3868.
- d) **Watch Dog Interval** (available if DPI capability is **TDF-Solicit**) — Enter the watchdog interval in seconds. The default is 30 seconds.
- e) **Response Timeout** (available if DPI capability is **TDF-Solicit**) — Enter the response timeout interval in seconds. The default is 5 seconds.
- f) **Reconnect Delay** (available if DPI capability is **TDF-Solicit** and **Allow direct connection from MPE** is selected) — Enter the response time in seconds. The default is 3 seconds.
- g) **Associated MRA identity** (available if DPI capability is **TDF-Solicit**) — Select the MRA device from the list.
You cannot associate a DPI device with an MRA device if you have selected **Allow direct connection from MPE**.
- h) **Backup TDF Identity** (available if DPI capability is **TDF-Solicit**) — Select the backup TDF device from the list.

6. Click **Save**.

The DPI device is configured.

Configuring a DSR Network Element

To configure an Oracle Communications Diameter Signaling Router (DSR) 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**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. Select the **DSR** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the following information:
 - a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **galactel.com**).
 - b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, **ne.galactel.com**).

Note: A vendor-specified host name and realm name (such as **ne.galactel.com**) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it from the list and click **Delete**.

5. Click **Save**.

The DSR device is defined.

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

For example:

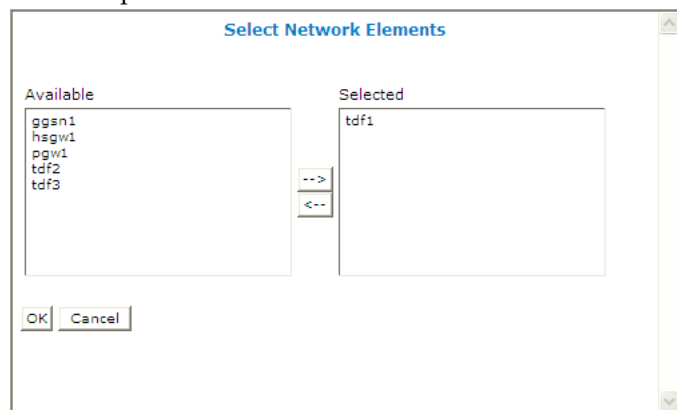


Figure 26: Select Network Elements

6. Select the network elements in the **Available** list and click **-->**.
If there are 50 or fewer defined network elements, they appear in the **Available** list. Select a network element from the **Available** list and click **-->**. The network element is moved to the **Selected** list.
If there are more than 50 defined network elements, the **Available** list is initially blank. To add available items, enter a search string in the **Search Patterns** field. Searches are not case sensitive. You can use the wildcard characters '*' and '?'. Click **Filter**. The network elements are moved to the **Selected** list.
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.
7. Click **OK**.
The selected network elements are added to the list of network elements managed by this MPE device.

8. To associate a network element group with the MPE device, select the group from the list of network element groups located under **Associations**.
9. 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

Network element groups exist in a distributed network to perform specific duties.

Use this procedure if you are creating a network element group to perform specific functions in your distributed network. After you create a network group, you can then create network elements to associate with devices such as an MPE or MRA.

To create a 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 **ALL** group.
The **Network Element Administration** page opens in the work area.
3. 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 and location of the network group.
6. Click **Save**.

You have created a network element group.

Adding a Network Element to a Network Element Group

After a network element group is created, you can add individual network elements to the group.

To add a network element to a 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 **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.
 - If there are more than 25 network elements defined, the page does not display any elements. 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 (for example, **star***, ***pGw**, or ***-***). When you have defined a search string, click **Filter**; the page displays the filtered list.
4. Select the network element you want to add. Use the Ctrl or Shift keys 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.

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 of the sub-group.
6. Click **Save**.

The sub-group is added to the selected group, and now 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 **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 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. Remove the network element using one of the following methods:

- On the **Network Element Administration** page, click the  (trash can) icon, located to the right to the network element.
- From the content tree, select the network element; the **Network Element Administration** page opens. Click the **System** tab and then click **Remove**.

A confirmation message appears.

4. Click **OK**.

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

Modifying a Network Element Group or Sub-Group

To modify a network element group or sub-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 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, description, or both.
5. Click **Save**.

The group or sub-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. You cannot delete the **ALL** group.

To delete a network element group or sub-group:

1. From the **Network** 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.

Chapter 8

Managing the Protocol Timer Profiles Function

Topics:

- *About Protocol Timer Profiles.....175*
- *Viewing a Protocol Timer Profile.....176*
- *Creating a Protocol Timer Profile.....176*
- *Modifying a Protocol Timer Profile.....178*
- *Deleting a Protocol Timer Profile.....178*

This chapter describes how to define and manage protocol timer profiles within the CMP system.

A protocol timer profile configures the Diameter response timeout values for specific applications and the different message types within an application.

About Protocol Timer Profiles

A Protocol Timer profile contains the configuration of Diameter response timeout values for specific applications and message types within an application. A Protocol Timer profile is associated at both the global level for an MPE or MRA device, as well as for a specific diameter peer. For example, a peer with the identity of **ggsn.realm.com** can have a response timeout of 4500ms for an RAR message sent over Gx from the MPE device. You can also configure the maximum amount of time a received Diameter request can be processed by the MPE or MRA device. If an answer is not generated within the configured amount of time, then the request is discarded. This value is global to the entire MPE or MRA population. The values allow for a granularity of a tenth of a second.

Note: A timer configured at the peer level takes precedence over a value configured at the global level.

A profile can be associated with any MPE, MRA device, pooled MPE device, backup MRA device, associated MRA devices, Diameter peer, network element, or data source (Sh and Sy). Any profile associated with an MPE or MRA device is considered the global timer profile for that element. Therefore, each MPE or MRA has only one global timer profile.

In the deployment of an MRA device, it is possible that both the MRA and MPE device could have the same network elements associated with them through the CMP system. In this case, the Protocol Timer profile configured for the network element would only apply to the MRA device since the MRA device is the only one with direct connections to the network elements. The MPE device would be directly communicating with the MRA device and therefore the values configured in the global timer profile for the MPE device would apply. Specific values for a peer level profile pertaining to the MPE device to MRA device communication can be defined by adding the MRA device to the Diameter peer table for the MPE device. See the *Policy Front End User's Guide* for more information about Diameter peer tables.

[Table 10: Supported Diameter Applications and Messages](#) lists the Diameter applications and message types supported.

Table 10: Supported Diameter Applications and Messages

Application / Interface	Message
Gx	CCR, RAR
Rx	AAR, RAR, STR, ASR
S9	CCR, RAR
Rx over S9	AAR, RAR, ASR, STR
Sh	UDR, SNR, PNR, PUR
Sy	SLR, STR, SNR
Gy	CCR, RAR, ASR
Sd	CCR, TSR, RAR
Gxx	CCR, RAR
VZr	SDR

Viewing a Protocol Timer Profile

To view a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
The content tree displays the **Protocol Timer Profiles** folder.
2. Select a profile.
The configuration for the profile displays in the work area.
3. Change the view of the list using the following options:
 - When the list is expanded, click **Collapse All** to show the list of applications/interfaces only.
 - When the list is collapsed, click ► (right arrow) to the left of the interface/application to view the settings for an individual application/interface.
 - When the list is collapsed, click **Expand All** to show list of settings for all the applications/interfaces.
 - When the list is expanded, click ▼ (down arrow) to the left of the interface/application to close the settings view for an individual application/interface.

The Protocol Timer Profile Timeout configuration displays by Application and Interface Message type. Timeout values are in milliseconds (msec).

Creating a Protocol Timer Profile

A Protocol Timer Profile defines timeout values for messages in applications/interfaces.

To create a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
The content tree displays the **Protocol Timer Profiles** folder.
2. Click **Create Protocol Timer Profile**.
The **Protocol Timer Profile Administration** page opens.
3. Enter the following information:
 - a) **Name** — Name of the profile. 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 (,)
 - b) **Description** (optional) — Information that defines the profile.
 - c) Set the **Timeout** values. The following table lists the defaults:

Note: The timeout value must be in a multiple of 100. For example, 4955 is not a valid value and displays a validation error.

Table 11: Supported Diameter Applications and Messages

Application / Interface	Message	Default (msec)
Gx	CCR	5000
	RAR	5000
Rx	AAR	5000
	RAR	5000
	STR	5000
	ASR	5000
S9	CCR	5000
	RAR	5000
Rx over S9	AAR	5000
	RAR	5000
	STR	5000
	ASR	5000
Sh	UDR	3000
	SNR	3000
	PNR	3000
	PUR	3000
Sy	SLR	3000
	STR	3000
	SNR	3000
Gy	CCR	5000
	RAR	5000
	ASR	5000
Sd	CCR	5000
	TSR	5000
	RAR	5000
Gxx	CCR	5000
	RAR	5000
VZr	SDR	5000

4. Click **Save**.

The profile appears in the list of Protocol Timer Profiles and can be associated with any MPE device, MRA device, pooled MPE device, backup MRA device, associated MRA device, Diameter peer, network element, or data source (Sh and Sy).

Modifying a Protocol Timer Profile

A Protocol Timer Profile defines timeout values for messages in applications/interfaces.

To modify a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
The content tree displays the **Protocol Timer Profiles** folder.
2. Select a profile.
The configuration for the profile displays in the work area.
3. Change the view of the list using the following options:
 - When the list is expanded, click **Collapse All** to show the list of applications/interfaces only.
 - When the list is collapsed, click ► (right arrow) to the left of the interface/application to view the settings for an individual application/interface.
 - When the list is collapsed, click **Expand All** to show list of settings for all the applications/interfaces.
 - When the list is expanded, click ▼ (down arrow) to the left of the interface/application to close the settings view for an individual application/interface.
4. Click **Modify**.
The **Protocol Timer Profile Administration** page opens with editable fields.
5. Modify the information.
See [Creating a Protocol Timer Profile](#) for more information on the fields.
Note: The timeout value must be expressed in multiples of 100. For example, 4955 is not a valid value and displays a validation error.
6. Click **Save**.

The profile is updated.

Deleting a Protocol Timer Profile


A Protocol Timer Profile defines timeout values for messages in applications/interfaces.

Note: You cannot delete a Protocol Timer Profile that is associated with a device or group.

To delete a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
The content tree displays the **Protocol Timer Profiles** folder.
2. You can delete a profile using one of the following methods:

Managing the Protocol Timer Profiles Function

- Select the **Protocol Timer Profiles** folder and then click **Delete** (). A confirmation message displays. Click **OK** to delete.
- Select a profile from the **Protocol Timer Profiles** folder and then click **Delete**. A confirmation message displays. Click **OK** to delete.

The profile is deleted.

Chapter 9

Managing Charging Servers

Topics:

- *About Charging Servers.....181*
- *Defining a Charging Server.....181*
- *Modifying a Charging Server.....182*
- *Deleting a Charging Server.....182*
- *Associating a Charging Server with an MPE Device.....183*

This chapter describes how to define and manage charging servers within the CMP system.

A charging server is an application that calculates billing charges.

About Charging Servers

A charging server is an application that calculates billing charges for a wireless subscriber. The CMP system supports both online and offline charging servers:

- An online charging server (OCS) calculates charges against a prepaid account for an event and returns information on how long the subscriber can use the service; it can affect, in real time, the service rendered.
- An offline charging server (OFCS) calculates charges for a service to an account, and does not affect (in real time) the service rendered.

Defining a Charging Server

To define a charging server:

1. From the navigation pane, select **Charging Servers**.
The content tree displays the **Charging Servers** group.
2. Select the **Charging Servers** group.
The **Charging Server Administration** page opens in the work area.
3. Click **Create Charging Server**.
The **New Charging Server** page opens.
4. (Required) Enter the **Name** for the charging server.
The name can be up to 255 characters long and must not contain colons (:), quotation marks ("), or commas (,).
5. Enter the **Description/Location**.
Free-form text that identifies the charging server within the network. Enter up to 250 characters.
6. (Required) Enter the **Host Name**.
The FQDN (fully qualified domain name assigned) to the charging server.
7. Enter the **Port** number on which the charging server is listening for messages.
If left blank, port 3868 is used.
8. Select the **Transport** protocol used to communicate with the charging server:
Available options include:
 - **tcp** — Transmission Control Protocol (used with TACACS+)
 - **udp** — User Datagram Protocol (used with RADIUS)

Note: If you configure the **Transport** protocol as **udp**, you cannot configure the AAA **Protocol** as **diameter**.

 - **sctp** — Stream Control Transmission Protocol
9. Select the Authentication, Authorization, and Accounting (AAA) **Protocol** used to communicate with the charging server.
Available options include:

- **diameter** — Diameter (see [About Diameter Protocol](#) for more information)
- **radius** — RADIUS (see [About RADIUS Protocol](#) for more information)
RADIUS uses UDP Transport protocol.
- **tacacs+** — TACACS Plus (see [About TACACS Plus Protocol](#) for more information)
TACACS+ uses TCP Transport protocol.

10. Select if transport **Security** is used to communicate with the charging server.

11. Click **Save**.

The charging server is displayed on the **Charging Server Administration** page.

After you define charging servers, you can select them as default charging servers when configuring an MPE device (see [Configuring MPE Protocol Options](#)) or use them in policy actions in the policy wizard (see [Policy Wizard Reference](#)).

Modifying a Charging Server


To modify the definition of a charging server:

1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.
The **Charging Server Administration** page opens in the work area, listing the defined charging servers.
2. Select the charging server you want to modify.
The **Charging Server Administration** page displays information about the charging server.
3. Click **Modify**.
The **Modify Charging Server** page opens.
4. Modify charging server information as required.
For a description of the fields contained on this page, see [Defining a Charging Server](#).
5. Click **Save**.

The charging server definition is modified.

Deleting a Charging Server

To delete a charging server:

1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.
The **Charging Server Administration** page opens in the work area and lists the defined charging servers.
2. Delete the charging server using one of the following methods:
 - From the work area, click  (**Delete** icon), located to the right of the charging server name.
 - From the content tree, select the charging server name and click **Delete**.

A confirmation message displays.

3. Click **OK** to delete the charging server.

The charging server definition is removed from the list.

Associating a Charging Server with an MPE Device

To associate a charging server with an MPE device:

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 policy server.
The **Policy Server Administration** page opens in the work area.
3. Select the **Policy Server** tab.
The **Default Charging Servers** section of the page lists charging servers associated with this policy server.
4. Click **Modify**.
The **Modify Policy Server** page opens.
5. In the **Default Charging Servers** section, select the following:
 - Primary Online Server
 - Primary Offline Server
 - Secondary Online Server
 - Secondary Offline Server
6. Click **Save**.

The selected charging servers are defined as serving this MPE device.

Chapter 10

Mapping Serving Gateways to MCCs/MNCs

Topics:

- *About Mapping Serving Gateways to MCCs/MNCs.....185*
- *Creating a Mapping.....185*
- *Modifying a Mapping.....185*
- *Deleting a Mapping.....186*

This chapter describes how to map serving gateways (SGW) to mobile country codes (MCCs) and mobile network codes (MNCs) in the CMP system.

About Mapping Serving Gateways to MCCs/MNCs

It is possible that an SGSN (Serving GPRS Support Node) does not provide a GGSN (Gateway GPRS Support Node) with accurate or complete mobile country code (MCC) or mobile network code (MNC) information. If not, the GGSN cannot pass this information on to the PCRF (including an MPE device), reducing the PCRF's ability to detect specific roaming scenarios. The MCC/MNC mapping table provides a mechanism for the MPE device to convert an SGSN IP address (a value the GGSN can determine without SGSN input) to the proper MCC/MNC value. You can map multiple serving gateways to each MCC/MNC pair. After the MCC/MNC values are determined, they can be used in policies to differentiate subscriber treatment based on the specific roaming scenario.

Creating a Mapping

To create a mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
The content tree displays the **Serving Gateway/MCC-MNC Mappings** group.
2. Select the **Serving Gateway/MCC-MNC Mappings** group.
The **Serving Gateway/MCC-MNC Mappings Administration** page opens in the work area, listing available mappings.
3. Click **Create Serving Gateway/MCC-MNC Mapping**.
The **New Serving Gateway/MCC-MNC Mapping** page opens.
4. Enter the following information:
 - a) **Name** (required) — The name assigned to the mapping.
The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
 - b) **Description** — A descriptive phrase.
 - c) **MCC-MNC** (required) — The MCC-MNC pair, in the format *mccmnc*; for example, 310012 for Verizon Wireless in the United States.
 - d) **Serving Gateway IP Address/Subnet** (required) — The IP address or subnet, in IPv4 or IPv6 format, of a serving gateway.
 - To add an address to the mapping list, enter it and click **Add**.
 - To remove one or more mappings from the list, select them and click **Delete**.
5. Click **Save**.

The mapping is created and stored in the **Serving Gateway/MCC-MNC Mappings** group.


Modifying a Mapping

To modify a Serving Gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
The content tree displays the **Serving Gateway/MCC-MNC Mappings** group.
2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.
The **Serving Gateway/MCC-MNC Mappings Administration** page opens, displaying the list of defined mappings.
3. Select the mapping you want to modify.
Mapping information is displayed.
4. Click **Modify**.
The **Modify Serving Gateway/MCC-MNC Mapping** page opens.
5. Modify mapping information as required.
For a description of the fields contained on this page, see [Creating a Mapping](#).
6. Click **Save**.
The mapping is modified.

Deleting a Mapping

To delete a serving gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
The content tree displays the **Serving Gateway/MCC-MNC Mappings**.
2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.
The **Serving Gateway/MCC-MNC Mappings Administration** page opens, displaying the list of defined mappings.
3. Delete the mapping using one of the following methods:
 - From the work area, click **Delete** () located to the right of the mapping you want to delete.
 - From the content tree, select the mapping and click **Delete**.A confirmation message displays.
4. Click **OK** to delete the Serving Gateway/MCC-MNC mapping.
The mapping is deleted.

Chapter 11

About Subscriber Profile Repositories

Topics:

- [About Subscriber Profile Repositories.....188](#)
- [About Subscriber Profiles.....190](#)
- [About Subscriber Quota Categories.....193](#)
- [About Subscriber Entity States.....196](#)
- [About Pool Profiles.....198](#)
- [About Pool Quota Profiles.....201](#)
- [About Pool States.....203](#)
- [About Subscriber Dynamic Quotas.....205](#)

This chapter describes how to define and manage an optional Subscriber Profile Repository (SPR) using the CMP system.

An SPR is a system for storing and managing subscriber-specific policy control data as defined in the 3GPP standard.

Note: For information on operating Oracle Communications Enhanced Subscriber Profile Repository devices, refer to the *Enhanced Subscriber Profile Repository User's Guide*.

About Subscriber Profile Repositories

A Subscriber Profile Repository (SPR) is a system for storing and managing subscriber-specific policy control data as defined under the 3GPP standard.

An SPR can be deployed in environments where the MPE device needs access to a separate repository for subscriber data. The SPR acts as a centralized repository for this data so that multiple MPE devices can access and share the data. This data can include profile data (pre-provisioned information that describes the capabilities of each subscriber), quota data (information that represents the subscriber's use of managed resources), or other subscriber-specific data.

The following SPR systems can be used in the CMP system:

- The Oracle Communications Subscriber Database Management (SDM) product includes interfaces for provisioning subscriber information, as well as managing, changing, and accessing this information. These interfaces include an application programming interface for XML provisioning of subscriber profile data, as well as an interactive user interface through the Configuration Management Platform system using a proprietary RESTful API interface.

The SDM system is built upon an existing software base and technology. It not only manages static provisioned subscriber data, but also dynamic intra- and inter-session data from MPE devices—for example, when it is critical to store inter-session quota data centrally so that it can be retrieved upon the next subscriber attachment, wherever that attachment occurs within the network. Intra-session data such as mappings from IP addresses to MSISDNs becomes important as well, especially when managing enforcement points such as DPI devices and optimization gateways where MSISDN/IMSI data is not available. With this the Subscriber Database Management system provides both a storage and notification platform for policy operations, as well as a platform for provisioning.

For detailed information on the Subscriber Database Management system, see the Subscriber Data Management documentation.

- The Oracle Communications User Data Repository (UDR) is a highly-scalable, consolidated database back end for subscriber and profile data. User Data Repository utilizes multiple application front ends with the database. UDR supports the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application, a function used for the storage and management of subscriber policy control and pool data. XML-REST and XML-SOAP interfaces are used by Enhanced Subscriber Profile Repository for creating, retrieving, modifying, and deleting subscriber and pool data.

For detailed information on the UDR, see the User Data Repository documentation.

- A customer-specified SPR.

See the Subscriber Profile Repository documentation for more information.

To use an SPR with the CMP system, you must perform the following actions:

- [Configuring the CMP System to Manage SPR Subscriber Data](#)
- [Configuring the SPR Connection](#)

You can also modify an SPR connection. See [Modifying the SPR Connection](#) for details.

Configuring the CMP System to Manage SPR Subscriber Data

The CMP system can manage SPR subscriber data. Before this can occur, the CMP operating mode must support managing SPR clusters.



Caution: CMP operating modes should only be set in consultation with My Oracle Support. Setting modes inappropriately can result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

To reconfigure the CMP operating mode:

1. From the **Help** section of the navigation pane, select **About**.
The **About** page opens, displaying the CMP software release number.
2. Click the **Change Mode** button.
Consult with My Oracle Support for information on this button.
The **Mode Settings** page opens.
3. In the Mode section, select the mode **Diameter 3GPP**, **Diameter 3GPP2**, or **PCC Extensions**, as appropriate.
4. At the bottom of the page, select **Manage SPR Subscriber Data**.
5. Click **OK**.
The browser page closes and you are automatically logged out.
6. Refresh the browser page.
The **Welcome** page opens.

You are now ready to define an SPR cluster profile and manage SPR subscriber profile and pooled quota data.

Configuring the SPR Connection

You must define the operation mode and connection details for the SPR database before you can look up subscriber information from the CMP system.

To configure the SPR connection:

1. From the **SPR** section of the navigation pane, select **Configuration**.
The **SPR Connection Configuration** page opens in the work area, displaying connection information.
2. On the **SPR Connection Configuration** page, click **Modify**.
The **Configuration** page opens.
3. Enter information as appropriate for the SPR system:
 - a) **SPR Operation Mode** (required) — Select from the list:
 - **SDM RESTful API** (default)
 - b) **Remote Port** — Enter the port (a number from 1 to 65535) to listen on for SPR traffic.
The default port is 8787.
 - c) **Secure Connection** — Select to establish a secure connection.
 - d) **SDM Profile Fields**—Defines the custom fields for the SDM profile.
Enter the field name in the field and click **Add**. To remove a field from the list, select the field and click **Delete**.

- e) **SDM Pool Fields**—Defines the custom fields for the SDM pool.

Enter the field name in the field and click **Add**. To remove a field from the list, select the field and click **Delete**.

4. Click **Save**.

The SPR connection is configured.

Modifying the SPR Connection

To modify the SPR connection:

1. From the **SPR** section of the navigation pane, select **Configuration**.
The **SPR Connection Configuration** page opens in the work area, displaying connection information.
2. Click **Modify**.
The **Configuration** page opens.
3. Modify the configuration information.
See [Configuring the SPR Connection](#) for information on the fields on this page.
4. Click **Save**.

The SPR connection configuration is modified.

About Subscriber Profiles

A subscriber profile defines the general information for the subscriber, as well as feature-specific information such as, quotas, pools, etc.

The CMP system allows you to perform the following subscriber profile management actions:

- [Finding a Subscriber Profile](#)
- [Creating a Subscriber Profile](#)
- [Modifying a Subscriber Profile](#)
- [Deleting a Subscriber Profile](#)

Finding a Subscriber Profile

After the SPR devices are defined, you can search them for a subscriber profile.

To find a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select the **Data Source Primary Diameter Identity**.
This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.
3. Select the **Key Type**:
 - **E.164 (MSISDN)** (default) — search by Mobile Station International Subscriber Directory Number. This is a number of up to 15 digits.

- **IMSI** — search by International Mobile Subscriber Identity. This is a number of up to 15 digits.
 - **NAI** — search by Network Access Identifier.
 - **Pool ID** — search by quota pool identifier.
4. **Key String** — enter a search string in the format appropriate for the selected key type. The string must match exactly; partial or wildcard searching is not supported.
 5. Click **Search**.
The **Subscriber Profile** page opens, displaying information about the subscriber.
Note: If no matching subscriber profile is found, the page displays the message `No matching user is found`.
 6. Click **Back to Search Page**.
The **Subscriber Profile Administration** page opens.

Creating a Subscriber Profile

If an SPR database is configured to use the RESTful API interface, you can manually create a subscriber profile.

To create a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Click **Create Subscriber Profile**.
The **New Subscriber Profile** page opens in the work area.
3. Enter the following information:
 - a) Select the **Data Source Primary Diameter Identity**.
You can select any SPR device configured for the Policy Management network.
 - b) In the **Key Fields** section, enter one format:
 - **NAI** — Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters `&*+0-9?a-z_A-Z{|!#$%^&/'= | ~-`, optionally separated by a period (.). A valid realm name consists of the characters `0-9a-zA-Z-` separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
 - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
 - **IMSI** — International Mobile Subscriber Identity. Enter up to 15 Unicode digits.
 - c) Optionally, in the **Subscriber Information** section, enter the following:
 - **Account ID** — Free-form string that identifies the account for the subscriber. You can enter up to 255 characters.
 - **Billing Day** — The day of the month on which the quota for the subscriber is reset. If you enter 0 or leave this field blank, then the default global value configured for this MPE device is used instead.
 - **Tier** — The tier for the subscriber. Enter a tier name defined in the CMP database; or, if you click **Manage**, a window opens from which you can select a tier name. In order to add a tier, you must enter the tier name prior to clicking **Manage**. See [Managing Subscribers](#) for information on managing tiers.

- **Entitlements** — The entitlements for the subscriber. Enter the entitlement names; or, if you click **Manage**, a window opens from which you can enter or select entitlement names defined in the CMP database. See [Managing Subscribers](#) for information on managing entitlements.

Note: Entitlements are defined external to the CMP system.

- **Custom** — Free-form strings representing custom subscriber fields. You can enter up to 255 characters per field. By default, five fields are available, but if the subscriber profile has more than five custom fields defined, the page displays them. Click **Add** to create additional fields as needed.
- **User Billing Type** — The type of billing. Enter a value of 0 (online charging) or 1 (offline charging). The default value is 1.
- **User Notify MSISDN** — The mobile number used to send messages or reminders to users. Enter a character string of 1 - 15 characters in length.
- **User Status** — The quota status for the user. This value determines whether the user is within quota. Enter a value between 1 and 100. A value of 1 means the user is within the quota. A value of 2 means the user is outside the quota. A value of 3 means the user exceeds the value of the top-up. Values of 4 - 50 are used for united expansion in Group Company. Values of 51 - 100 are used for expansion in companies in each province.

If the user status has a value of 2 or 3, the value is reset to the default (0) on the date configured by the **Billing Day** field.

4. Click **Save**.

The subscriber profile is created.

Modifying a Subscriber Profile

To modify a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select the subscriber profile you want to modify.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Click **Modify**.
The **Subscriber Profile Administration** page opens.
4. Modify subscriber profile information as required.
For a description of the fields contained on this page, see [Creating a Subscriber Profile](#).
5. Click **Save**.

The subscriber profile is modified.

Deleting a Subscriber Profile

Using the RESTful API operation mode, you can delete a subscriber profile. See [Configuring the SPR Connection](#) for information on setting the operation mode.

To delete a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to delete.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Click **Delete**.
A confirmation message displays.
4. Click **OK** to delete the subscriber profile.
The subscriber profile is deleted.

About Subscriber Quota Categories

A subscriber quota category defines a category's name, type (that is, quota (plan), pass, rollover, top-up, or default rollover), consumption time, volumes, state, etc.

The CMP system allows you to perform the following subscriber quota category management actions:

- [Viewing Subscriber Quota Information Associated with a Subscriber](#)
- [Adding a Subscriber Quota Category](#)
- [Modifying a Subscriber Quota Category](#)
- [Deleting a Subscriber Quota Category](#)

Viewing Subscriber Quota Information Associated with a Subscriber

To view the subscriber quotas information associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile.
The profile information is shown. (See [Finding a Subscriber Profile](#) for information on locating a subscriber profile.)
3. Select the **Quota** tab.
The **Subscriber Profile Quota Usage** page opens. The table provides the following information:
 - **Name** — Quota name defined in the CMP system.
 - **Time Usage** — Usage counter, in seconds, to track time-based resource consumption.
 - **Time Limit** — Time limit, in seconds, defined in the named quota.
 - **Total Volume Usage** — Usage counter, in bytes, to track volume-based resource consumption.
 - **Total Volume Limit** — Volume limit, in bytes, defined in the named quota.
 - **Upstream Volume Usage** — Usage counter, in bytes, to track upstream bandwidth volume-based resource consumption. Also known as Input Volume.
 - **Upstream Volume Limit** — Upstream volume limit, in bytes, defined in the named quota.
 - **Downstream Volume Usage** — Usage counter, in bytes, to track downstream bandwidth volume-based resource consumption. Also known as Output Volume.
 - **Downstream Volume Limit** — Downstream volume limit, in bytes, defined in the named quota.
 - **Service Specific Event** — Usage counter to track service-specific resource consumption.

- **Service Specific Event Limit** — Resource consumption limit defined in the named quota.
- **Next Reset Time** — The time after which the usage counters need to be reset.
- **CID** — A unique identifier, assigned by the CMP system. Top-ups and rollovers have the CID of their associated plan.
- **Type** — Defines whether the data is for a quota (plan), pass, rollover, top-up, or default rollover.
- **Quota State** — An internal identifier, which defines whether the option selected in the **Type** field is active or expired.
- **RefInstanceId** — The CID of the plan.


4. Click **Back to Search Page**.

You have viewed the subscriber quota information.

Adding a Subscriber Quota Category

To add a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Quota** tab.
The **Quota Usage** information is shown in the work area.
4. Click **Create**.
The **Quota Usage** page opens.
5. If there are more than 10 quotas, a message displays prompting you to add more. Click **Yes**.
6. Enter the following information:
 - a) **CID**: A unique identifier assigned by the CMP system. Rollovers and top-ups have the CID of their associated plan.
Note: This information is assigned by the system, and you should not change it.
 - b) **Name** (required): Select the name of a quota. You cannot add the same quota twice for a subscriber. See the *Policy Wizard Reference* for information on creating quotas.
 - c) **Type**: Select the type of quota defined in the CMP system. You can select **quota** (plan), **pass**, **rollover**, **top-up**, or **default rollover**.
 - d) **Time (seconds)**: Enter a value, in seconds, to track time consumption.
The valid range is: -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - e) **Total Volume (bytes)**: Enter a value, in bytes, to track bandwidth volume consumption.
The valid range is: -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - f) **Upstream Volume (bytes)**: Enter a value, in bytes, to track upstream bandwidth volume consumption.
The valid range is: -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - g) **Downstream Volume (bytes)**: Enter a value, in bytes, to track downstream bandwidth volume consumption.
The valid range is: -2^{63} to $2^{63} - 1$ (a 64-bit value).
 - h) **Service Specific Event**: Enter a value representing service-specific resource consumption.
The valid range is: -2^{63} to $2^{63} - 1$ (a 64-bit value).

- i) **Next Reset Time** (required): Enter a date and time after which the quotas need to be reset, in the format *yyyy-mm-ddThh:mm:ss[Z]* (for example, **2011-11-01T00:00:01-5:00**). Alternatively, click  (calendar) and select a date, enter a time, and optionally select a UTC offset (time zone). Click **OK**.
- j) **Quota State**: This field is an internal identifier and should not be defined by the user.
- k) **RefInstanceID**: The CID of the associated plan. This field only applies to a top-up type quota.
Note: This field is an internal identifier, and you should not change it.

7. Click **Save**.

The subscriber quota is defined.

Modifying a Subscriber Quota Category

To modify a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
The profile information is shown. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Quota** tab.
The **Subscriber Profile Quota Usage** page opens.
4. Click the **Name** of the quota you want to modify.
The **Quota Usage** page opens, displaying information about the quota.
5. Modify the subscriber quota information as required.
For a description of the fields contained on this page, see [Adding a Subscriber Quota Category](#).
6. Click **Save**.

The subscriber quota category is modified.

Deleting a Subscriber Quota Category

To delete a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to modify.
The profile information is shown. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Quota** tab.
The **Subscriber Profile Quota Usage** page opens.
4. In the list of quotas:
 - Use the check boxes to select the quota or quotas you want to delete.
 - To select all quotas, click **All**.
 - To deselect all quotas, click **None**.
5. Click **Delete**.

A confirmation message displays.

6. Click **OK**.

The quota or quotas are removed from the list.

The subscriber quota categories are deleted.

About Subscriber Entity States

Subscriber entity states are sets of name-value pairs associated with a subscriber.

The CMP system allows you to perform the following subscriber entity state actions:

- [Viewing Subscriber Entity States Associated with a Subscriber](#)
- [Creating a Subscriber Entity State Property](#)
- [Modifying a Subscriber Entity State Property](#)
- [Deleting a Subscriber Entity State Property](#)

Viewing Subscriber Entity States Associated with a Subscriber

To view the subscriber entity states associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
That subscriber profile information is shown. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Click the **State** tab.
Entity state information is shown.
4. Click **Back to Search Page**.

You have viewed the subscriber entity states.

Creating a Subscriber Entity State Property

To create a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select the subscriber profile you want to modify.
That profile information is shown. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **State** tab.
The entity state information is shown.
4. Click **Create**.
The **Create Property** page opens.
5. Enter the following information:
 - a) **Name** — The name assigned to the property.

The name cannot be blank and must be unique within this list of properties.

b) **Value** — The property value.

The value cannot be blank.

6. Click **Save**.

The profile information page opens and displays the message `Properties created successfully`.

7. To create additional properties, repeat steps 4 through 6.

If you exceed 100 states, you are prompted whether you want to add more. Click **Yes** to continue, or **No** to stop.

8. Click **Back to Search Page**.

The page displays the message `Properties created successfully`.

The subscriber entity state property is defined.

Modifying a Subscriber Entity State Property

You can modify the value (but not the name) of a subscriber profile entity state property. To modify a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

The **Subscriber Profile Administration** page opens.

2. Select the subscriber profile you want to modify.

The profile information is shown. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)

3. Select the **State** tab.

The entity state information is shown.

4. In the list of entity state properties, click the property you want to modify.

The **Modify Property** page opens.

5. Modify the property value as required.

The value cannot be blank.

6. Click **Save**.

The subscriber entity state property value is modified.

Deleting a Subscriber Entity State Property

To delete a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

The **Subscriber Profile Administration** page opens.

2. Search for the subscriber profile you want to modify.

The profile information is shown. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)

3. Select the **State** tab.

The entity state information is shown.

4. In the list of entity state properties:

- Use the check boxes to select the property or properties you want to delete.

- To select all properties, click **All**.
 - To deselect all properties, click **None**.
5. Click **Delete**.
A confirmation message displays.
 6. Click **OK**.
The property or properties are removed from the list.
- The subscriber entity state properties are deleted.

About Pool Profiles

A pool profile groups subscribers' information (such as, billing day, tier, and entitlements) to provide services to families and businesses.

Subscribers who share a pool profile are members of the same pooled quota group. Pool members have a common pool profile, pool quota usage, pool state, and pool dynamic quota.

The CMP system allows you to perform the following pool profile management actions:

- [Querying by Pool ID](#)
- [Adding a Member to a Basic Pooled Quota Group](#)
- [Modifying a Pool Profile](#)
- [Deleting a Pool Profile](#)

About Pool Types

There are two types of pooled quota group: basic pools and enterprise pools. Basic pools contain up to 25 members and are suitable for families and small businesses. Enterprise pools contain up to 1500 members and are suitable for corporate settings.

A basic pool sends notification and re-authorization requests for each member whenever any pool object is changed. You can view and modify the membership information of a basic pool in the CMP system at any time.

An enterprise pool validates notification and re-authorization requests at the configured session re-validation interval. Membership information is provisioned from the SPR and cannot be viewed or modified in the CMP system. See your SPR documentation for information about provisioning pooling information.

A basic pool can be converted to an enterprise pool at any time by modifying the pool type. An enterprise pool can be converted to a basic pool in the same way provided that the pool contains 25 or fewer members. See [Creating a Pooled Quota Group](#) for information about setting the pool type.

Querying by Pool ID

You can query a new quota by specifying the Pool ID Key Type and Key String value.

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.

2. Select **Pool ID** in the **Key Type** list, enter a **Key String** and click **Search**.
The **Pool Group Quota Profile** page opens with the search results. The following tabs appear:
 - **Pool Profile**
 - **Pool Quota**
 - **Pool State**
3. You can select the **Modify**, **Delete**, or **Back to Search Page** options.

Creating a Pooled Quota Group

You can use a pooled quota group to create a shared pool profile for groups of subscribers.

To create a pooled quota group:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select **Create Pooled Quota Group**.
The **New Pooled Quota Group Profile** page opens.
3. In the **Data Source Primary Diameter Identity** section of the page, select one of the configured ProfileV3 or ProfileV4 data sources.
4. In the **Pool Quota Group Key Fields** section of the page, enter the **Pool ID**.
The pool ID must be a numeric value that is greater than 0 and can have a maximum of 22 decimals.
5. (Optional) In the **Pool Information** section of the page, enter the following:
 - a) **Type** — Select one of the following:
 - **basic** (default) — A pool containing up to 25 subscribers. The basic pool type is suitable for small groups of subscribers, for example a family or a small business.
 - **enterprise** — A pool containing up to 1500 subscribers. The enterprise pool type is suitable for large groups of subscribers, for example employees of a large company.
 - b) **Billing Day** — The billing day of the subscriber pool. This field is used only for monthly billing.
 - c) **Tier** — Enter the name of a tier defined in the CMP database or click **Manage** to select a tier.
 - d) **Entitlements** — Click **Manage** and select one or more entitlement names defined in the CMP database.
 - e) **Custom 1, Custom 2, Custom 3, Custom 4, Custom 5** — Enter name value fields. You can refer to them in policies.
 - f) **Custom N** — If you click **Add**, you can add additional custom fields.
6. Click **Save**.

The pooled quota group is created.

Adding a Member to a Basic Pooled Quota Group

You can use pooled quota groups to create a shared pool profile for multiple subscribers. A basic pool can include up to 25 subscribers as pooled quota group members. You can add members or modify the membership list from the CMP when the pool is a basic pool.

Note: The **Modify Membership** button is hidden when the pool is an enterprise pool. Pooling information for enterprise pools, including pool membership, is provisioned from the SPR.

To add a member to a pooled quota group:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Use the **Search** function to find the desired pool quota group.
 - a) Select the **Data Source Primary Diameter Identity**.
This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.
 - b) Select **Pool ID** as the **Key Type**.
 - c) In the **Key String** field, enter the Pool ID of the desired pool quota group.
The Pool ID must match exactly; partial or wildcard searching is not supported.
 - d) Click **Search**.
The **Pool Profile** page opens.
3. On the **Pool Profile** tab, click **Modify Membership Information**.
The **Pool Profile Configuration** page opens.
4. In the **Membership Information** section of the page, enter the following:
 - a) **Key Type** — The type of subscriber identifier. You can select one of the following:
 - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number.
 - **IMSI** — International Mobile Subscriber Identity.
 - **NAI** — Network Access Identifier.
 - b) **Key String** — Enter the key string for the subscriber.
Note: When associating a subscriber, you must enter the subscriber **Key String**.
 - c) Click **Add** to add the subscriber to the pooled quota group.
A confirmation message is displayed.
Note: Click **Cancel** to return to the **Pool Profile** page.
5. Click **Save**.

The member is added to the pooled quota group.

Modifying a Pool Profile

You can modify a pool profile to make changes to the subscriber information or membership information.

To modify a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of the **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens with Pool Profile as the default.
4. Click **Modify**.
The **Subscriber Profile Configuration** page opens.

5. Modify any of the field information.
6. Click **Save**.

The pool profile is modified.

Deleting a Pool Profile

To delete a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens with **Pool Profile** as the default.
4. Click **Delete**.
A confirmation message displays.
5. Click **OK**.

The pool profile is deleted.

About Pool Quota Profiles

A pool quota profile sets usage quota parameters. This allows the CMP system to track and display usage threshold events. Policies may refer to a pool quota profile. Refer to the *Policy Wizard Reference* for additional information.

The CMP system allows you to perform the following pool quota profile management actions:

- [Creating a Pool Quota Profile](#)
- [Modifying a Pool Quota Profile](#)
- [Deleting a Pool Quota Profile](#)

Creating a Pool Quota Profile

The CMP system uses a pool quota profile for tracking and displaying usage threshold events.

To create a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
The **Quota Usage** section displays.
5. Click **Create**.
6. Enter the following:

- a) **Name** — Select the name of the pool state.
- b) **Type** — Select the quota being assigned to the pool:
 - **quota (plan)**
 - **pass**
 - **top-up**
 - **roll-over**
 - **roll-over-def**

Note: If you select **roll-over-def**, rollover units are consumed before top-up units unless the highest priority top-up expires in the next 24 hours.

- c) **Time (seconds)** — The amount of time attributed to the quota in seconds.
- d) **Total Volume (bytes)** — The amount of volume attributed to a length of time.
- e) **Upstream Volume (bytes)** — Traffic from the handset (or other device) to the network.
- f) **Downstream Volume (bytes)** — Traffic directed to the handset or other device.
- g) **Service Specific Event** — Tracks text information.
- h) **Next Reset Time** — The reset date and time of the subscriber or pool quota usage.

Note: This is typically the billing day, although for a daily quota the usage is normally reset at midnight or shortly thereafter.

7. Click **Save**.

The pool quota profile is created.

Modifying a Pool Quota Profile

To make changes to the subscriber information or membership information, modify the pool quota profile.

To modify a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens with **Pool Profile** as the default.
4. Click **Pool Quota Profile**.
The **Pool Quota Profile** view displays.
5. Select the profile that you want to modify.
6. Modify any of the fields.

Note: The **Name** field cannot be changed.

7. Click **Save**.

The pool quota profile is modified.

Deleting a Pool Quota Profile

To delete a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
The Quota Usage section displays.
5. Select the name of the profile you want to delete and click **Delete**.
A confirmation message displays.
6. Click **OK**.
The selected properties are deleted.

About Pool States

When using an Sh ProfileV3 or ProfileV4 data source, you can use Pool States. A pool state consists of a name-value pair that is associated with the quota pool. For more information, see [Configuring MPE Protocol Options](#).

The CMP system allows you to perform the following pool state actions:

- [Creating a Pool State](#)
- [Modifying a Pool State](#)
- [Deleting a Pool State](#)

Creating a Pool State

When using an Sh ProfileV3 or ProfileV4 data source, you can create a pool state.

To create a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Subscriber Profile** page opens.
4. Select the **Pool State** tab.
The **Pool Profile** page opens.
5. Click **Create**.
The Create Property section displays.
6. Enter the following:

- **Name** — The name of the pool state.
- **Value** — The value can be any string, for example, **ProfileV3** or **ProfileV4**.

7. Click **Save**.

The pool state is created. The Pool Entity State Properties section displays the **Pool Quota Group Key Fields** and the **Pool ID**.

Modifying a Pool State

If you want to make changes to the subscriber information or membership information, you can modify the pool state.

To modify a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Subscriber Profile** page opens.
4. Select the **Pool State** tab.
The **Pool Entity State Properties** section displays.
5. Click the **Name** of the pool state that you want to modify.
The **Modify Property** section displays.
6. The **Name** and **Value** fields are displayed but you can only modify the **Value** field.
7. Modify the **Value** field.
8. Click **Save**.

The system saves the modified pool state.

Deleting a Pool State

To delete a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.
The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
The **Subscriber Profile** page opens.
4. Select the **Pool State** tab.
The **Pool Entity State Properties** section is displayed.
5. Select a check box for one or more properties to delete and click **Delete**.

The specified properties are deleted.

About Subscriber Dynamic Quotas

A subscriber dynamic quota allows subscriber access based on time-limited subscriber quotas.

The CMP system allows you to perform the following dynamic quota management actions:

- [Viewing Subscriber Dynamic Quota Information](#)
- [Adding a Subscriber Dynamic Quota Category](#)
- [Modifying a Subscriber Dynamic Quota Category](#)
- [Resetting a Subscriber Dynamic Quota](#)
- [Deleting a Subscriber Dynamic Quota Category](#)

Viewing Subscriber Dynamic Quota Information

To view the dynamic quota information associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Search for the subscriber profile you want to view.
The **Subscriber Profile** page opens. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Dynamic Quota** tab.
The **Dynamic Quota Usage** page opens. The page provides the following information:
 - **Name** — Name of the dynamic quota.
 - **Time Limit** — Time limit, in seconds, defined for the dynamic quota.
 - **Total Volume Limit** — Volume limit, in bytes, defined for the dynamic quota.
 - **Upstream Volume Limit** — Upstream volume limit, in bytes, defined for the dynamic quota.
 - **Downstream Volume Limit** — Downstream volume limit, in bytes, defined for the dynamic quota.
 - **Service Specific Event Limit** — Resource consumption limit defined for the dynamic quota.
 - **Purchase Time** — The time the dynamic quota was purchased.
 - **Active Time** — The time that the dynamic quota is in effect.
 - **Expire Time** — The time that the dynamic quota expires.
 - **Type** — Defines whether the dynamic quota is a pass or top-up.
 - **Priority** — Defines the order in which the dynamic quota is processed.
 - **InstanceId** — A unique identifier for the dynamic quota.
4. Click **Back to Search Page**.

You have viewed the subscriber dynamic quota information.

Adding a Subscriber Dynamic Quota Category

To add a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.

2. Find the subscriber profile you want to view.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the Dynamic Quota tab.
The **Dynamic Quota** page is displayed.
4. Click **Create**.
The **Create Subscriber Dynamic Quota** page opens. If you exceed 10 dynamic quotas, you are prompted with a message to add more; click **Yes** to continue, or **No** to stop.
5. Enter the following information:
 - **InstanceID** — A unique identifier.
Note: Do not enter a colon (:) as part of this identifier.
 - **Name** — Select the name of a dynamic quota.
 - **Description/Location** — Free-form text.
 - **Type** — Select the type of quota defined in the CMP system. You can select **pass** or **top-up**.
 - **Priority** — Defines the order in which the dynamic quota is processed.
The range is -32768 to 32767 (Max 16-bit short). Higher priority passes are used before lower priority passes. A higher number indicates a higher priority.
 - **Initial Time Limit (seconds)** — The initial value for time units granted by the dynamic quota.
 - **Initial Total Volume Limit (bytes)** — The initial value for total volume units granted by the dynamic quota.
The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).
 - **Initial Upstream Volume Limit (bytes)** — Enter a value, in bytes, to track upstream bandwidth volume consumption.
The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).
 - **Initial Downstream Volume Limit (bytes)** — Enter a value, in bytes, to track downstream bandwidth volume consumption.
The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).
 - **Initial Service Specific Limit (events)** — Enter a value representing service-specific resource consumption.
The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).
 - **Purchase Time** — The date and time that the dynamic quota was purchased.
For the **Purchase Time**, **Active Time**, and **Expire Time** fields, use the format `yyyy-mm-ddThh:mm:ss[Z]` (for example, `2011-11-01T00:00:01-5:00`). Alternatively, click on the calendar icon, and from the window that opens, select a date, enter a time, and optionally select a UTC offset (time zone). Click **OK**.
 - **Active Time** — The time period during when the dynamic quota can be used.
 - **Expire Time** — The date and time the dynamic quota expires. If undefined, the dynamic quota does not expire.
 - **Duration (seconds)** — The amount of time after the first use that the dynamic quota expires.
 - **Interim Reporting Interval (seconds)**
If the units are granted from a top-up, then the **Interim Reporting Interval** is:

- The number of seconds until the next quota reset
- The interim reporting interval defined for the plan
- The time until the top-up expires
- The time until a higher priority top-up becomes active

If the units are granted from a pass, then the **Interim Reporting Interval** is:

- The interim reporting interval defined for the pass
- The time until the pass expires
- The earliest time that the current time will be outside the valid time period (if defined)
- The time until a higher priority pass becomes active

6. Click **Save**.

The subscriber quota is defined and the page displays the message `Quota created successfully`.

Modifying a Subscriber Dynamic Quota Category

To modify a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to view.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Dynamic Quota** tab.
The **Dynamic Quota** page is displayed.
4. Select the name of the quota you want to modify.
The **Modify Subscriber Dynamic Quota** page opens, displaying information about the dynamic quota.
5. Modify subscriber quota information.
For a description of the fields contained on this page, see [Adding a Subscriber Dynamic Quota Category](#).
6. Click **Save**.

The subscriber dynamic quota category is modified.

Resetting a Subscriber Dynamic Quota

If you reset a dynamic quota, then the time, total volume, upstream volume, downstream volume and service specific events limit values that were provisioned in the **SPR>Profile Data** option are replaced with the initial values that were configured in the **Quota Profiles** or **Quota Conventions** option.

To reset a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to view.
Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)
3. Select the **Dynamic Quota** tab.

The **Dynamic Quota** page is displayed.

4. Select the quotas you want to reset.

To select all dynamic quotas, click **All**. To deselect all dynamic quotas, click **None**.

5. Click **Reset**.

A confirmation message displays.

6. Click **Ok** to reset the values.

7. Click **Save**.

The subscriber dynamic quota values are reset.

Deleting a Subscriber Dynamic Quota Category

To delete a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

The Subscriber Profile Administration page opens.

2. Find the subscriber profile you want to modify.

Profile information is displayed. (See [Finding a Subscriber Profile](#) for information on finding a subscriber profile.)

3. Select the Dynamic Quota tab.

The Dynamic Quota page is displayed.

4. In the list of quotas, use the check boxes to select the dynamic quotas you want to delete.

To select all dynamic quotas, click **All**. To deselect all dynamic quotas, click **None**.

5. Click **Delete**.

A confirmation message displays.

6. Click **OK**.

The subscriber dynamic quota categories are deleted.

Chapter 12

Managing Subscribers

Topics:

- [Creating a Subscriber Tier.....210](#)
- [Deleting a Tier.....210](#)
- [Creating an Entitlement.....211](#)
- [Deleting an Entitlement.....211](#)
- [Displaying Static Session and Binding Data for a Subscriber.....212](#)

This chapter describes how to create and manage subscriber tiers and quota usage within the Configuration Management Platform system.

Note: The actual options you see depend on whether or not your Configuration Management Platform system is configured to operate with a Subscriber Profile Repository. For information about the Oracle Communications Subscriber Database Management product, see the Subscriber Database Management documentation. For information about the Oracle Communications User Data Repository product, see the User Data Repository documentation.

Creating a Subscriber 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. After 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. Click **Save**.

You can now use the tier in policy rules.

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 Entitlement

Entitlements are defined within a Subscriber Profile Repository. You can define entitlement names in the CMP database. After you define entitlements, you can use them in policy rules.


To create an entitlement:

1. From the **Subscriber** section of the navigation pane, select **Entitlements**.
The content tree displays the **Entitlements** folder.
2. Select the **Entitlements** folder.
The **Entitlement Administration** page opens.
3. Click **Create Entitlement**.
The **New Entitlement** page opens.
4. Enter information as follows:
 - a) **Entitlement ID** (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.
5. Click **Save**.

The entitlement is created in the CMP database, and you can now refer to it in a policy rule.

Deleting an Entitlement

To delete an entitlement:

1. From the **Subscriber** section of the navigation pane, select **Entitlements**.
The **Entitlements** folder appears in the content tree, and a list of defined entitlements appears in the work area.
2. Delete the entitlement using one of the following methods:
 - From the work area, click  (trash can icon), located to the right of the entitlement you wish to delete.
 - From the content tree, select the entitlement and click **Delete**.

A confirmation message displays.
3. Click **OK**.

The entitlement is deleted.

Displaying Static Session and Binding Data for a Subscriber

You can display static session and binding data for a specific subscriber from the Policy Management device that is managing the session. Depending on how the data is indexed on the device, you can search for a subscriber by IMSI, MSISDN, IP address, or NAI. You can also delete obsolete sessions.

Note: This function is not supported by Policy Management devices before release 7.5.

To display the static session and binding data for a subscriber:

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. Select the Policy Management device managing the session you want to view.
The **Policy Server Administration** page opens in the work area.
3. Select the **Session Viewer** tab.
The **Session Viewer** page opens.
4. Enter search information as follows:
 - a) **Identifier type** (required) — Select one of the following identifier types:
 - **NAI** (default)
 - **E.164(MSISDN)**
 - **IMSI**
 - **Diameter Session ID**
 - **Diameter IPv4Address**
 - **Diameter IPv6Prefix**

The identifier types you can specify are determined by the configuration of the Policy Management device. For example, if the **Index By NAI** setting is not specified on the device, then you cannot select **NAI**.

Note: When searching primary Gx sessions by IPv6 prefix, only 64-bit masks are supported.

- b) **Identifier name** — Free-form text.
Enter up to 250 characters.
 - c) Select **Show advanced details** to view the detailed (that is, verbose) results.
5. Click **Search**.
If sessions are available for the subscriber, **Subscriber Session Data** page appears. [Figure 27: Session Viewer Page](#) shows an example. If the subscriber has correlated secondary sessions, the correlated secondary session data is also displayed.

If you are viewing subscriber data from a stateful MRA system, subscriber binding data is displayed, including an identifier for the MPE device handling sessions for that subscriber. If that MPE device is managed by this CMP system, you can click the identifier to view session data from the MPE device.

Note: If an external system generates data that, when translated to ASCII, creates illegal characters, they are displayed by the Session Viewer as question marks (?).

For each session displayed from an MPE device, you can click **Delete Session** to delete the session. For each subscriber displayed from an MPE device, you can click **Delete Subscriber's All Session** to delete all sessions for that subscriber. For each session binding displayed from an MRA device, you can click **Delete Binding** to delete the binding. This deletes the record in the appropriate database.



Caution: Only obsolete sessions should be deleted. If you delete an active session, there is no signal to any associated gateways or external network elements.

Policy Server Administration

Policy Server: mpe230-127

System
Reports
Logs
Policy Server
Diameter Routing
Policies
Data Sources
Session Viewer

Session Viewer:

Identifier type: IMSI Identifier name: 56575657885 Search

Subscriber Session Data:

2 session(s) has been found.

Delete Subscriber's All Session

User: IMSI:56575657885 key: 270002
Account ID:null

User IDs:
IMSI:56575657885

Pool ID:null
Usagekey:IMSI:56575657885

[Read more...](#)

Delete Session

SessionId: pgw.tekelec.com;1408989258;1

AppId: 16777238
AppName: Gx [REL9, REL8]
PeerId: pgw.tekelec.com
DestinationHost: pgw.tekelec.com
DestinationRealm: tekelec.com

[Read more...](#)

Delete Session

Figure 27: Session Viewer Page

Chapter 13

Managing Policy Front End Devices

Topics:

- *Configuring the CMP System to Manage an MRA Cluster.....215*
- *Defining an MRA Cluster Profile.....215*
- *Modifying an MRA Cluster Profile.....216*
- *Associating Network Elements with an MRA Device.....216*
- *Configuring MRA Protocol Options.....217*
- *Configuring Diameter Peers.....219*
- *Configuring Diameter Host Based Peer Routes.....221*
- *Configuring Diameter Realm Based Peer Routes.....223*
- *Working with MRA Groups.....225*
- *About Stateless Routing.....228*

This chapter describes how to define and manage Oracle Communications Policy Management Policy Front End (also known as MRA) devices in the CMP system.

Note: For more information on using MRA servers, refer to the *Policy Front End Wireless User's Guide*.

Configuring the CMP System to Manage an MRA Cluster

The Policy Front End (also known as the MRA) device is a standalone entity that supports MPE devices in either a wireless or wireline mode. The CMP system is used to manage all MRA functions. Before this can occur, the CMP operating mode, (Wireless or Wireline), must support managing MRA clusters.

Follow these steps to configure the CMP to the appropriate operating mode so that it can manage MRA devices:



Caution: CMP operating modes should only be set in consultation with My Oracle Support. Setting modes inappropriately can result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

1. From the **Help** navigation pane, select **About**.
The **About** page opens, displaying the CMP software release number.
2. Click the **Mode** button.
Consult with My Oracle Support for information on this button.
The **Mode Settings** page opens.
3. On the bottom of the page, select **Manage MRAs**.
4. Click **OK** which closes the browser page and logs you out.
5. Refresh the browser page.
The **Welcome admin** page is displayed.

You are now ready to define an MRA cluster profile, specify network settings for the MRA cluster, and associate MPE devices with the MRA cluster.

Defining an MRA Cluster Profile

In order to get accurate session analysis, log, error, and reporting information, you must define certain parameters of an MRA device to give a specific profile for each MRA cluster you are managing.

To define an MRA cluster profile:

1. From the **MRA** section of the navigation pane select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **MRA Administration** page opens in the work area.
3. Click **Create Multi-protocol Routing Agent**.
The **New MRA** page opens.
4. Enter information as appropriate for the MRA cluster:
 - a) **Associated Cluster** (required): Select the MRA cluster from the list.
 - b) **Name** (required): Enter a name for the MRA cluster.
The name can be up to 250 characters long. The name can contain any alphanumeric characters except quotation marks (") and commas (.).
 - c) **Description/Location** (optional): Free-form text box.

Enter up to 250 characters.

- d) **Secure Connection:** Select to enable a secure HTTP connection (HTTPS) instead of a normal connection (HTTP).

Note: The default is a non-secure (HTTP) connection.

- e) **Stateless Routing:** Select to enable stateless routing. In stateless routing, the MRA cluster only routes traffic; it does not process traffic.

The default is stateful routing.

5. Click **Save**.

The MRA cluster profile is defined. If you are setting up multiple MRA clusters, you must define multiple cluster profiles. Repeat the above steps to define additional profiles.

Modifying an MRA Cluster Profile

As your network changes, is reconfigured, or adds new capabilities, such Diameter and its associated interfaces, you will have to modify your existing MRA to meet these needs.

To modify MRA cluster profile settings:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the **MRA** cluster profile located in the content tree.
3. Select the **System** tab located in the **MRA Administration** page.
4. Click **Modify** which opens the **Modify System Settings** page.
5. Modify those system settings that need modification.
6. When you finish, click **Save**.

Associating Network Elements with an MRA Device

Adding network elements to an MRA device is similar to how network elements are added to an MPE device: a list of supported network elements, which are pre-entered into the system is available for selection.

Use this procedure when you need to add new or upgraded MRA to your Diameter-enabled system and then associate a network element (for example PCEF) to that MRA.

To add a network element to an MRA, complete the following:

1. From within the **MRA** tab, click **Modify**.
The **MRA Administration Modify** page opens.
2. In the Associations section of the **MRA Administration Modify** page, click **Manage**.
The Select Network Elements window displays showing a list of network elements.

For example:

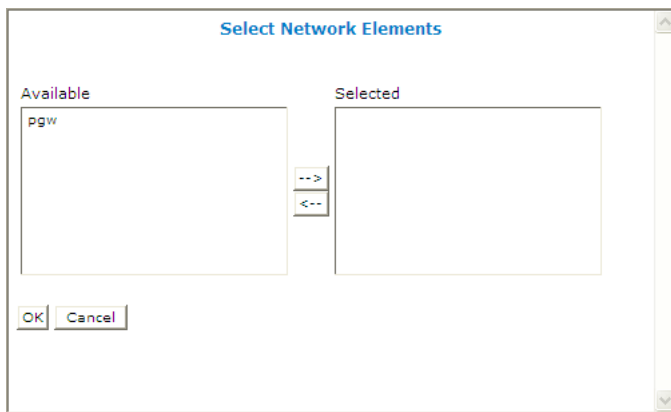


Figure 28: Select Network Elements

3. Select a network element in the **Available** list, click the right arrow to move the network element to the **Selected** list.
4. (Optional) Add additional network elements to the **Selected** list.
5. Click **OK**.

The network element is added to the MRA.

Configuring MRA Protocol Options

MRA must be configured to work with protocols and capabilities, such as Subscriber Indexing, APN override, Diameter, S9, RADIUS, and others capabilities to function in your network.

To configure protocol options on an MRA device:

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. From the content tree, select the MRA device that requires protocol configuration.
The **MRA Administration** page opens.
3. Select the **MRA** tab that displays the configuration options.
4. Click **Modify** and define options as necessary.

Table 12: MRA Protocol Configuration Options defines available options that pertain specifically to MRA devices. (The options may vary depending on the configuration mode of the system.)

5. When you finish, click **Save**.

Table 12: MRA Protocol Configuration Options

Attribute	Description
Subscriber Indexing	Note: The indexing parameters to use depend on what user IDs are needed for correlating various messages to ensure they all end up on the same MPE device for the same user. If you are unsure which indexing methods to configure, contact My Oracle Support (https://support.oracle.com).

Attribute	Description
Index by IPv4	Select if the MRA devices in the association should index by IPv4 address.
Index by IP-Domain-Id	Select if the MRA devices in the association should index by IP domain ID. The combination of framed IPv4 address and IP domain ID ensures a globally unique binding, even if the same IPv4 address is locally assigned in multiple networks.
Index by IPv6	Select if the MRA devices in the association should index by IPv6 address.
Index by Username	Select if the MRA devices in the association should index by account ID.
Index by NAI	Select if the MRA devices in the association should index by network access ID.
Index by E.164 (MSISDN)	Select if the MRA devices in the association should index by E.164 phone number.
Index by IMSI	Select if the MRA devices in the association should index by IMSI number.
Index by Session ID	Select if the MRA devices in the association should index by session ID.
Overrides by APN	<p>Select to perform subscriber indexing for a specific IP address and a specific APN name.</p> <ol style="list-style-type: none"> 1. In the Overrides by APN section, click Add. 2. Enter the APN name and click Save to enable Index by IPv4, Index by IP-Domain-Id, Index by IPv6, Index by Username, Index by NAI, Index by E.164 (MSISDN), Index by IMSI, or Index by Session ID. <p>You can create APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.</p>
Protocol Timer Profile	The timer profile to use.
S9	
Primary DEA	If one or more Diameter Edge Agents is defined, you can select the primary agent from the list. For information on defining a DEA, see Configuring Diameter Peers .
Secondary DEA	If multiple Diameter Edge Agents are defined, you can select the secondary agent from the list. If you select both primary and secondary DEAs, the MRA device establishes a connection to both DEAs. If the primary connection is down, the MRA device sends messages over the secondary connection; after the primary connection is back up, communication reverts back to it.

Configuring Diameter Peers

The MPE and MRA devices support Diameter Rx, Gq, Ty, Gxx, Gx, Gy, S9, and Sd applications. For example, traffic control is supported using the Diameter Gx application. When a subscriber attaches to the network (for example, using a phone) via a GGSN (Gateway GPRS Support Node), the GGSN can establish a session with both the MPE and MRA devices using a Diameter Gx CCR (Credit Control Request) message. The MPE and MRA devices respond to the request with a Gx CCA (Credit Control Answer) message.

Use this procedure if you need to configure system devices (peers) to a diameter-based network.

To configure Diameter peers for either an MPE or MRA device:

1. Either in the **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server or MRA groups.
2. From the content tree, select the MPE or MRA device.
The **Administration** page for that device opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings appear.
4. Click **Modify Peers** which opens the **Modify the Diameter Peer Table**.
5. Add a peer to the table using these steps.

- a) Click **Add**.

The **Add Diameter Peer** window opens.

Figure 29: Add Diameter Peer




- b) Enter the following:

- **Configured MRAs/MPes (optional)** — If you are defining an existing Policy Management cluster as a Diameter peer, select it from this list; the other fields are populated.

- **Name** (required) — Name of the peer device (which must be unique within the CMP database).
- **IP Address** (required) — IP address in IPv4 or IPv6 format of the peer device.
If not specified, the MPE device uses a DNS lookup to resolve the value in the Diameter Identity field into an IP address and try to connect.
- **Diameter Realm** (required) — The peer's domain of responsibility (for example, **Example.com**).
- **Diameter Identity** (required) — Fully qualified domain name (FQDN) of the peer device (for example, **mpe33.Example.com**).
- **Protocol Timer Profile** — Select from the list.
- **Initiate Connection** — Select to initiate an S9 connection for this Diameter peer.
- **Transport** — Select either **TCP** or **SCTP** (shown as Transport Info in the Diameter peer table). For TCP select **Connections** (range 1-8, default 1). For SCTP select **Max Incoming Streams** and **Max Outgoing Streams**(1-8 connections, default is 8) which will be shown as Connection Info in the Diameter peer table.
- **IP Port** — Enter the IP Port number.
- **Watchdog Interval** — Enter the watchdog interval in seconds. The default is 30 seconds.
- **Reconnect Delay** — Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout** — Enter the response timeout interval in seconds. The default is 5 seconds.

c) Click **Save**.

6. Complete these steps to add, edit or delete additional Diameter Peers.

- Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is added to the table
- Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
- Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.

7. Click **Save**.

Configuring Diameter Host Based Peer Routes

Host based diameter routes are used in cases where messages are intended for a specific Destination-Host, (or a list of Destination-Hosts), and need to be routed to an intermediary peer because the Destination-Host cannot be reached directly.

Note: The routing table can be used with a stateful MRA by creating a route with an action of LOCAL. In order to use routes in tandem with a stateful MRA, a route with an action of LOCAL must be created.

Use this procedure if you have a very wide network where direction Destination-Host connections must be routed through an intermediary peer.

To configure the Diameter host based route table:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of policy server/MRA groups.
2. From the content tree, select the **MRA** device.
The **MRA Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings are displayed for that server or device.
4. Click **Modify Routes**.
The **Modify the Diameter Route Table** page opens.
5. Add a route to the table:
 - a) Click the **Add** button and select **Host Based Route**.
the **Add Host Based Route** window opens.
 - b) Configure the route using the following fields.
 - **Name** — The name for the Destination Host.
 - **Type** — This column lists whether the route is "realm-based" or "host-based."
 - **Host Identities** — This option enables you to manually type in any number of host identities.
Note: The wildcards * (match any number of characters) and ? (match only one character) can be used. This is an alphanumeric field with a 255 character limit.
 - (Optional) **Evaluate as a Regular Expression** — The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards. (See [Examples of JAVA Regular Expressions for MRA Routes](#) for examples of using JAVA Regular Expressions.)
 - **Add** — This adds the host identities to the field.
Note: Clicking **Delete** deletes a selected host identity.
 - **Origin (Default "Any")** — Enables a message to be routed based on the message's Origin-Host. For example, if **MPE** is selected, then it is an MPE originated message (meaning that any messages that originated from any managed MPE are applied to this route).
Note: If topology hiding is enabled, the message is processed based on the original Origin-Host in the routing table, since topology hiding processing takes place after the routing table.
 - **Application ID** — Select **Rx** (default), **Gq**, **Ty**, **Gx**, **Gy**, **Gxx**, **Sh**, **Sd**, **Sy**, **S9**, or **All**.




Note: You can include only one application per route rule. For multiple applications, create multiple rules.

- **User ID type** — Select **ANY** (default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
- **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use an asterisk (*) as a wildcard character. To add the user ID to the list, click **Add**; to remove one or more user IDs from the list, select them and click **Delete**.
- **Action** — Select **PROXY** (stateful route, the default), **RELAY** (stateless route), or **LOCAL** (process on this device).
- **Server ID** — Select a destination peer from the list.



Note: You can define a server with a Diameter identity.

c) When you finish, click **Save**.

6. (Optional) Clone, Add, delete, modify, or order entries.

- Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is added to the table
- Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
- Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.
- Ordering the list.

If you define multiple entries, they are searched in the order displayed in this list. To change the order:

1. Select an entry.
2. Click  **Up** or  **Down**. The search order is changed.

7. Define the default route:

- a) Click **Edit** in the **Default Route** section.
- b) Select the default action. (**PROXY**, **RELAY**, or **LOCAL**) and peer server ID. When you finish, click **Save**.

8. To delete the default route, click **Delete**.

9. When you finish, click **Save**.

The Diameter routes are configured with the Realm/Host Identities column displaying the Realm or Host name for the configured route.

Configuring Diameter Realm Based Peer Routes

By default, Diameter messages are processed locally. In a network with multiple Policy Management devices, messages can be routed, by realm, application, or user ID, for processing by peers or other realms.

Note: Diameter messages can be routed in either an MPE or MRA the steps listed below can be used for either device.




Use this procedure if you have an extensive peer network or a network that includes multiple realms, user IDs or applications.

To configure the Diameter realm based peer routes:



1. From the Policy Management device (either **Policy Server** or **MRA** 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 Server** or **MRA** that needs diameter routing.
The **Policy Server Administration** or **MRA Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
The Diameter Routing configuration settings display.
4. Click **Modify Routes**.
The **Modify the Diameter Route Table** page opens.
5. Add a route to the table
 - a) Click **Add**.
The **Add Diameter Route** window opens.
 - b) Configure the route using the following fields.
 - **Diameter Realm** — For example, **Example.com**.
 - **Application ID** — Select Rx (default), Gq, Ty, Gx, , Gxx, Sd, Sh, Sy, Gy, S9, or All.
Note: You can include only one application per route rule. For multiple applications, create multiple rules.
 - **User ID type** — Select ANY (default), E.164(MSISDN), IMSI, IP, NAI, PRIVATE, SIP_URI, or USERNAME.
 - **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use a period followed by an asterisk (.) as a wildcard character. To add the user ID to the list, click **Add**; to remove one or more user IDs from the list, select them and click **Delete**.
 - **Evaluate as Regular Expression** — The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards.
Note: Regular expressions are specifically JAVA expressions and using any other language expression will result in a failed status. See [Examples of JAVA Regular Expressions for MRA Routes](#) for more information about using regular expressions for MRA routes.

- **Action** — Select **PROXY** (stateful route, default), **RELAY** (stateless route), or **LOCAL** (process on this device).
- **Server ID** — Select a destination peer from the list.

Note: You can define a server with a Diameter identity.

- c) Click **Save**.
6. (Optional) Add, delete, modify, or order entries.
 - Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is added to the table
 - Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
 - Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.
 - Ordering the list.

If you define multiple entries, they are searched in the order displayed in this list. To change the order:

 1. Select an entry.
 2. Click  **Up** or  **Down**. The search order is changed.
7. Define the default route:
 - a) Click **Edit** in the **Default Route** section.
 - b) Select the default action: **PROXY**, **RELAY**, or **LOCAL**.
 - c) Select the peer server ID.
 - d) Click **Save**.
8. To delete the default route, click **Delete**.
9. Click **Save**.

The Diameter realm based peer routes are configured.

Examples of JAVA Regular Expressions for MRA Routes

The following sample regular expressions are for MRA Routes.

- For E164 numbers ending in 00 to 24: `#E164:1234.*?(?:0\d|1\d|2[0-4])`

- For E164 numbers ending in 25 to 49: #E164:1234.*?(?:2[5-9]|3\d|4\d)
- For E164 numbers ending in 50 to 74: #E164:1234.*?(?:5\d|6\d|7[0-4])
- For E164 numbers ending in 75 to 99: #E164:1234.*?(?:7[5-9]|8\d|9\d)

Working with MRA Groups

MRA groups let you organize MRA cluster profiles into groups. You can create, rename, and delete MRA groups, and add and remove MRA cluster profiles from groups.

Creating an MRA Group

You create an MRA group to manage various MRA functions (such as creating stateless sessions) on your wireless network.

To create an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
The **MRA Administration** page opens in the work area.
3. Click **Create Group**.
The **Create Group** page opens.
4. Enter the name of the new MRA group.
The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. Click **Save**.

The MRA group is created.

Adding an MRA Cluster Profile to an MRA Group

After an MRA group is created, you can add MRA cluster profiles to it. To add an MRA cluster profile to an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA group.
The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.
3. Click **Add Multi-protocol Routing Agent**.
The **Add Multi-protocol Routing Agent** page opens.
4. Select the MRA cluster profile you want to add or press the Ctrl or Shift key to select multiple MRA cluster profiles.
5. Click **Save**.

The MRA cluster profile is added to the MRA group.

Removing an MRA Cluster Profile from an MRA Group

As your network system changes, say from an upgrade or addition of a new protocol, the profiles on your existing MRAs may become outdated. In such instances, you can remove an MRA profile from an existing MRA.

Note: Removing an MRA cluster profile from an MRA group does not delete the MRA cluster profile from the **ALL** group, so it can be used again if needed. But removing an MRA cluster profile from the **ALL** group will delete it from all other groups in the system.

To remove an MRA cluster profile from an MRA group (other than **ALL**):

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. Select the MRA group which displays the contents of MRA group.
3. Remove the MRA cluster profile using one of the following methods:
 - Select **All** from the navigation pane. From the **MRA Administration** page, click the **Remove** icon (scissors), located to the right of the MRA cluster profile you want to remove.
 - From the content tree, select the MRA cluster profile which displays the **MRA Administration** page. On the **System** tab, click **Remove**.

The MRA cluster profile is removed from the group.

Deleting an MRA Group or Sub-group

An existing MRA groups as well as any associated sub-groups can be deleted from a system, for example if an MRA is to be replaced or upgraded.

Note: Deleting an MRA group also deletes any associated sub-groups. However, any MRA cluster profiles associated with the deleted groups or sub-groups remain in the **ALL** group.

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

To delete an MRA group or sub-group:

1. From the **MRA** section of the navigation pane, select **Configuration** which displays a list of the MRA groups; the initial group is **ALL**.
2. Select the **MRA** group or subgroup from the content tree.
The contents of the selected MRA group are displayed.
3. Click **Delete** which opens a confirmation message.
4. Click **OK** to complete the procedure.

Enabling Stateless Routing

Use this procedure to be able to manage more sessions within a time period.

To enable a stateful MRA device to run as statelessly:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the MRA from the content tree.
The **MRA Administration** page displays the configuration for the MRA.

3. Select the **System** tab.
The **Modify System Settings** page opens.
4. Select **Stateless Routing** ([Figure 30: Enabling Stateless Routing](#) shows an example).

The stateful MRA configuration is hidden.

The screenshot shows the 'MRA Administration' window. At the top, it says 'Multi-protocol Routing Agent: MRA1'. Below this is a tabbed interface with 'System', 'Reports', 'Logs', 'MRA', 'Diameter Routing', and 'Session Viewer'. The 'System' tab is active, displaying the 'Modify System Settings' page. Under the 'Configuration' section, there are fields for 'Associated Cluster' (set to 'MRA1'), 'Name' (set to 'MRA1'), and 'Description / Location'. Below these are checkboxes for 'Secure Connection' (unchecked) and 'Stateless Routing' (checked). At the bottom are 'Save' and 'Cancel' buttons.

Figure 30: Enabling Stateless Routing

Reapplying the Configuration to Policy Management Devices

You can reapply the configuration to an individual MPE or MRA device (server), or to all MPE or MRA devices in a group. When you reapply the configuration, the CMP system completely reconfigures the server with topology information, ensuring that the configuration matches the data in the CMP system. 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 server 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 status of the failed servers.
- After upgrading the software on a server, it is recommended that you reapply the configuration from the CMP system to ensure that the upgraded server and the CMP system are synchronized.
- The server configuration may 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 server). If such a condition occurs, the CMP system displays the server status on its **System** tab with the notation **Config Mismatch**. You can click the notice to display a report comparing the server configuration with the CMP database information. Reapplying the configuration brings the server back into synchronization with the CMP database.

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. To reapply the configuration for an individual MPE or MRA device:

- a) From the content tree, select the **ALL** group.
The **Policy Server Administration** page opens in the work area.
- b) From the **ALL** group, select the server.
The **Policy Server Administration** page opens to the **System** tab, displaying information for that server.
- c) Click **Reapply Configuration**.
An in-progress message appears. When the operation is complete you are prompted, The configuration was applied successfully.

The individual server or all of the servers in a group are synchronized with the CMP system.

Resetting Counters

The **Reset Counters** option is included in the **Operations** list when the **Stats Reset Configuration** option is set to **Interval**. The **Reset All Counters** option is included in the **Operations** list when the **Stats Reset Configuration** option is set to **Manual**. See [Setting Stats Settings](#) for more information.

To reset the counters associated with a group of MPE or MRA servers:

1. From the **Policy Server** or **MRA** 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 group that contains the servers of interest.
The **Policy Server Administration** page opens in the work area.
3. From the **Operations** list, select **Reset Counters** or **Reset All Counters**.
The **Bulk Reset All Counters** or **Bulk Reset Counters** dialog displays showing the number of servers affected.
4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60.
The default value is 0.

The counters are reset.

About Stateless Routing

Stateless routing allows the MRA to route diameter messages to MPE devices or other devices, without the need to maintain state. Typically, the MRA selects an MPE device for a user, and continues to use the same MPE for the user by maintaining session state. Using stateless routing, static routes are configured ahead of time, so the state does not need to be maintained.

Using stateless routing, the MRA establishes a diameter connection with every peer that is defined in the Diameter Peer Table, where a peer consists of a name, IP address, diameter realm, diameter identity, and port. A route consists of a diameter realm, application ID, user ID, action, and server ID. The Action can be either proxy or relay.

Stateless routing uses routing based on FramedIPAddress and FramedIPv6Prefix, with wildcard pattern matching. The IP address must be configured in either dotted decimal notation for IPv4 or expanded notation for IPv6 excluding the prefix length.

The MRA processes routes in the order of their configured priority, which is based on the order in which they were configured in the route. If the destination of a route is unreachable, the route with the next highest priority is used. If no available routes are found, the MRA returns a

DIAMETER_UNABLE_TO_DELIVER error message. If a destination is currently up when the route is chosen but the forwarded request times out, the MRA returns a DIAMETER_UNABLE_TO_DELIVER error message and does not try the next route.

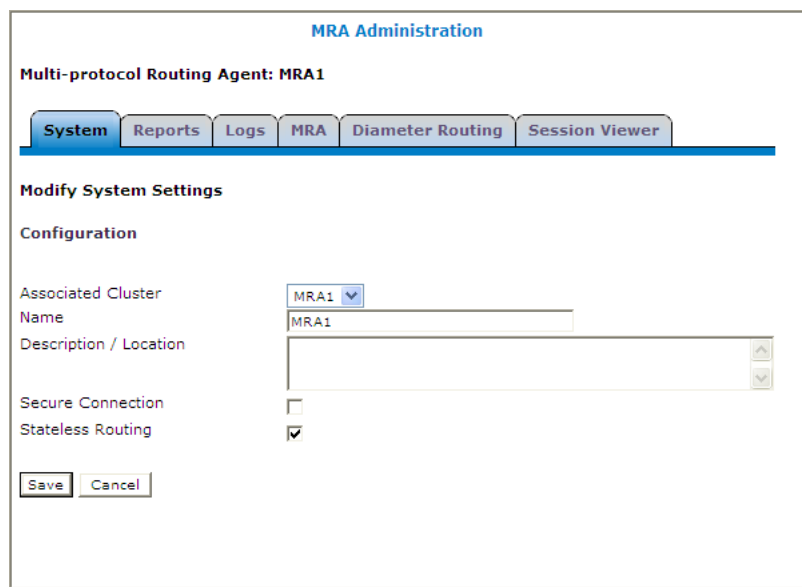
Enabling Stateless Routing

Use this procedure to be able to manage more sessions within a time period.

To enable a stateful MRA device to run as statelessly:

1. From the **MRA** section of the navigation pane, select **Configuration**.
The content tree displays a list of MRA groups; the initial group is **ALL**.
2. Select the MRA from the content tree.
The **MRA Administration** page displays the configuration for the MRA.
3. Select the **System** tab.
The **Modify System Settings** page opens.
4. Select **Stateless Routing** ([Figure 31: Enabling Stateless Routing](#) shows an example).

The stateful MRA configuration is hidden.



The screenshot shows the 'MRA Administration' window for 'Multi-protocol Routing Agent: MRA1'. It has tabs for 'System', 'Reports', 'Logs', 'MRA', 'Diameter Routing', and 'Session Viewer'. The 'System' tab is active, showing 'Modify System Settings'. Under the 'Configuration' section, there are fields for 'Associated Cluster' (set to 'MRA1'), 'Name' (set to 'MRA1'), and 'Description / Location'. Below these are checkboxes for 'Secure Connection' (unchecked) and 'Stateless Routing' (checked). At the bottom are 'Save' and 'Cancel' buttons.

Figure 31: Enabling Stateless Routing

Modifying the Stateless Migration Mode in an Existing MRA

When modifying an existing MRA, you can enable or disable the **Enable Stateless Migration Mode** which enables the MRA device to use static routes to transition to a stateless migration mode.

Use this procedure when you want to use static routes in your transition to stateless migration

To enable and disable the migration mode setting:

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

2. Select the MRA device from the content tree.
The **MRA Administration** page opens, displaying information about the selected MRA device.
3. Select the **MRA** tab.
4. Click **Advanced**.
5. In the **Stateful MRA Settings** section of the page, select **Enable Stateless Migration Mode** (or leave the box unchecked if you do not want to enable the migration mode).
The stateless migration mode is enabled.
6. Click **Save**.

The MRA device is put into migration mode.

Loading MPE/MRA Configuration Data when Adding Diameter Peer

When adding a diameter peer, select a peer from the list on the **Diameter Routing** tab. After the peer is selected, the peer configuration fields are automatically populated.

Chapter 14

Managing S-CMP Devices

Topics:

- [About S-CMP Devices.....232](#)
- [About S-CMP Groups.....234](#)

This chapter describes how to use the NW-CMP system to configure and manage S-CMP devices in a tiered CMP system. The S-CMP devices manage the MPE and MRA devices in a tiered the Policy Management policy server.

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

About S-CMP Devices

A System Configuration Management Platform (S-CMP) device manages MPE and MRA devices in a tiered Network CMP system. The Network CMP system contains one or more S-CMP. The S-CMP can view, but not modify anything that is created, edited, or deleted at the Network Configuration Management Platform (NW-CMP) level. The S-CMP blocks users from changing associations set at the NW-CMP layer in order to maintain data integrity between the NW-CMP and the S-CMP devices.

The S-CMP can create the following associations to the MPE device:

- Applications
- Network Elements
- Network Element Groups
- Policies
- Policy Groups

The S-CMP can create the following associations to the MRA device:

- MPE and MRA Pools
- Network Elements
- Network Element Groups

Creating an S-CMP Device

To create an S-CMP device:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
The **S-CMP Administration** page opens in the work area.
3. Click **Create S-CMP**.
The **New S-CMP** page opens.
4. Enter information for the S-CMP:
 - a) **Name** (required) — The name you assign to the S-CMP.
The name can be up to 255 characters long and must not contain colons (:), quotation marks ("), or commas (,).
 - b) **Site One VIP** (required) — The first Virtual IP Address (VIP) for the S-CMP.
 - c) **Site Two VIP** — The second VIP for the S-CMP. If the S-CMP has is in a georedundant cluster, then both VIP sites (1 and 2) must be specified. These VIP addresses are populated in the NW-CMP and are used by the NW-CMP when querying or pushing data to the S-CMP.
 - d) **Secure Connection** — Indicates that this S-CMP has https enabled, therefore, the NW-CMP connects to the S-CMP using a secure connection secure connection (https).
 - e) **Description** — Free-form text that identifies the S-CMP device within the network.
Enter up to 250 characters.

5. Click **Save**.

The S-CMP device is displayed in the **S-CMP Administration** page.

Opening an S-CMP Device from an NW-CMP

To open an S-CMP device from an NW-CMP:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
The **S-CMP Administration** page opens in the work area.
3. Select an S-CMP.
The configuration for the S-CMP displays in the Work Area.
4. If the server is active, click the S-CMP name in the work area.

The S-CMP opens in a new browser tab.

Modifying an S-CMP Device

To modify an S-CMP device:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
The **S-CMP Administration** page opens in the work area.
3. Select an S-CMP.
The configuration for the S-CMP displays in the work area.
4. Click **Modify**.
The **Modify S-CMP** page opens in the work area.
5. Make configuration changes.
See [Creating an S-CMP Device](#) for information about the fields.
6. Click **Save**.

The S-CMP device is updated with the new configuration.

Reapplying the Configuration to S-CMP Devices

You can reapply the configuration to an individual S-CMP device. You must reapply the configuration after the S-CMP is modified.

To reapply the configuration to the S-CMP device:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.


2. Select the **S-CMPs** group.
The **S-CMP Administration** page opens in the work area.
3. Select an S-CMP.
The configuration for the S-CMP displays in the work area.
4. Click **Reapply Configuration**.
The current setting for the S-CMP are applied.

The individual server is synchronized with the configuration on the NW-CMP device.

Deleting an S-CMP Device

To delete an S-CMP:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. You can delete a profile using one of the following methods.
 - Select the **S-CMPs** folder and then click  (trash can) in the work area for the device. A confirmation message displays.
 - Select a device from the **S-CMPs** folder and then click **Delete**. A confirmation message displays.
3. Click **OK** to delete.
The profile is deleted.

About S-CMP Groups

For organizational purposes, you can aggregate the S-CMP devices in your tiered network into groups. The following subsections describe how to manage S-CMP groups.

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

Creating an S-CMP Group

To create an S-CMP group:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
The **S-CMP Administration** page opens in the work area.
3. Click **Create Group**.
The **Create Group** page opens.
4. Enter the name of the new S-CMP group.
The name cannot contain quotation marks (") or commas (,).

5. (Optional) Enter a description for the group.
The description must not exceed 250 characters.
6. Click **Save**.

You have created a an S-CMP group.

Adding S-CMP Devices to a Policy Server Group

To add S-CMP devices to an S-CMP group:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices. See [About Mode Settings](#) for more information.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. From the content tree, select the S-CMP group.
The **S-CMP Administration** page opens in the work area displaying the contents of the selected S-CMP group.
3. Click **Add S-CMP**.
The **Add S-CMP** page opens, displaying the S-CMP devices not already part of the group.
4. Click the S-CMP device you want to add; use Ctrl or Shift-Ctrl to select multiple S-CMP devices.
5. Click **Save**.

The S-CMP devices are added to the selected group.

Creating an S-CMP Sub-group

You can create sub-groups to further organize your tiered CMP network. To add an S-CMP sub-group to an existing S-CMP group:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. From the content tree, select the S-CMP group.
The **S-CMP Administration** page opens in the work area, displaying the contents of the selected S-CMP 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. (Optional) Enter a description for the group.
The description must not exceed 250 characters.
6. Click **Save**.

The sub-group is added to the selected group.

Renaming an S-CMP Group

To modify the name assigned to an S-CMP group or sub-group:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. Select the policy server group or sub-group.
The **S-CMP 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.

Deleting an S-CMP Group

Deleting an S-CMP group also deletes any associated sub-groups. You cannot delete the ALL group.

To delete an S-CMP group or subgroup:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
The content tree displays the **S-CMPs** group.
2. Select the S-CMP group or sub-group.
The **S-CMP Administration** page opens in the work area, displaying the contents of the selected S-CMP group or sub-group.
3. Click **Delete**.
A confirmation message displays.
4. Click **Save**.
The S-CMP group is deleted.

Chapter 15

System-Wide Report

Topics:

- [KPI Dashboard.....238](#)
- [Subscriber Activity Log.....266](#)
- [Viewing the Trending Reports.....272](#)
- [Viewing Alarms.....279](#)
- [Viewing Session Reports.....283](#)
- [Viewing Other Reports.....287](#)

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.

KPI Dashboard

The KPI Dashboard provides a multi-site system-level summary of performance and operational health indicators. The display includes indicators for:

- Offered load (transaction rate)
- System capacity (counters for active sessions)
- Inter-system connectivity
- Resource utilization (memory, CPU)
- System status
- Alarms
- Protocol errors

The KPI dashboard displays the indicators for all the systems on a single page, with each MRA KPIs in a separate table when MRA systems are managed by the CMP system or with all MPE KPIs in one table when MRA systems are not managed by the CMP system (that is, an MPE-only deployment). Each row within a table represents a single system (either an MPE or MRA server). The table cells are rendered using a color scheme to highlight areas of concern that is well adopted by the telecommunication industry. The table contents are periodically refreshed every 10 seconds; this time period is not configurable. The color changing thresholds are user configurable.

Note: When you are in a NW-CMP, the KPI Dashboard lists the S-CMP servers only. Click an S-CMP name to open the KPI Dashboard for that specific server.

Figure 32: Example of KPI Dashboard with MRA Devices Managed by the CMP System illustrates the dashboard's contents when MRA systems are managed by the CMP system.

KPI Dashboard (Stats Reset: Interval / Last Refresh: 09/20/2013 11:59:27)

	Performance			Alarms			Protocol Errors	
	TPS	PDN	Active Subscribers	Critical	Major	Minor	Sent	Received
MRAs selected	40	6000	6000	0	0	0	0	0
MPEs selected	37	13262	13261	0	0	0	0	0

mra17-118		Performance					Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-118(Server-A)	Standby				3	34								
mra17-118(Server-B)	Active	20 (0%)	3000 (0%)	3000 (0%)	4	46	3 of 4	2 of 2	1 of 4	0	0	0	0	0
MPE		State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources	Critical	Major	Minor	Sent	Received
mpe17-111(Server-A)	Standby				4	37								
mpe17-111(Server-B)	Active	11 (0%)	3953 (0%)	3951 (0%)	4	60	2 of 2	0 of 0		0	0	0	0	0
mpe17-115(Server-A)	Active	7 (0%)	4810 (0%)	4811 (0%)	3	55	1 of 2	0 of 0		0	0	0	0	0

mra17-122		Performance					Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-122(Server-A)	Standby				3	33								
mra17-122(Server-B)	Active	20 (0%)	3000 (0%)	3000 (0%)	3	46	2 of 3	2 of 2	1 of 4	0	0	0	0	0
MPE		State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources	Critical	Major	Minor	Sent	Received
mpe17-116	Off-line	----	----	----	----	----	----	----	----	----	----	----	----	----
mpe17-117(Server-A)	Standby				4	39								
mpe17-117(Server-B)	Active	19 (0%)	4499 (0%)	4499 (0%)	4	60	2 of 2	0 of 0		0	0	0	0	0

Figure 32: Example of KPI Dashboard with MRA Devices Managed by the CMP System

The **MRAs selected** row displays the aggregation count for user-selected MRA devices. The **MPEs selected** row displays the aggregation count for the MPE devices that belong to the user-selected MRA devices.

The following counts are aggregated for selected MRA databases and the associated MPE devices:

- TPS
- PDNs
- Active Subscribers
- Critical Alarm Count
- Major Alarm Count
- Minor Alarm Count
- Protocol Errors Sent
- Protocol Errors Received

Note: Isolated MPE devices are not included in the aggregation counts.


When there are no MRA devices managed by the CMP system, the displayed headings are:

- Name of MPE
- Performance:
 - State
 - TPS
 - PDN
 - Active Sessions
 - CPU %
 - Memory %
- Connections
 - Data Sources
 - Network Elements
- Alarms
 - Critical
 - Major
 - Minor
- Protocol Errors
 - Sent
 - Received

In the top right corner there is a **Change Thresholds** button that allows you to change threshold settings used to determine cell coloring. When MRA devices are managed by the CMP system, a button on the top left corner lists each of the MRA devices with a check box that allows the user to enable/disable the table for that MRA device.

Individual servers are identified by name and the order in which they were defined within their cluster (Server-A, Server-B, Server-C). If any of these are set to Reverse Site Preference, then an "R" will appear by the server's State. For the standby or spare server, several columns are not populated (since those servers are not active); the only columns that contain data are: Status, CPU%, and Memory%. For

Connections, Alarms, and Protocol Errors, the column's information is a hyperlink that will open a more detailed report.

A cloud icon () indicates that the server is executing on a virtual machine.

If a monitored system is unreachable, or if the data is unavailable for some reason, then the status is set to `Off-line` and the values in all the associated columns is cleared. In this situation, the entire row is displayed with the error color (red). If a monitored system does not support KPI retrieval then the status is set to `N/A` and the values in all the associated columns are cleared. No coloring is applied.

The columns that display information in the form of X (Y%) (e.g. TPS and PDN Connections"/"Sessions) correspond to the following: X represents the actual numeric value and Y represents the % of rated system capacity that is consumed. If the system is executing on a virtual machine, values for TPS, Sessions, and Active Subscribers are only calculated if capacity values are explicitly set. See [Configuring Expert Settings](#) for more information.

The columns that display connection counts are displayed in the form X of Y where X is the current number of connections and Y is the configured number of connections. When X and Y are not the same, the column uses the warning color to indicate a connectivity issue, unless X is 0, in which case the error color is displayed.

The Alarm and Protocol Errors columns display the number of current events. If there are any Critical or Major alarms, then these cells will be colored red or yellow, respectively.

Note: To learn more about an alarm and how to resolve it, see the *Troubleshooting Reference* for this release.

Click the name of an MPE or MRA device to display detailed statistics. For more information on detailed device statistics, see the description on the **Reports** tab for the device.

Mapping Display to KPIs

The following tables explain how each of the columns in the KPI dashboard are mapped to a specific statistic in the KPI statistics. On the initial KPI Dashboard window, KPIs for each MRA and MPE device are shown. Since the tables contain row entries for the active, standby and spare servers (if georedundancy is configured), the mapping is described for all three servers. [Table 13: KPI Definitions for MRA Devices](#) shows the mappings for MRA devices; [Table 14: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System](#) shows the mappings for MPE devices when the MRA devices are managed by the CMP system; and [Table 15: KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System](#) shows the mappings for MPE devices when the MRA devices are not managed by the CMP system.

Table 13: KPI Definitions for MRA Devices

KPI Dashboard Column	Mapping to Statistics	
	Active server	Standby and spare server (spare only shows Status, CPU % and Memory%)
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus

KPI Dashboard Column	Mapping to Statistics	
	Active server	Standby and spare server (spare only shows Status, CPU % and Memory%)
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOfCapacity	None
Active Subscribers	CurrentMRABindingCount and CurrentMRABindingPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
MPE Connections	A value in the form X of Y, where: X is CurrentMPEConnectionCount Y is ConfiguredMPEConnectionCount	None
MRA Connections	A value in the form X of Y, where: X is CurrentMRAConnectionCount Y is ConfiguredMRAConnectionCount	None
Network Element Connections	A value in the form X of Y, where: X is CurrentConnectedNECount Y is ConfiguredNECount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Table 14: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	Standby server
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOfCapacity	None
Active Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
MRA Connections	A value in the form X of Y , where: X is CurrentMRAConnectionCount Y is ConfiguredMRAConnectionCount	None
Data Sources	A value in the form X of Y , where: X is CurrentSPRConnectionCount Y is ConfiguredSPRConnectionCount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Table 15: KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	Standby server
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
Active Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
SPR Connections	A value in the form X of Y , where: X is CurrentSPRConnectionCount Y is ConfiguredSPRConnectionCount	None
Network Element Connections	A value in the form X of Y , where: X is CurrentConnectedNECount Y is ConfiguredConnectedNECount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Clicking on an MRA or MPE name opens the **Reports** tab. See the **Reports** tab for the device for details on reports.

Mapping Reports Display to KPIs

From the KPI Dashboard, you can click any MPE or MRA system shown to open the **Reports** page. From there, a variety of statistics and measurements can be viewed. In the following tables, these statistics are mapped to their names as they appear in OSSI XML output.

- [Table 16: Policy Statistics](#)
- [Table 17: Quota Profile Statistics Details](#)
- [Table 18: Diameter Application Function \(AF\) Statistics](#)
- [Table 19: Diameter AF Peer Stats \(in Diameter AF Stats window\)](#)
- [Table 20: Diameter Policy Charging Enforcement Function \(PCEF\) Statistics](#)
- [Table 21: Diameter Charging Function \(CTF\) Statistics](#)
- [Table 22: Diameter Bearer Binding and Event Reporting Function \(BBERF\) Statistics](#)
- [Table 23: Diameter TDF Statistics](#)
- [Table 24: Diameter Sh / Sh Peer Statistics](#)
- [Table 25: Diameter S9 Statistics](#)
- [Table 26: Diameter Distributed Routing and Management Application \(DRMA\) Statistics](#)
- [Table 27: Diameter DRA Statistics](#)
- [Table 28: Diameter Sy Statistics](#)
- [Table 29: RADIUS Statistics](#)
- [Table 30: Diameter Latency Statistics](#)
- [Table 31: Diameter Event Trigger Statistics](#)
- [Table 32: Diameter Protocol Error Statistics](#)
- [Table 33: Diameter Connection Error Statistics](#)
- [Table 34: LDAP Data Source Statistics](#)
- [Table 35: Sh Data Source Statistics](#)
- [Table 36: Sy Data Source Statistics](#)
- [Table 37: KPI Interval Statistics](#)

For more information on the OSSI XML interface, see *OSSI XML Interface Definitions Reference*.

Table 16: Policy Statistics

Display	MPE	MRA	Name
Peg Count	Y	N	Policy Count
Evaluated	Y	N	Evaluated Count
Executed	Y	N	Executed Count
Ignored	Y	N	Ignored Count
Policy Details Stats			
Name	Y	N	Policy Name
Evaluated	Y	N	Eval Count
Executed	Y	N	Trigger Count
Ignored	Y	N	Ignore Count

Display	MPE	MRA	Name
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	Data for each installed rule

Table 17: Quota Profile Statistics Details

Display	MPE	MRA	Name
Peg Count	Y	N	Quota Count
Activated	Y	N	Quota Activated Count
Volume Threshold Reached	Y	N	Quota Volume Threshold Reached Count
Time Threshold Reached	Y	N	Quota Time Threshold Reached Count
Event Threshold Reached	Y	N	Quota Event Threshold Reached Count

Table 18: Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
AAR messages received/sent	Y	Y	AAR Recv Count\AAR Send Count
AAR Initial messages received/sent	Y	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR Modification messages received/sent	Y	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages received/sent	Y	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages received/sent	Y	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages received/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count

Display	MPE	MRA	Name
ASA success messages received/sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages received/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages received/sent	Y	Y	STR Recv Count\STR Send Count
STR messages timeout	Y	Y	STR Timeout Count
STA success messages received/sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages received/sent	Y	Y	STA Recv Failure Count\STA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Cleanup ASA received	Y	Y	ASA Received Count
Cleanup ASR sent	Y	Y	ASR Sent Count
Current number of active sponsored sessions	Y	N	Current Sponsored Session Count
Max sponsored active sessions	Y	N	Max Sponsored Session Count
Current number of active sponsors	Y	N	Current Sponsor Count
Max number of sponsors	Y	N	Max Sponsor Count
Current number of active service providers	Y	N	Current Service Provider Count
Max number of service providers	Y	N	Max Service Provider Count
Currently active emergency sessions	Y	N	Current Emergency Session Count
Max active emergency sessions	Y	N	Max Active Emergency Session Count

Table 19: Diameter AF Peer Stats (in Diameter AF Stats window)

Display	MPE	MRA	Name
ID	Y	Y	
IP Address: Port			

Display	MPE	MRA	Name
Currently active connections			
Currently active sessions			
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time

Table 20: Diameter Policy Charging Enforcement Function (PCEF) Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count (SCTP or TCP)
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count

Display	MPE	MRA	Name
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Currently active emergency sessions	Y	N	Current Emergency Session Count
Max active emergency sessions	Y	N	Max Active Emergency Session Count

Table 21: Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Connections	N	Y	Conn Count
Currently OK peers	N	Y	Peer Okay Count
Currently down/suspect/reopened peers	N	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	N	Y	Msg In Count\Msg Out Count
CCR messages sent/received	N	Y	CCR Recv Count\CCR Send Count
CCA success messages recd/sent	N	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages sent/received	N	Y	CCR-I Recv Count\CCR-I Send Count
CCA-I success messages recd/sent	N	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	N	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages sent/received	N	Y	CCR-U Recv Count\CCR-U Send Count

Display	MPE	MRA	Name
CCA-U success messages recd/sent	N	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	N	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages sent/received	N	Y	CCR-T Recv Count\CCR-T Send Count
CCA-T success messages recd/sent	N	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	N	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages sent/received	N	Y	RAR Recv Count\RAR Send Count
RAA success messages recd/sent	N	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	N	Y	RAA Recv Failure Count\RAA Send Failure Count
ASR messages sent/received	N	Y	ASR Recv Count\ASR Send Count
ASA success messages recd/sent	N	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages recd/sent	N	Y	ASA Recv Failure Count\ASA Send Failure Count
Currently active sessions	N	Y	Active Session Count
Max active sessions	N	Y	Max Active Session Count

Table 22: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count

Display	MPE	MRA	Name
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter BBERF connections	Y	Y	

Table 23: Diameter TDF Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count

System-Wide Report

Display	MPE	MRA	Name
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
TSR messages received/sent	Y	Y	
TSA success messages received/sent	Y	Y	
TSA failure messages received/sent	Y	Y	
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter TDF connections	Y	Y	

Table 24: Diameter Sh / Sh Peer Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
Messages retried due to error response	Y	N	
Messages retried due to response timeout	Y	N	
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count
UDR messages timeout	Y	N	UDR Timeout Count
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages from session updates	Y	N	
UDA success messages received/sent	Y	N	UDA Success Messages Received Count\UDA Success Messages Sent Count
UDA failure messages received/sent	Y	N	UDA Failure Messages Received Count\UDA Failure Messages Sent Count
PNR messages received/sent	Y	N	PNR Messages Received Count\PNR Messages Sent Count
PNA success messages received/sent	Y	N	PNA Success Messages Received Count\PNA Success Messages Sent Count
PNA failure messages received/sent	Y	N	PNA Failure Messages Received Count\PNA Failure Messages Sent Count

Display	MPE	MRA	Name
PUR messages received/sent	Y	N	PUR Messages Received Count\PUR Messages Sent Count
PUR messages timeout	Y	N	PURTimeout Count
PUR messages retried due to error response	Y	N	
PUR messages retried due to response timeout	Y	N	
PUA success messages received/sent	Y	N	PUA Success Messages Received Count\PUA Success Messages Sent Count
PUA failure messages received/sent	Y	N	PUA Failure Messages Received Count\PUA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SNR Messages Sent Count
SNR messages timeout	Y	N	SNRTimeout Count
SNR messages retried due to error response	Y	N	
SNR messages retried due to response timeout	Y	N	
SNA success messages received/sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/send	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
Currently active sessions	Y	N	Active Sessions Count
Max active sessions	Y	N	Maximum Active Sessions Count
Diameter Sh connections			

Table 25: Diameter S9 Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count

Display	MPE	MRA	Name
CCR messages received/sent	Y	N	CCR Messages Received Count\CCR Messages Sent Count
CCR messages timeout	Y	N	CCRTimeout Count
CCA success messages received/sent	Y	N	CCA Success Messages Received Count\CCA Success Messages Sent Count
CCA failure messages received/sent	Y	N	CCA Failure Messages Received Count\CCA Failure Messages Sent Count
CCR-I messages received/sent	Y	N	CCR-I Messages Received Count\CCR-I Messages Sent Count
CCR-I messages timeout	Y	N	CCRTimeout Count
CCA-I success messages received/sent	Y	N	CCA-I Success Messages Received Count\CCA-I Success Messages Sent Count
CCA-I failure messages received/sent	Y	N	CCA-I Failure Messages Received Count\CCA-I Failure Messages Sent Count
CCR-U messages received/sent	Y	N	CCR-U Messages Received Count\CCR-U Messages Sent Count
CCR-U messages timeout	Y	N	CCRTimeout Count
CCA-U success messages received/sent	Y	N	CCA-U Success Messages Received Count\CCA-U Success Messages Sent Count
CCA-U failure messages received/sent	Y	N	CCA-U Failure Messages Received Count\CCA-U Failure Messages Sent Count
CCR-T messages received/sent	Y	N	CCR-T Messages Received Count\CCR-T Messages Sent Count
CCR-T messages timeout	Y	N	CCRTimeout Count
CCA-T success messages received/sent	Y	N	CCA-T Success Messages Received Count\CCA-T Success Messages Sent Count
CCA-T failure messages received/sent	Y	N	CCA-T Failure Messages Received Count\CCA-T Failure Messages Sent Count
RAR messages received/sent	Y	N	RAR Messages Received Count\RAR Messages Sent Count
RAR messages timeout	Y	N	RARTimeout Count

Display	MPE	MRA	Name
RAA success messages received/sent	Y	N	RAA Success Messages Received Count\RAA Success Messages Sent Count
RAA failure messages received/sent	Y	N	RAA Failure Messages Received Count\RAA Failure Messages Sent Count
Currently active inbound sessions	Y	N	Active Inbound Sessions Count
Max active inbound sessions	Y	N	Maximum Active Inbound Sessions Count
Currently active outbound sessions	Y	N	Active Outbound Sessions Count
Max active outbound sessions	Y	N	Maximum Active Outbound Sessions Count

Table 26: Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently okay peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
DBR messages received/sent	N	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	N	Y	DBRTimeout Count
DBA success messages received/sent	N	Y	DBARecv Success Count\DBASend Success Count
DBA failure messages received/sent	N	Y	DBARecv Failure Count\DBASend Failure Count
DBA message received/sent – binding found	N	Y	Binding Found Recv Count\Binding Found Send Count
DBA messages received/sent – binding not found	N	Y	Binding Not Found Recv Count\Binding Not Found Send Count
DBA messages received/sent – PCRF down	N	Y	Binding Found Pcrf Down Recd Count\ Binding Found Pcrf Down Send Count
DBA messages received/sent – all PCRFs down	N	Y	All Pcrfs Down Recv Count\ All Pcrfs Down Send Count
DBR-Q messages received/sent	N	Y	

Display	MPE	MRA	Name
DBR-Q messages timeout	N	Y	
DBA-Q success messages received/sent	N	Y	
DBA-Q failure messages received/sent	N	Y	
DBR-QC messages received/sent	N	Y	
DBR-QC messages timeout	N	Y	
DBA-QC success messages received/sent	N	Y	
DBA-QC failure messages received/sent	N	Y	
DBR-U messages received/sent	N	Y	
DBR-U messages timeout	N	Y	
DBA-U success messages received/sent	N	Y	
DBA-U failure messages received/sent	N	Y	
DBR-T messages received/sent	N	Y	
DBR-T messages timeout	N	Y	
DBA-T success messages received/sent	N	Y	
DBA-T failure messages received/sent	N	Y	
DBR-S messages received/sent	N	Y	
DBR-S messages timeout	N	Y	
DBA-S success messages received/sent	N	Y	
DBA-S failure messages received/sent	N	Y	
RUR messages received/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages received/sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages received/sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages received/sent	Y	Y	LNRRecv Count\ LNRSend Count

Display	MPE	MRA	Name
LNK messages timeout	Y	Y	LNKTimeout Count
LNA success messages received/sent	Y	Y	LNAREcv Success Count\ LNASend Success Count
LNA failure messages received/sent	Y	Y	LNAREcv Failure Count\ LNASend Failure Count
LSR messages received/sent	Y	Y	LSRREcv Count\ LSRSend Count
LSR messages timeout	Y	Y	LSRTimeout Count
LSA success messages received/sent	Y	Y	LSAREcv Success Count\ LSASend Success Count
LSA failure messages received/sent	Y	Y	LSAREcv Failure Count\ LSASend Failure Count
SQR messages received/sent			
SQR messages timeout			
SQA messages received/sent			
SQA messages timeout			
Session found received/sent			
Session not found received/sent			
Diameter DRMA connections			

Note: The statistics listed in apply only to MRA devices.

Table 27: Diameter DRA Statistics

Display	MPE	MRA	Name
Currently active bindings	N	Y	DRABinding Count
Max active bindings	N	Y	Max DRABinding Count
Total bindings	N	Y	DRATotal Binding Count
Suspect bindings	N	Y	Suspect Binding Count
Detected duplicate bindings	N	Y	Detected Duplicate Binding Count
Released duplicate bindings	N	Y	Released Duplicate Binding Count
Diameter Release Task Statistics	N	Y	
Bindings Processed	N	Y	Release Bindings Processed
Bindings Released	N	Y	Release Bindings Removed
RAR messages sent	N	Y	Release RARs Sent
RAR messages timed out	N	Y	Release RARs Timed Out

Display	MPE	MRA	Name
RAA success messages recd	N	Y	Release RAAs Received Success
RAA failure messages recd	N	Y	Release RAAs Received Failure
CCR-T messages processed	N	Y	Release CCRTs Received

Table 28: Diameter Sy Statistics

Display	MPE	MRA	Name
Connections	Y	N	Current Connections Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Messages In Count\Messages Out Count
SLR messages received/sent	Y	N	SLR Messages Received Count\SLR Messages Sent Count
SLR messages timeout	Y	N	SLRTimeout Count
SLA success messages received/sent	Y	N	SLA Success Messages Received Count\SLA Success Messages Sent Count
SLA failure messages received/sent	Y	N	SLA Failure Messages Received Count\SLA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SMR Messages Sent Count
SNA success messages received/sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/sent	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
STR messages received/sent	Y	N	STR Messages Received Count\STR Messages Sent Count
STR messages timeout	Y	N	STRTimeout Count
STA success messages received/sent	Y	N	STA Success Messages Received Count\STA Success Messages Sent Count
STA failure messages received/sent	Y	N	STA Failure Messages Received Count\STA Failure Messages Sent Count

Display	MPE	MRA	Name
Currently active sessions	Y	N	Active Sessions Count
Max active sessions	Y	N	Maximum Active Sessions Count
Diameter Sy connections			

Table 29: RADIUS Statistics

Display	MPE	MRA	Name
Connections	Y	Y	
Total messages in/out	Y	Y	Messages In Count\ Messages Out Count
Total RADIUS messages received	Y	Y	
Total RADIUS messages send		Y	
Messages successfully decoded	Y	Y	
Messages dropped	Y	Y	
Total errors received	Y	Y	
Total errors sent	Y	Y	
Accounting Start sent	Y	Y	
Accounting Start received	Y	Y	Accounting Start Count
Accounting Stop sent	Y	Y	
Accounting Stop received	Y	Y	Accounting Stop Count
Accounting Stop received for unknown reason	Y	Y	
Accounting On sent	Y	Y	
Accounting On received	Y	Y	
Accounting Off sent	Y	Y	
Accounting Off received	Y	Y	
Accounting Response sent	Y	Y	Accounting Response Count
Accounting Response received	Y	Y	
Duplicates detected	Y	Y	Duplicated Message Count
Unknown/Unsupported messages received	Y	Y	
Interim Update Received	Y	Y	Accounting Update Count
Interim Update Received for unknown reason	Y	Y	

Display	MPE	MRA	Name
Currently active sessions	Y	Y	
Max active sessions	Y	Y	
Messages with Authenticator field mismatch	Y	Y	
Last RADIUS message received time	Y	Y	
COA-request sent	Y	Y	CoA Request Count
COA-request received	Y	Y	
COA-ACK sent	Y	Y	CoA Ack Count
COA-ACK received	Y	Y	CoA Success Count
COA-NAK sent	Y	Y	
COA-NAK received	Y	Y	CoA Nck Count
Parsed under 100m(icro)s	Y	Y	
Parsed under 200m(icro)s	Y	Y	
Parsed under 500m(icro)s	Y	Y	
Parsed under 1m(illi)s	Y	Y	
Parsed over 1m(illi)s	Y	Y	
Total Parse Time	Y	Y	
Average Parse Time	Y	Y	
Maximum Parse Time	Y	Y	
Unknown BNG. Message dropped	Y	Y	Unknown Gateway Request Count
Unknown BNG. Account Start dropped	Y	Y	
Unknown BNG. Account Stop dropped	Y	Y	
Unknown BNG. Interim Update dropped	Y	Y	
Stale sessions deleted	Y	Y	
Stale sessions deleted due to missed Interim Update	Y	Y	
Stale sessions deleted on Account-On or Account-Off	Y	Y	
Invalid subscriber key. Message dropped	Y	Y	

Display	MPE	MRA	Name
Invalid subscriber identifier specified. Message dropped	Y	Y	Unknown Subscriber Request Count

Table 30: Diameter Latency Statistics shows information for these Diameter Statistics:

- Application Function (AF)
- Policy and Charging Enforcement Function (PCEF)
- Bearer Binding and Event Reporting (BBERF)
- Traffic Detection Function (TDF)
- Diameter Sh protocol
- Distributed Routing and Management Application (DRMA)
- Diameter Sy protocol

Table 30: Diameter Latency Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Active Connection Count
Max Processing Time recd/sent (ms)	Y	Y	Max Trans In Time\ Max Trans Out Time
Avg Processing Time recd/sent (ms)	Y	Y	Avg Trans In Time\ Avg Trans Out Time
Processing Time recd/sent <time frame> (ms)	Y	Y	Processing Time [0-20] ms Processing Time [20-40] ms Processing Time [40-60] ms Processing Time [60-80] ms Processing Time [80-100] ms Processing Time [100-120] ms Processing Time [120-140] ms Processing Time [140-160] ms Processing Time [160-180] ms Processing Time [180-200] ms Processing Time [>200] ms

Table 31: Diameter Event Trigger Statistics

Display	MPE	MRA	Name
Diameter Event Trigger Stats by Code	Y	N	
Diameter Event Trigger Stats by Application:			

Display	MPE	MRA	Name
Diameter PCEF Application Event Trigger	Y	N	
Diameter BBERF Application Event Trigger	Y	N	

Table 32: Diameter Protocol Error Statistics

Display	MPE	MRA	Name
Total errors received	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error received	Y	Y	Last Error In Time
Last time for total error sent	Y	Y	Last Error Out Time
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 33: Diameter Connection Error Statistics

Display	MPE	MRA	Name
Total errors received	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error received	Y	Y	Last Error In Time
Last time for total error sent	Y	Y	Last Error Out Time
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 34: LDAP Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time

Display	MPE	MRA	Name
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time
Number of successful updates	Y	N	Update Hit Count
Number of unsuccessful updates	Y	N	Update Miss Count
Number of updates that failed because of errors	Y	N	Update Err Count
Time spent on successful updates (ms)	Y	N	Update Total Hit Time
Time spent on unsuccessful updates (ms)	Y	N	Update Total Miss Time
Max Time spent on successful update (ms)	Y	N	Update Max Hit Time
Max Time spent on unsuccessful update (ms)	Y	N	Update Max Miss Time
Average time spent on successful update (ms)	Y	N	Update Avg Hit Time
Average time spent on unsuccessful updates (ms)	Y	N	Update Avg Miss Time

Table 35: Sh Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Number of search errors that triggered the retry	Y	N	
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time
Number of successful updates	Y	N	Update Hit Count
Number of unsuccessful updates	Y	N	Update Miss Count

Display	MPE	MRA	Name
Number of updates that failed because of errors	Y	N	Update Err Count
Number of update errors that triggered the retry	Y	N	
Time spent on successful updates (ms)	Y	N	Update Total Hit Time
Time spent on unsuccessful updates (ms)	Y	N	Update Total Miss Time
Max Time spent on successful update (ms)	Y	N	Update Max Hit Time
Max Time spent on unsuccessful update (ms)	Y	N	Update Max Miss Time
Average time spent on successful updates (ms)	Y	N	Update Avg Hit Time
Average time spent on unsuccessful updates (ms)	Y	N	Update Avg Miss Time
Number of successful subscriptions	Y	N	Subscription Hit Count
Number of unsuccessful subscriptions	Y	N	Subscription Miss Count
Number of subscriptions that failed because of errors	Y	N	Subscription Err Count
Number of subscription errors that triggered the retry	Y	N	
Time spent on successful subscriptions (ms)	Y	N	Subscription Total Hit Time
Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Total Miss Time
Max Time spent on successful subscriptions (ms)	Y	N	Subscription Max Hit Time
Max Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Max Miss Time
Average time spent on successful subscriptions (ms)	Y	N	Subscription Avg Hit Time
Average time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Avg Miss Time
Number of successful unsubscriptions	Y	N	Unsubscription Hit Count

Display	MPE	MRA	Name
Number of unsuccessful unsubscriptions	Y	N	Unsubscription Miss Count
Number of unsubscriptions that failed because of errors	Y	N	Unsubscription Err Count
Number of unsubscription errors that triggered the retry	Y	N	
Time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Total Hit Time
Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Total Miss Time
Max Time spent on successful unsubscription (ms)	Y	N	Unsubscription Max Hit Time
Max Time spent on unsuccessful unsubscription (ms)	Y	N	Unsubscription Max Miss Time
Average time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Avg Hit Time
Average time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Avg Miss Time

Table 36: Sy Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time

Table 37: KPI Interval Statistics

Display	MPE	MRA	Name
Interval Start Time	Y	Y	Interval Start Time

Display	MPE	MRA	Name
Configured Length (Seconds)	Y	Y	Configured Length (Seconds)
Actual Length (Seconds)	Y	Y	Actual Length (Seconds)
Is Complete	Y	Y	Is Complete
Interval MaxTransactions Per Second	Y	Y	Interval Max Transactions Per Second
Interval MaxMRABinding Count	Y	Y	Interval Max MRABinding Count
Interval MaxSessionCount	Y	Y	Interval Max Session Count
Interval MaxPDNConnectionCount	Y	Y	Interval Max PDNConnection Count

About Color Threshold Configuration

The **KPI Dashboard Configuration** dialog appears when you click the **Change Thresholds** button located in the top right corner of the KPI Dashboard.

The dialog shows the current settings for the specified parameters. You can modify the values and click **Save** to put the new values into effect. The values are saved so the next time the dashboard is opened it uses the new values.

Note: Saving the thresholds affects other users that may be viewing the dashboard at the same time.

Cancel	Closes the dialog without any changes to the KPI dashboard display.
Reset	Restores the values to their defaults. The TPS and Session limits for the Policy Management device are set to the officially supported rates for the current software release.

Subscriber Activity Log

The CMP system can perform real-time tracing of Gx, Rx, SOAP, TCP provisioning, and Sh protocol messages for a subscriber from multiple MPE devices.

Subscriber tracing is activated using a global CMP configuration setting (see [Configuring the Activity Log](#)). After activation, traces for subscriber diameter application messages are merged from all MPE devices in the network to the CMP system. Messages are selected for tracing based on a subscriber identification. Allowable subscriber ID types are:

- IMSI
- MSISDN_E.164
- NAI
- UE IPv4/IPv6 address
- Session ID

Up to 100 subscriber IDs can be configured in the subscriber configuration window. Up to 20 subscribers can be enabled for tracing.

Note: Tracing subscriber activity affects performance.

After activating subscriber tracing, you can perform the following tasks using the **Subscriber Activity Log** option under **System Wide Reports**:

- View the subscriber activity log.
- Modify subscriber activity log settings. This task includes adding subscribers for tracing.
- View and modify the log backup settings.
- View the real-time subscriber activity log data display window.
- View the subscriber activity log history.

Subscriber Activity Log Limitations

The Subscriber Activity Log has the following limitations:

- Because of the additional processing required for the Subscriber Activity Log, only 20 subscribers can be enabled for logging, and only 10 subscribers can be viewed.
- There is also a limit to the overall amount of data that can be recorded by the system.
- Most MRA messages are not shown in the log because MRA messages do not have user IDs or bindings for a secondary session and cannot be traced.
- CCR-U is rejected by Diameter validation as an invalid message. There is no correlation between the established session and this message.
- For UDR/UDA and CCA-T, use NAI, E164, or IMSI , not Ipv4 or Ipv6.

Viewing a Subscriber Activity Log

To view the activity of a subscriber:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log** page opens.
2. If there are no subscribers in the **Subscriber Identifier List**, add one or more subscribers. See [Adding Subscriber Identifiers](#) for information on adding subscribers.
3. In the **Subscriber Identifier List** section, click **View** for a subscriber. The log for the subscriber opens.

The workspace displays the trace data in real time for the selected subscriber.

The **Trace Time** field shows the start time of the real-time data trace. The **End Time** field shows the day and time when the log is set to stop. The **Description** field shows the first 50 characters of the description for the Subscriber Identifier. The full description displays in the real-time page view.

You can perform the following actions in this window:

- Select a specific time in the **Time Index** list to display messages that appear during a specific time period.
- Select a message type from the **Activity Type** list to filter messages in the window by message type. The message types are:
 - All (default)
 - Gx
 - Rx
 - GxLite

- Gxx
 - Gy
 - Sd
 - Sh
 - Sy
 - LDAP
 - Policy
 - MDF Provisioning
 - SPR Provisioning
 - MGW Provisioning
- Select to enable or disable the **Automatic Scroll**. When enabled, the output scrolls in the window. When disabled, the window does not scroll, and new messages are added at the bottom of the window.
 - Click **Pause** to temporarily keep messages from being added to the window. If selected, the button changes to **Resume**. Click **Resume** for new real-time data to be added to the window.
- Note:** If the day and time in the **End Time** setting is in the past, then clicking **Resume** displays a message directing you to change the **End Time** setting.
- Click **Export** to export the currently displayed trace logs to a text file.

Configuring Subscriber Activity Logs

To configure subscriber activity logs:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens.
2. Click **Modify**.
A new **Subscriber Activity Log Settings** page opens, containing fields for configuring the log.
3. In the **Configuration** section, configure the following information:
 - a) **Trace Enable**—When selected, warning level trace logs are generated for errors that occur during subscriber activity processing.
 - b) **Include MRA**—When selected, the system will check the MRA devices in subscriber tracing checks and include them in the warning level trace logs.
 - c) **Severity**—Select the level of messages written to the log: **INFO** (default), **NOTIFY**, or **DEBUG**.
 - d) **Activity Type**—Select the types of information to include in the log. The types available are **Protocol** and **Policy**. By default, all activity types are selected.



Note: To reduce the volume of logging and improve performance, select the activity types to narrow the focus of the log.
4. Add subscriber identifiers. See [Adding Subscriber Identifiers](#) for more information.
5. Configure the backup settings for the log. See [Configuring Subscriber Activity Log Backup Settings](#) for more information.
6. Click **Save**.



You have defined and saved the Subscriber Activity Log configuration.

Adding Subscriber Identifiers

Before adding subscribers, configure the Subscriber Activity Log. See [Configuring Subscriber Activity Logs](#).

To add subscriber identifiers to the activity log:




1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens.
2. Select the **Configuration** tab.
3. Click **Modify**.
The **Subscriber Activity Log** page opens, containing fields for configuring the log.
4. To add subscribers to the log in the **Subscriber Identifier List**:
 - a) Click **Add**.
The **Add Subscriber Identifier** window opens.
 - b) Select the type of identifier and enter the subscriber identifier:
 - **IMSI** (default) — International Mobile Subscriber Identity. Enter up to 15 Unicode digits.
 - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
 - **NAI** — Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters `&*+0-9?a-z_A-Z{}!#$%'^/= `| ~-`, optionally separated by a period (.). A valid realm name consists of the characters `0-9a-zA-Z-` separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
 - **IPv4Address** — An IPv4 address in the standard dot format.
 - **IPv6Address** — An IPv6 address, in the standard 8-part colon-separated hexadecimal string format, and the subnet mask in CIDR notation from 0–128.
 - **SessionID** — A valid session ID. A valid session ID consists of the characters `&*+0-9?a-z_A-Z{}!#$%'^/= `| ~-`.
5. To select a date and time to stop tracing:
 - a) Click  to open the **Select Date** window.
 - b) Select a date on the calendar.
 - c) Enter a time using the format *hh:mm*. Valid values for *hh* are 00 to 23. Valid values for *mm* are 00 to 59.
6. Select **Enable** to start the trace for the subscriber ID.
7. (Optional) Enter a description about the trace for this subscriber. Enter up to 1000 characters.
Note: Only the first 50 characters appear in the list view.
8. Click **Save**.
9. (Optional) Add, edit, or delete subscribers.
 - Cloning an entry in the table
 1. Select an entry in the table.
 2. Click  **Clone**. The **Clone** window opens with the information for the entry.
 3. Make changes as required.

4. Click **Save**. The entry is added to the table
- Editing an entry in the table
 1. Select the entry in the table.
 2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.
 3. Make changes as required.
 4. Click **Save**. The entry is updated in the table.
 - Deleting a value from the table
 1. Select the entry in the table.
 2. Click  **Delete**. A confirmation message displays.
 3. Click **Delete** to remove the entry. The entry is removed from the table.

10. Click **Save**.

The Subscriber Identifier List is populated with the defined subscribers. You have defined and saved the subscribers in the **Subscriber Identifier List**. The **Subscriber Identifier List** displays the information configured for the subscriber identifier and the status of that subscriber.


Table 38: Status and Related Icons

Status	Icon	Condition
Running		Indicates the log is currently active (running). This status occurs when: <ul style="list-style-type: none"> • The End Time has not been reached or has just turned null. • Enable is selected.
Disabled		Indicates the log is not active. This status occurs when Enable is not selected and the End Time has not been reached.
Expired		Indicates the log is no longer active. This status occurs when the End Time is reached.

Configuring Subscriber Activity Log Backup Settings

To configure the subscriber activity logs backup settings:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens.
2. Select the **Log Backup Settings** tab.
3. Click **Modify**.
The **Configuration** page opens.

4. Configure the log backup settings:
 - a) Select **Enabled Subscriber Activity log Backup** to create a backup of the log.
 - b) In the **First Running Time** field, enter a date and time to start the backup in the format *mm/dd/yyyy hh:mm* (for example, **01/01/2015 12:15**).
Note: The date must be in the future.
 Alternatively, click  (calendar) and select a date and click **Enter**.
 - c) In **Run Interval(hours)**, set the time between backup runs. Valid values are from 1 to 99,999. The default is 24 hours.
 - d) In **Max Keep Days**, set the maximum number of day to keep the log. Valid values are from 1 to 60. The default is 60 days.
 - e) In **Folder Max Size(MB)**, set the maximum size of the backup storage folder. The default is 16000 MB.

Backup Destination Folder indicates the storage location for the backup files (for example, */var/camiant/subtracing*).

5. Click **Save**.

You have configured the Subscriber Activity Log backup settings.

Editing a Subscriber Identifier

To edit a subscriber identifier:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens.
2. Click **Modify**.
A new **Subscriber Activity Log Settings** page opens, containing fields for configuring the log.
3. In the **Subscriber Identifier List** section, select a subscriber and identifier and click **Edit**. The **Edit Subscriber Identifier** window opens.
4. Edit the identifier.
5. Click **Save**.

You have edited a subscriber identifier.

Deleting a Subscriber Identifier from the Activity Log

To delete one or more subscriber identifiers from the Activity Log:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens.
2. Click **Modify**.
A new **Subscriber Activity Log Settings** page opens, containing fields for configuring the log.
3. In the **Subscriber Identifier List** section, select a subscriber. Press the Ctrl or Shift key to select multiple subscribers. Click **Delete**.
A confirmation message displays.
4. Click **Delete** to delete the subscriber identifiers.
The subscriber identifier or identifiers are removed from the list.

You have deleted one or more subscriber identifiers.

Viewing Subscriber Activity Log History

To view the activity log history for subscribers:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens in the work area.
2. Click **Activity Log History**. The **Subscriber Activity Log History Log** window opens, displaying the activity log.
3. Filter the display by using one or more of the following criteria and clicking **Filter**:

- Start Date

Note: If the trace start date and end date are both entered, then the window displays the logs that occur between the two time points.

- End Date
- Identifier Type
- Identifier Value
- Activity Type
- Server
- Contains Text

A filtered view of the history displays.

From the log window you can optionally do the following:

- Click a message summary to display the content for the selected message in the bottom pane of the window.
- Click **Reset** to reset the filter conditions to their defaults. The log is refreshed to show all messages.
- Click **Export** to export the filtered trace logs data into a text file. The traced messages are exported in descending order according to the time stamp.

Viewing the Trending Reports

To view the trending reports, from the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

The navigation pane displays the four trending reports. The reports display separate aggregate MPE and MRA statistics in graph tables.

The trending report columns display the following data:

- **MRA Binding Count** — The number of bindings (for example, UE or Policy rules and charge function MPE pairs) which are maintained in the MRA system.

Note: A binding is the MPA routing information. The UE stores the user identity UE NAI, UE IP addresses, the selected MPE identity IP-CAN session, and APN if it is available.

- **PDN Connection Count** — The number of PDN connections that communicate to the Diameter network elements.
- **Session Count** — The number of Diameter sessions (for example, Gx or Gy) which are maintained in the MPE device.

- **Transaction Per Second** — The number of Diameter requests and answer pairs processed in a second.


Viewing MRA Binding Count

The MRA binding count determines the number of MRA bindings between user equipment (UE) and MPE devices maintained in the MRA system. This is recorded by the counter MaxMRABindingCount.

To view the MRA Binding Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
The content tree displays a list of trending reports.
2. From the content tree, select **MRA Binding Count**.
The **MRA Binding Count** page displays the MRA Binding Count graph.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph.
- **Search Filter** — You can specify which MRA devices are graphed (all or specific devices) and which counters to graph (all or binding counts for MRA devices, which for this report is the same thing). You can also specify the graph parameters:
 - **Start Date & Time** — The start date and time for the graph. Click  (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
 - **Duration** — Displays the time duration of the data. A list provides the following options:
 - **24 hours** (default)
 - **2 days**
 - **3 days**
 - **4 days**
 - **5 days**
 - **6 days**
 - **7 days**
 - **Show Aggregation** — If you check this box, the aggregated data for all MRA devices is displayed in the graph.
- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_MRA Binding Count.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.


Viewing PDN Connection Count

This report plots the counter Interval MaxPDNConnectionCount for each managed MPE and MRA device.

To view the PDN Connection Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
The content tree displays a list of trending reports.
2. From the content tree, select **PDN Connection Count**.
The **PDN Connection Count** page displays the PDN Connection Count MRA and policy server (MPE device) graphs.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph table.
- **Search Filter** — You can specify which MPE and MRA devices are graphed (all or specific devices) and which counters to graph (all, PDN connections for MPE devices, or PDN connections for MRA devices). You can also specify the graph parameters:
 - **Start Date & Time** — The start date and time for the graph. Click  (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
 - **Duration** — Displays the time duration of the data. A list provides the following options:
 - 24 hours (default)
 - 2 days
 - 3 days
 - 4 days
 - 5 days
 - 6 days
 - 7 days
 - **Show Aggregation** — If you check this box, the aggregated data for all selected MPE or MRA content is displayed in the graph.
- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_PDN Connection Count.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing Session Count


The session counts determine the number of Gx or Gy sessions maintained in the MPE device, graphed over time periods equal to the KPI interval length (by default 15 minutes). The session count is recorded by the counter `MaxSessionCount`.

To view the Session Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
The content tree displays a list of trending reports.
2. From the content tree, select **Session Count**.
The **Session Count** page displays the Session Count for policy server (MPE) device graph.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph.

- **Search Filter** — You can specify which MPE devices are graphed (all or specific devices) and which counters to graph (all or session counters for MPE devices, which for this report is the same thing). You can also specify the graph parameters:
 - **Start Date & Time** — The start date and time for the graph. Click  (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
 - **Duration** — Displays the time duration of the data. A list provides the following options:
 - 24 hours (default)
 - 2 days
 - 3 days
 - 4 days
 - 5 days
 - 6 days
 - 7 days
- Note:** The durations available depend on the settings of the OM Statistics scheduled task.
- **Show Aggregation** — If you check this box, the aggregated data of all selected MPE content is displayed in the graph.
 - **Settings** — The table parameters are displayed; click **Run** to generate the graph.
 - **Printable Format** — The most recently updated graph is displayed in a separate window.
 - **View Raw Data** — The interval data statistics are displayed in a separate window.
 - **Export CSV** — A comma-separated value (CSV) file named `Export_Session_Count.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
 - **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.


Viewing Transaction Per Second

Transactions per second is defined as the number of Diameter request or Diameter answer pairs processed in a second, graphed over time periods equal to the KPI interval length (by default 15 minutes). Transactions are recorded by the counter `MaxTransactionsPerSecond`.

To view the Transaction Per Second trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**. The content tree displays a list of trending reports.
2. From the content tree, select **Transaction Per Second**. The **Transaction Per Second** page displays the Transaction Per Second graph.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph.
- **Search Filter** — You can specify which Policy Management devices are graphed (all or specific devices) and which counters to graph (all or TPS for each class of Policy Management device). You can also specify the graph parameters:
 - **Start Date & Time** — The start date and time for the graph. Click  (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
 - **Duration** — Displays the time duration of the data. A list provides the following options:

- **24 hours** (default)
- **2 days**
- **3 days**
- **4 days**
- **5 days**
- **6 days**
- **7 days**
- **Show Aggregation** — If you check this box, the aggregated data for all selected devices is displayed in the graph.
- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_Transaction Per Second.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Custom Trending Reports

Along with the four pre-configured trending reports, you can create custom trending reports based on one or more counters.

The following statistics are associated with the MPE server type:

- AFRatTypeStats
- DiameterAfLatencyStats
- DiameterBberfLatencyStats
- DiameterBberfStats
- DiameterCTFStats
- DiameterDrmaLatencyStats
- DiameterDrmaStats
- DiameterPcefLatencyStats
- DiameterPcefStats
- DiameterShLatencyStats
- DiameterShStats
- DiameterSyLatencyStats
- DiameterSyStats
- DiameterTdfLatencyStats
- DiameterTdfStats
- IntervalStats
- KpiStats
- PDNConnectionAPNStats
- PdnRatTypeStats
- PolicyStats

The following statistics are associated with the MRA server type:

- DiameterMraAfLatencyStats
- DiameterMraAfStats
- DiameterMraBberfLatencyStats
- DiameterMraBberfStats
- DiameterMraCtfStats
- DiameterMraDraStats
- DiameterMraDrmaLatencyStats
- DiameterMraDrmaStats
- DiameterMraPcefLatencyStats
- DiameterMraPcefStats
- DiameterMraTdfLatencyStats
- DiameterMraTdfStats
- IntervalMraStats
- KpiMraStats

After creation, customized trending reports appear in the **Trending Reports** list following the pre-configured Trending Reports in alphabetical order.

Creating a Custom Trending Report

To create a custom trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**. The **Trending Report Definition Administration** page opens.
2. Click **Create Trending Report Definition**.
A new **Trending Report Definition Administration** page opens, containing fields for configuring a customized trending report.

See [Figure 33: Trending Report Definition Configuration Page](#) shows a sample.

Figure 33: Trending Report Definition Configuration Page

3. Enter the following information for the new trending report:
 - a) **Name** — The name of the trending report.

The name can contain up to 255 characters, cannot contain double quotes or commas, and cannot begin or end with a space.


- b) **Y-title** — The title of the Y series.

The title can contain up to 40 characters and cannot begin or end with a space.

- c) **Description** — The description of the trending report.

The description can contain up to 250 characters and cannot begin or end with a space.

4. Add counters to the report:

- a) Click  **Add** next to the **Counters Setting** field.

The **Add Stats Definition** popup opens.

- b) Enter a name for the counter in the **Name** field.

The name can contain up to 40 characters, cannot contain double quotes (") or commas (,), and cannot begin or end with a space.

- c) Select the server type from the **Server Type** list.

- d) Select a statistic from the **Statistic Name** list.

After selecting a statistic, all counters supported by that statistic populate the **Counter Name** list.

- e) Select a counter from the **Counter Name** list.


- f) Click **Save** to add the counter to the **Counters Setting** list.

You have added a single counter to the trending report. You can continue to add individual counters to the report, using this step. You can also add counters by cloning an existing counter (described in the following step).

5. (Optional) Add, edit, or delete reports.

- Cloning an entry in the table

1. Select an entry in the table.


2. Click  **Clone**. The **Clone** window opens with the information for the entry.

3. Make changes as required.

4. Click **Save**. The entry is added to the table

- Editing an entry in the table

1. Select the entry in the table.


2. Click  **Edit**. The **Edit Response** window opens, displaying the information for the entry.

3. Make changes as required.

4. Click **Save**. The entry is updated in the table.

- Deleting a value from the table

1. Select the entry in the table.

2. Click  **Delete**. A confirmation message displays.

3. Click **Delete** to remove the entry. The entry is removed from the table.

6. Click **Save**.

You have defined and saved a custom trending report. The custom trending report appears, in alphabetical order by name, in the list of custom trending reports.

Editing a Custom Trending Report

You can edit any of the configured information for an existing custom trending report. You can also add, edit, or delete the counters associated with the report.

To edit a custom trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
The **Trending Report Definition Administration** page opens.
2. Select the custom trending report.
The report opens.
3. Click **Settings**.
The **Trending Report Definition Administration** page displays for the report.
4. Click **Modify**.
You can edit the **Name**, **Y-Title**, or **Description** of the report. You can also add, edit, or delete the counters associated with the report. See [Creating a Custom Trending Report](#) for additional information.

Deleting a Custom Trending Report

You can delete any of the existing custom trending reports. You cannot delete the pre-configured trending reports.

To delete a custom trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
The **Trending Report Definition Administration** page opens.
2. Select the custom trending report.
The report opens.
3. Click **Settings**.
The **Trending Report Definition Administration** page displays for the report.
4. Click **Delete**.
A confirmation message displays.
5. Click **OK**.

You have deleted the report.

Viewing Alarms

To view alarms or the alarms history:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.
2. Select the report to view.

The navigation pane displays the available alarms reports.

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:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.
The **Alarms** section expands to show the available alarm reports.
2. Select **Active Alarms**.
The **Active Alarms** report opens in the work area.

Figure 34: Sample Active Alarms Report shows a sample active alarm report.

Active Alarms (Stats Reset: Manual / Last Refresh: 04/15/2014 11:47:01)

Display results per page: 50

[First/Prev] 1 [Next/Last] Total 1 pages




Server	Server Type	Severity	Alarm ID	Age/Auto Clear	Description	Time	Operation
cmp16-171 10.15.16.171	CMP	Minor	32508	14h 14m 4s / ---	Server Core File Detected	04/14/2014 21:32:50 EDT	
mpe16-172 10.15.16.172	CMP	Minor	32508	13h 52m 33s / ---	Server Core File Detected	04/14/2014 21:54:22 EDT	
mra16-197 10.15.16.197	MRA	Minor	32508	13h 17m 6s / ---	Server Core File Detected	04/14/2014 22:29:48 EDT	

Figure 34: 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 yellow.)

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**, **MRA**, 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.
- To save your formatting changes to the report page, click **Save Layout**.
- **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 **Alarms**.
The **Alarms** section expands to show the available alarm reports.
2. 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.

3. 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.)
4. After entering filtering information, click **Filter** to refresh the display with the filtering applied. The alarm list is filtered.
 5. Click **Close**.

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 yellow).
 - **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 or IPv6 format.
- **Server** — Name and IP address, in IPv4 or IPv6 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:

Date/Time	Sep 29, 2013 12:56 AM EDT
Severity	Info
Text	CMP User login.
Count	41
First Occurrence	Sep 28, 2013 10:44 PM EDT
Last Occurrence	Oct 01, 2013 02:24 PM EDT
Server	cmp200,10.60.30.200
Details	CMP - successful login of user {0}

Figure 35: Alert Details

Viewing Session Reports

To view the session reports, from the **System Wide Reports** section of the navigation pane, select **Sessions**.

The navigation pane displays the available session reports.

Viewing the AF Session Report

The application function (AF) session report shows information on the current and maximum number of AF sessions for each specific radio access technology type (RAT-Type) for each MPE device.

The following RAT-Types are supported:

- WLAN (0) — Wireless local area network
- VIRTUAL (1) — Virtual network
- UTRAN (1000) — Universal Terrestrial Radio Access Network
- GERAN (1001) — GSM EDGE Radio Access Network
- GAN (1002) — Generic Access Network
- HSPA_EVOLUTION (1003) — High Speed Packet Access Evolution
- EUTRAN (1004) — Evolved UTRAN
- CDMA2000_1x (2000)
- HRPD (2001) — High Rate Packet Data
- UMB (2002) — Ultra Mobile Broadband
- EHRPD (2003) — Enhanced HRPD

To view the AF session report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **AF Session Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **Associated MRA** — The MRA device managing this device, or N/A if no MRA device is managing this device. (If your CMP system is not configured to manage MRA devices, this option is not available.)
- **Server Name** — The name defined for the server.
- **Server Type** — Either **MPE** or **MRA**. All MPE devices managed by an MRA device are displayed together, followed by a row for that MRA device that represents the total counts for all MPE devices managed by that MRA device. Any MRA devices not managed by an MRA device are displayed after the last configured MRA device.
- **WLAN - Current** — The current number of WLAN connections to this device.

- **WLAN - Max** — The highest number of WLAN connections recorded to this device.
- **Virtual - Current** — The current number of Virtual connections to this device.
- **Virtual - Max** — The highest number of Virtual connections to this device.
- **UTRAN - Current** — The current number of UTRAN connections to this device.
- **UTRAN - Max** — The highest number of UTRAN connections recorded to this device.
- **GERAN - Current** — The current number of GERAN connections to this device.
- **GERAN - Max** — The highest number of GERAN connections recorded to this device.
- **GAN - Current** — The current number of GAN connections to this device.
- **GAN - Max** — The highest number of GAN connections recorded to this device.
- **HSPA_EVOLUTION - Current** — The current number of HSPA_EVOLUTION connections to this device.
- **HSPA_EVOLUTION - Max** — The highest number of HSPA_EVOLUTION connections recorded to this device.
- **EUTRAN - Current** — The current number of EUTRAN connections to this device.
- **EUTRAN - Max** — The highest number of EUTRAN connections recorded to this device.
- **CDMA2000_1X - Current** — The current number of CDMA2000_1X connections to this device.
- **CDMA2000_1X - Max** — The highest number of CDMA2000_1X connections recorded to this device.
- **HRPD - Current** — The current number of HRPD connections to this device.
- **HRPD - Max** — The highest number of HRPD connections recorded to this device.
- **UMB - Current** — The current number of UMB connections to this device.
- **UMB - Max** — The highest number of UMB connections recorded to this device.
- **EHRPD - Current** — The current number of EHRPD connections to this device.
- **EHRPD - Max** — The highest number of EHRPD connections recorded to this device.

The first row in the table displays the total for all configured MRA devices.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (default), server totals only, or one specific server.
- **Server Type** — Filter in all server types (default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA** — Filter in all MRA devices (default), totals only, or one specific MRA device. (If your CMP system is not configured to manage MRA devices, this option is not available.)

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; an **AF Session Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the PDN Connection Report

The PDN Connection Report shows information on the current and maximum number of packet data network (PDN) connections for each specific radio access technology type (RAT-Type) for each MPE device.

The following RAT-Types are supported:

- WLAN (0) — Wireless local area network
- UTRAN (1000) — Universal Terrestrial Radio Access Network
- GERAN (1001) — GSM EDGE Radio Access Network
- GAN (1002) — Generic Access Network
- HSPA_EVOLUTION (1003) — High Speed Packet Access Evolution
- EUTRAN (1004) — Evolved UTRAN
- CDMA2000_1x (2000)
- HRPD (2001) — High Rate Packet Data
- UMB (2002) — Ultra Mobile Broadband
- EHRPD (2003) — Enhanced HRPD
- UNKNOWN (-1)

To view the PDN Connection report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **PDN Connection Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **Associated MRA** — The MRA device managing this device, or N/A if no MRA device is managing this device. (If your CMP system is not configured to manage MRA devices, this option is not available.)
- **Server Name** — The name defined for the server.
- **Server Type** — Either **MPE** or **MRA**. All MPE devices managed by an MRA device are displayed together, followed by a row for that MRA device that represents the total counts for all MPE devices managed by that MRA device. Any MRA devices not managed by an MRA device are displayed after the last configured MRA device.
- **WLAN - Current** — The current number of WLAN connections to this device.
- **WLAN - Max** — The highest number of WLAN connections recorded to this device.
- **UTRAN - Current** — The current number of UTRAN connections to this device.
- **UTRAN - Max** — The highest number of UTRAN connections recorded to this device.
- **GERAN - Current** — The current number of GERAN connections to this device.
- **GERAN - Max** — The highest number of GERAN connections recorded to this device.
- **GAN - Current** — The current number of GAN connections to this device.
- **GAN - Max** — The highest number of GAN connections recorded to this device.

- **HSPA_EVOLUTION - Current** — The current number of HSPA_EVOLUTION connections to this device.
- **HSPA_EVOLUTION - Max** — The highest number of HSPA_EVOLUTION connections recorded to this device.
- **EUTRAN - Current** — The current number of EUTRAN connections to this device.
- **EUTRAN - Max** — The highest number of EUTRAN connections recorded to this device.
- **CDMA2000_1X - Current** — The current number of CDMA2000_1X connections to this device.
- **CDMA2000_1X - Max** — The highest number of CDMA2000_1X connections recorded to this device.
- **HRPD - Current** — The current number of HRPD connections to this device.
- **HRPD - Max** — The highest number of HRPD connections recorded to this device.
- **UMB - Current** — The current number of UMB connections to this device.
- **UMB - Max** — The highest number of UMB connections recorded to this device.
- **EHRPD - Current** — The current number of EHRPD connections to this device.
- **EHRPD - Max** — The highest number of EHRPD connections recorded to this device.
- **UNKNOWN - Current** — The current number of connections of unclassified type to this device.
- **UNKNOWN - Max** — The highest number of connections of unclassified type recorded to this device.

The first row in the table displays the total for all configured MRA devices.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (default), server totals only, or one specific server.
- **Server Type** — Filter in all server types (default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA** — Filter in all MRA devices (default), totals only, or one specific MRA device. (If your CMP system is not configured to manage MRA devices, this option is not available.)

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **PDN Connection Count Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the PDN APN Suffix Report

The PDN APN suffix report shows information on PDN connection counts per access point name (APN) suffix.

To view the PDN APN suffix report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **PDN APN Suffix Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **APN** — The access point name.
- **Server Name** — The server name.
- **Server Type** — Either **MPE** or **MRA**.
- **Current** — The current number of PDN connection counts for each suffix that have been matched on each server.
- **Max** — The highest number of PDN connection counts for each suffix that have been matched on each server.

The first row in the table displays the total values for all configured servers.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **APN** — Filter in all APN suffixes (default), all PDN connections without a configured APN suffix match (OtherAPNs), or APN suffix totals only.
- **Server Name** — Filter in all servers (default), server totals only, or one specific server.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **PDN APN Suffix Statistics Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing Other Reports

To view the miscellaneous reports:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select the report to view.

The navigation pane displays the available reports.

Viewing the Connection Status Report

The connection status report provides an aggregate view of connections maintained by managed Policy Management systems. The display is refreshed every ten seconds.

To view the connection status report.

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **Connection Status**

Figure 36: *Sample Connection Status Report* shows a sample connection status report.

Server	Server Type	Remote Identity	Type	Status	Up/Down Since	# Total Connect	# Active Connect	Msgs Sent	Msgs Received	Errors Sent	Errors Received
mpe17-79	MPE	mra17-38.camiant	Diameter AF	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter PCEF	normal	06/10/2013 10:34:03 EDT	15	1	872	872	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter SBC	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter TDF	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter CTF	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter CTF	Down	N/A	15	1	0	0	0	0

Figure 36: Sample Connection Status Report

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **Server** — name of the associated system
- **Server Type** — **MPE** (Multimedia Policy Engine) or **MRA** (Policy Front End)
- **Remote Identity** — the Diameter ID (if known) or IP address of the remote system
- **Type** — the type of connection
- **Status** — the status of the connection (the possible values are protocol-specific)
- **Up/Down Since** — the timestamp when the connection reached its current state (N/A if the connection has never been established)
- **# Total Connect** — the number of times that the connection has been re-established

Note: This counter is reset if the cluster is restarted.

- **# Active Connect** — the number of active connections

Note: This counter is reset if the cluster is restarted.

- **Msgs Sent** — the number of Diameter or RADIUS protocol messages that have been sent to the remote system
- **Msgs Received** — the number of protocol messages that have been received from the remote system
- **Errors Sent** — the number of protocol error messages that have been sent to the remote system
- **Errors Received** — the number of protocol error messages that have been received from the remote system

If a connection is in a non-functional state, the row is displayed in red; if a connection is in a transitional state between functional and non-functional (including when a connection is being established), the row is displayed in yellow.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server** — Filter in all servers (default) or one specific server.
- **Server Type** — Filter in all server types (default), totals only, MPE devices only, or MRA devices only.
- **Remote Identity** — Filter in all remote devices (default) or one specific device.
- **Type** — Filter in all remote device types (default) or one specific device type: **Diameter AF**, **Diameter PCEF**, **Diameter BBERF**, **Diameter TDF**, **Diameter SH**, **Diameter CTF**, or **Diameter DRMA**.
- **Status** — Filter in all remote device status values (default) or one specific status: **down**, **normal**, or **reopen**.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **Connection Status Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the Protocol Errors Report

The protocol errors report provides an aggregate view of connection errors, with one row for each distinct error code or sub-code. The display is refreshed every ten seconds.

To view the protocol errors report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **Protocol Errors**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The following columns are available:

- **Server** — Name of the associated system
- **Server Type** — **MPE** or **MRA**
- **Remote Identity** — The Diameter ID (if known) or IP address of the remote system
- **Error** — The protocol error
- **# Received** — The number of protocol errors received from the remote system
- **# Sent** — The number of protocol errors sent to the remote system

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server** — Filter in all servers (default) or one specific server.
- **Server Type** — Filter in all server types (default), totals only, MPE devices only, or MRA devices only.

- **Remote Identity** — Filter in all remote devices (default) or one specific device.
- **Error** — Filter in all remote error types (default) or one specific error type.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **Connection Status Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the Policy Statistics Report

The policy statistics report provides an aggregate view of policy statistics, with one row for each policy, letting you gauge the performance of individual policies. The display is refreshed every ten seconds.

To view the policy statistics report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
The list of available reports displays in the navigation pane.
2. Select **Policy Statistics Report**.
The Policy Statistics report opens.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The following columns are available:

- **Server Name** — Name of the associated system
- **Server Type** — Either **MPE** or **MRA**
- **Policy Name** — The name of each policy defined and active on the displayed server
- **Evaluated** — The number of times the displayed policy was evaluated for the displayed server
- **Executed** — The number of times the displayed policy was executed for the displayed server
- **Ignored** — The number of times the displayed policy was ignored by the displayed server
- **Total Execution Time (ms)** — The total execution time for each policy, in milliseconds
- **Average Execution Time (ms)** — The average amount of time it takes a policy to execute, in milliseconds
- **Maximum Execution Time (ms)** — The maximum execution time for each policy, in milliseconds

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (default) or one specific server.
- **Policy Name** — Filter in all policies (default) or one specific policy.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **Policy Statistics Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the MPE/MRA Replication Statistics Report

The MPE/MRA replication statistics report provides a view of database replication statistics, with one row for each replication path in an MPE or MRA cluster. The display is refreshed every ten seconds.

To view the replication statistics report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **MPE/MRA Rep Stats**.

Figure 37: Sample MPE/MRA Replication Statistics Report shows a sample replication report.

Cluster Name	Server Type	Cluster State	Blade State	Sync State	Replication Delta (Min/Sec)
mpe-43-56-57	MPE	OK	OK	OK	0:0.499
mpe-43-56-57 (Active) -> mpe-43-56-57 (Standby)	MPE	OK	OK	OK	0:0.499
mpe-43-56-57 (Active) -> mpe-43-56-57 (Standby)	MPE	OK	OK	OK	0:0.499
mra-43-58-59	MRA	OK	OK	OK	0:0.501
mra-43-58-59 (Active) -> mra-43-58-59 (Standby)	MRA	OK	OK	OK	0:0.501
mra-43-58-59 (Active) -> mra-43-58-59 (Standby)	MRA	OK	OK	OK	0:0.499

Figure 37: Sample MPE/MRA Replication Statistics Report

From the report page you can do the following:





- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To save the any formatting changes in the page, click **Save Layout**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The following columns are available:

- **Cluster Name** — The name of the cluster and the blades participating in replication as well as their high availability (HA) states.
- **Server Type** — The type of cluster being utilized (MPE or MRA).
- **Blade State** — Displays the state of the blade replicating with the current active blade.











Table 39: Blade State Values in MPE/MRA Replication Stats Report










Blade Ha State	Value Displayed in the Report	Icon Used in the User Interface
Standby	OK	Green check mark

Blade Ha State	Value Displayed in the Report	Icon Used in the User Interface
Spare	OK	 Green check mark
Forcelandby	Minor	 Warning Sign
Out of Service	Critical	 Red X
Unknown	Critical	 Red X

- **Sync State** — displays the values reported from COMCOL.


Table 40: Sync State Values in MPE/MRA Replication Stats Report




Sync Status	Description	Value Displayed on the CMP	Icon Used in the User Interface
Down	The link is down and there is no current attempt to restore it.	Critical	 Red X
DownListening	The incoming link is down awaiting the other side to initiate the connect attempt.	Critical	 Red X
DownConnecting	The link is down by this side is trying to connect.	Critical	 Red X
DownRejected	The link is down because a connect attempt was rejected in the handshake phase.	Critical	 Red X
DownHandshake	The link is connected but not ready for application use (so it is down logically). The links is being validated in a handshake as legitimate.	Critical	 Red X
Connected	Connected and ready for use.	Critical	 Red X
ConnectedReinit	Connected and ready for use, but after an application error where the recovery is start over without either a link drop or a complete application restart.	Critical	 Red X
ConnectedIncompat	Connected but the schema are incompatible and replication cannot run until (1) the schema has the needed upgrade information or (2) problematic tables are excluded from replication.	Critical	 Red X
RegisterSent	RegisterSent means the link is exchanging application level credentials and information (such as data dictionary information). In this state, registration has been sent from one side and it is being awaited from the other side.	Critical	 Red X
RegisterAcked	In this state, registration has been sent acknowledged from the other side. In most configurations, it is a	Critical	 Red X

Sync Status	Description	Value Displayed on the CMP	Icon Used in the User Interface
	transitory state, but the end application can hold the link in this state before permitting an audit.		
Standby	Standby means the high-availability state is standby, but the applications have exchanged registration messages.	Critical	 Red X
Inhibited	Inhibited means the link administrative state is inhibited (or disabled), but the applications have exchanged registration messages.	Major	 Red Exclamation Mark
AuditWait	The audit is awaiting an OK to proceed message from the remote side.	Critical	 Red X
AuditQueue	The audit is queued because a limit on the number of simultaneous audits.	Critical	 Red X
Audit	Audit means the application is bringing the databases into agreement. It does so by comparing each table one-by-one, and then applying database updates since the audit began.	Major	 Red Exclamation Mark
Active	Active means the link is in the normal active steady-state conditions where updates are being transferred to the slave databases with a normal and acceptable delay.	OK	 Green Check Mark
ActiveBehind	ActiveBehind is the same as Active but the slave database is unacceptably behind for whatever reasons. After an audit, it would be typical to be in the ActiveBehind state until any queued updates are applied to the slave database.	Major	 Red Exclamation Mark
ActiveSwitch	A switchover is being attempted without an audit if the states of the databases allow it.	Major	 Red Exclamation Mark
ActivePost Audit	The database is coherent but has not caught back up to current after the preceding audit.	Major	 Red Exclamation Mark

- **Cluster State** — represents the overall state of the cluster. The Cluster State Column is an aggregation of the Blade State and Sync State columns. The value for the Cluster State is selected based on the maximum severity.

Table 41: Priority Table in MPE/MRA Replication Stats Report

Priority	Value	Icon Used in the User Interface
1	Critical	 Red X

Priority	Value	Icon Used in the User Interface
2	Major	 Red Exclamation Mark
3	Minor	 Warning Sign
4	OK	 Green Check Mark

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **App Type**— Filter in all applications (default) or filter by **MPE** or **MRA**.
- **Server Name** — Filter in all servers (default) or one specific server.
- **Cluster Name** — Filter in all clusters (default) or one specific cluster.

You can display the report in a format suitable for printing. Click **Printable Format**. The **MPE/MRA Rep Status Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the SGW Failure Report

The SGW failure report provides a list of the last 10 AN-GWs that failed and the corresponding time stamps.

To view the failure report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **SGW Failure Reports**.
The **SGW Failure Reports** page opens.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To save the any formatting changes in the page, click **Save Layout**.
- To display another page of the report, click the page number.

You can customize the the table by controlling which columns appear, using the **Columns** list. The following columns are available:

- **SGW IP** — the IP address for the SGW.
- **Last Failure Time** — the UTC date and time the specified SGW failed.
- **Status** — the current status for the specified SGW (that is, up or down).

You can customize the information displayed by using the **Filter** list to display information by **SGW IP** address and by **Status**.

You can display the report in a format suitable for printing. Click **Printable Format**; an **SGW Failure Reports** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Chapter 16

Upgrade Manager

Topics:

- [*Overview of Upgrade Manager.....297*](#)
- [*Overview of Upgrade.....297*](#)
- [*About ISO Files on Servers.....297*](#)
- [*About Performing an Upgrade.....300*](#)
- [*Upgrade Manager Page Elements.....309*](#)
- [*About Rolling Back an Upgrade.....312*](#)
- [*ISO Maintenance Page Elements.....316*](#)

This chapter describes the function of the Upgrade Manager in the CMP system. For upgrade instructions, see the upgrade document for your release.

Overview of Upgrade Manager

The Upgrade Manager enables you to manage upgrade files, patch, or upgrade software on clusters in the Policy Management network, or roll back an upgrade. Upgrade or rollback automatically processes a multi-server cluster or georedundant site in the proper order to minimize data loss and downtime. During the process, the **Upgrade Manager** page displays progress information.

Access to the Upgrade Manager can be restricted by user role; see [About Managing Users](#) for more information.

For instructions on upgrading your systems, download the upgrade instructions for your release from the Oracle Help Center (see [Locate Product Documentation on the Oracle Help Center Site](#) for more information).

Overview of Upgrade

The main tasks for upgrading a Policy Management system are as follows:

1. Add the ISO files to the CMP server. This can be done either automatically using the CMP interface or manually.

Note: If you are installing a patch or patch set, you must use the manual process. See [Preparing to install a Patch or Patch Set](#)

2. Selecting the ISO file to use for the upgrade. See [Selecting an ISO for Upgrade](#)
3. Upgrade the CMP Sites.
 - a. If you are upgrading from release 11.5, see [Upgrading a Release 11.5 Primary-site CMP Cluster](#).
 - b. If you are upgrading from release 12.x, see [Upgrading a Primary-site CMP Cluster](#).
4. Upgrade the georedundant servers. See [Upgrading a Georedundant Cluster](#).

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. ISO files contain both upgraded software and files that direct the upgrade process. When upgrading the Policy Management software, you can automatically distribute the files using the CMP interface or manually distribute the ISO files to the servers and clusters.

When upgrading, use the **ISO Maintenance** page to show the current Policy Management software release executing on each server, and determine what ISO files are available to use for upgrades. Operations performed from this page include distributing ISO files, deleting ISO files, and pushing an upgrade script to servers. An audit log records each update operation.

Note: When patching the Policy Management software, do not use the **ISO Maintenance** page. You must manually distribute the ISO files to the CMP servers. See [Preparing to install a Patch or Patch Set](#) for more information.

Pushing a Script to the Servers (Upgrade From Release 11.5 Only)

Use this procedure to upgrade from release 11.5. Before starting this procedure, you must have mounted the ISO file manually and copied the following files to `/opt/camiant/bin` on the CMP system on which you are performing this procedure:

- `policyUpgrade.pl`
- `policyUpgradeHelper.pl`
- `qpSSHKeyProv.pl`
- `policySSHKey.pl`
- `lvm_reclam.pl`

Upgrades are controlled by a set of script files. Use this procedure to push upgrade scripts to the remote servers receiving a software upgrade. This procedure is required before a software upgrade can occur on a server.

To push a script to a server:

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page opens.
2. Select the servers receiving the upgrade script.
3. Click the **Operations** list and select **Push Script**.
A confirmation message opens.
4. Click **OK**.
A progress bar displays the progress of the operation.

The script is pushed to the servers.

Adding an ISO File to a Server

Use this procedure to load an upgrade ISO file onto a remote server for a software upgrade.

To add an ISO file to a server:

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page opens.
2. Select the clusters or servers to receive the ISO file.
3. Click the **Operations** list and select **Upload ISO**.
The **Upload ISO** window opens.
4. Enter the following information for the ISO file (all fields are required):
 - a) **Mode** — Mode used to transfer the ISO file to remote servers. Currently, SCP is available.
 - b) **ISO Server Hostname/IP** — Enter the name or address of the server receiving the ISO file.
 - c) **User** — Enter the root account user name.
 - d) **Password** — Enter the root account password.
 - e) **Source ISO file full path** — Enter the location where the ISO file is to be stored on the remote server.
5. Click **Add** (or **Back** to abandon your request).
The **Upload ISO** window closes, and 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. When the process completes, the icon disappears.

The ISO file is added to the servers.

Deleting ISO Files from the Servers

Before you start a new upgrade, it is recommended that any ISO file from past upgrades are removed from the servers.

To delete ISO files from the server:

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page opens.
2. Select the clusters or servers.
3. Select the ISO file to be removed.
4. Click the **Operations** list and select **Delete ISO**.
A confirmation message opens.
5. Click **OK**.
A progress bar displays the progress of this operation.

The ISO files are deleted from the servers.

Manually Adding ISO Files to the Servers

You must add the upgrade file to all servers in the Policy Management system before performing an upgrade. This procedure describes the how to manually add the ISO files to the servers. To add the ISO files using the CMP interface, see [Preparing for an Upgrade](#).

Note: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.



Caution: After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

If you are upgrading from release 11.5, use the procedure described in [Upgrading a Release 11.5 Primary-site CMP Cluster](#).

If you are installing a patch or patch set, use the procedure described in [Preparing to install a Patch or Patch Set](#).

To manually add the ISO files to the Servers:

1. Log in to the active server of the primary-site CMP cluster as **root**.
The system displays the root-level prompt (#).
2. Enter the command **rm -f /var/camiant/iso/***.
Any files in the directory are removed.
3. Enter the command **cp /var/TKLC/upgrade/* /var/camiant/iso**.
Upgrade files are copied to the target directory on the active server.

4. Enter the command **logout**.
You are logged out of the active server.

The servers now contain the ISO file and are ready for upgrading.

About Performing an Upgrade

The information in this section is a general overview of the Upgrade Manager and the steps you take to upgrade a cluster. Specific details are provided by My Oracle Support. See [My Oracle Support \(MOS\)](#) for more information.

When you upgrade a cluster, the Upgrade Manager uses upgrade scripts to automate the process wherever possible. The Upgrade Manager performs pre-upgrade checks, monitors and reports detailed progress of an upgrade, and prevents you from specifying invalid or unnecessary operations at each step in the process (by graying out invalid operations). You control an upgrade from the **Upgrade Manager** page. The Upgrade Manager automatically handles replication, synchronization, and the order in which servers are upgraded and failed over.

During the upgrade process, the Upgrade Manager reports on the progress of the upgrade on each server.

Though the upgrade process is automated, you retain control over actions that require operator approval. You can pause an upgrade at an operator action, resume the process later at your convenience, or roll back the upgrade from that point. You can also specify optional, advanced actions. (The Upgrade Manager prevents you from selecting invalid optional actions.)

During an upgrade, the Upgrade Manager asserts (that is, generates) and displays appropriate alarms, such as when servers go into forced standby, and clears the alarms when appropriate, such as when server upgrades are complete. The Upgrade Manager will also assert an alarm if an unexpected error prevents it from continuing the upgrade.

Note: An upgrade typically triggers minor, major, and critical alarms as servers are taken out of service or failed over. This is normal and to be expected.

In addition to recording all user and system upgrade activity in the audit log, the Upgrade Manager maintains a separate upgrade log so that you can track the history of an upgrade.

You must upgrade the CMP cluster (or, in a georedundant topology, the primary-site CMP cluster and then the secondary-site CMP cluster) before upgrading any other Policy Management systems.

You can upgrade up to four MPE or MRA clusters in parallel.

If you are upgrading a Policy Management release 11.5 network, the upgrade procedure for the CMP cluster, or the primary-site CMP cluster in a georedundant network, is different from the upgrade procedure for other clusters because you must use the Upgrade Manager for release 11.5 to install release 12.1. After the (primary-site) CMP server is running release 12.1 software, you can use the procedures described in the rest of this chapter to upgrade the remaining Policy Management systems (including, if present, a secondary-site CMP cluster).

Preparing for an Upgrade

You must add the upgrade file to all servers in the Policy Management system before performing an upgrade. This procedure describes the how to add the file to the servers using the user interface. To add the files manually see [Manually Adding ISO Files to the Servers](#).

Note: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.



Caution: After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

If you are upgrading from release 11.5, use the procedure described in [Upgrading a Release 11.5 Primary-site CMP Cluster](#).

If you are installing a patch or patch set, use the procedure described in [Preparing to install a Patch or Patch Set](#).

To prepare for an upgrade:

1. Use **Delete ISO** to remove any old upgrade files from all servers in the Policy Management network.
See [Deleting ISO Files from the Servers](#).
The servers are now ready for the new upgrade file.
2. Use **Upload ISO** to distribute the upgrade ISO file to all servers in the Policy Management network.
See [Adding an ISO File to a Server](#).
The servers are now ready for upgrade.

The servers now contain the upgrade package and are ready for upgrading.

Preparing to install a Patch or Patch Set

Patch software is available for electronic download on My Oracle Support. See the release notes for the patch to determine the servers that require the patch installation. If there is an order requirement, the Upgrade Director manages that process.

To prepare to install a patch or patch set:

1. Copy the ISO file to all CMP servers.
 - a) Empty the `/var/camiant/iso` directory on the server.
 - b) Use the secure copy command, `scp`, to copy the ISO file to the `/var/camiant/iso` directory.
2. Open the CMP interface.
3. View the active alarms.
Identify the cause of any existing active alarms, and determine if the alarms have an impact on the patch or patch set. Export the current alarms and save to a file.

Note: If there are alarms present that could impact the patch or patch set, it is recommended that you contact Oracle Consulting services prior to adding the patch.
4. View the KPI stats. Verify that the system is running within expected parameters and export current KPI stats to a file.

5. Check the checksum file:
 - a) Transfer the md5sum.out file to the /var/camiant/tmp directory.
 - b) Use the catenate command, cat, to see the value of the checksum.

For Example:

```
[root@CMP-JB-126 tmp]# cat md5sum.out
cca84e669c8db680f3264a93fe83aab7/home/build/build/PLATFORM-70/iso/patch-12.1.1.1.x.x.x.iso
[root@CMP-JB-126 tmp]#
```

- c) Verify that the checksum value is the same as the value in the md5sum.out file.

For example:

```
[root@CMP-JB-126 iso]# md5sum patch-12.1.1.1.x.x.x.iso
cca84e669c8db680f3264a93fe83aab7 patch-12.1.1.1.x.x.x.iso
[root@CMP-JB-126 iso]#
```

6. Using the CMP interface, select the ISO file containing the patch or patch set. See [Selecting an ISO for Upgrade](#).
7. Continue with [Upgrading a Primary-site CMP Cluster](#).

Selecting an ISO for Upgrade

You must distribute an ISO file beforehand to all servers that will use it (see [Adding an ISO File to a Server](#)). When the distribution is complete, you must select the ISO file to use in an upgrade before beginning the process. If you have multiple ISO files available for an upgrade (for example, if you have a major release and an update release, or an update release and a patch), you can select which one to use. If you have multiple clusters to upgrade, you only have to select the ISO file for the CMP system.

To select an ISO:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
The **Upgrade Manager** page appears.
2. Click on the name of the file listed as the current ISO (which may appear as **Install Kit**).
The **Select ISOs** window opens, listing the available ISO files.
3. (Optional) You can click on a column heading to sort the rows on that column. You can click **Filter** list to filter out rows based on the data in one or more columns. You can click the **Columns** list to select which columns are displayed (by default, all columns are displayed). You can resize columns.
4. Select which ISO file to use and click the **Select** button at the bottom of the window.
You are prompted: Loading this ISO will cause the upgrade manager to abandon the current upgrade and start a new one. Are you sure you want to continue loading this ISO?
5. Click **OK**.
The **Select ISOs** window closes, and the selected ISO file is listed as the current ISO.

The ISO is selected for upgrade. The data in the Up to date column changes from n/a to Y (which means that the server is running up-to-date software) or N (which means that the server needs upgrading).

Upgrading a Release 11.5 Primary-site CMP Cluster

Note: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.



Caution: After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

Before upgrading a release 11.5 primary-site CMP cluster:

1. Use **Delete ISO** to remove any old upgrade files from all servers in the Policy Management network.
See [Deleting ISO Files from the Servers](#).
2. Use **Upload ISO** to distribute the upgrade ISO file to all servers in the Policy Management network.
See [Adding an ISO File to a Server](#).

To upgrade the primary-site CMP cluster:

1. Log in to the active server of the primary-site CMP cluster as **root**.
The system displays the root-level prompt (#).
2. Enter the command `mount -o loop /var/TKLC/upgrade/iso_name /mnt/upgrade` (where *iso_name* is the name of the ISO file).
The ISO file is mounted.
3. Enter the command `cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`.
Script files are copied to the target directory on the active server.
4. Enter the command `umount /mnt/upgrade`.
The ISO file is unmounted.
5. Enter the command `qpSSHKeyProv.pl --prov`.
SSH keys for the account **admusr** are provisioned on the active server.

Note: This step is always required.

6. Enter the command `logout`.
You are logged out of the active server.
7. Log in to the active CMP server as an administrator with upgrade privileges.
You have access to the **Upgrade Manager** menu in the navigation pane.
8. From the **Upgrade Manager** section of the navigation pane, select **System Maintenance**.
The **System Maintenance** page opens.
9. Select all servers, and from the **Operations** list select **Push Script**.
You are prompted: Are you sure you want to execute Push Script?
10. Click **OK**.
Upgrade scripts are distributed to all servers.
11. Select the standby server of the **CMP Site1 Cluster**, and from the **Operations** list, select **Force Standby**.
You are prompted: Are you sure you want to execute Force Standby?
12. Click **OK**.
The server's state changes to **Force Standby**.

13. Select the forced standby server of the **CMP Site1 Cluster**, and from the **Operations** list, select **Start Upgrade**.
You are prompted: CAUTION! Please make sure the remote server is not being either Upgraded or Backed-out at this moment!
14. Click **OK**.
The server is upgraded, restarts, and rejoins the cluster.

Note: This process, which involves disk repartition, can take 40 minutes or more, depending on the amount of data on the server. Wait for the server to rejoin the cluster before proceeding.
15. Select the primary (**CMP Site1 Cluster**) site, and from the **Operations** list, select **Switch ForceStandby**.
You are prompted: Are you sure you want to execute Switch ForceStandby?
16. Click **OK**.
The forced standby server becomes the active server and the active server becomes forced standby. You are logged out of the CMP system.
17. Log in to the active (upgraded) CMP server as an administrator with upgrade privileges.
You have access to the **Upgrade** menu in the navigation pane.
18. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
The **Upgrade Manager** page opens.
19. Click the **Current ISO Install Kit**.
The **Select ISOs** window opens.
20. Select the release 12.1 ISO and click **Select ISO**.
You are prompted: Loading this ISO will cause the upgrade manager to abandon the current upgrade and start a new one. Are you sure you want to continue loading this ISO?
21. Click **OK**.
The ISO is selected for upgrade. The data in the **Up to date** column changes from **n/a** to **Y** (which means that the server is running up-to-date software) or **N** (which means that the server needs upgrading), and the alarms **SYSTEM_MIXED_VERSION** and **CLUSTER_MIXED_VERSION** are asserted.
22. Select the primary (**CMP Site1 Cluster**) site.
The **Continue Upgrade** button becomes available.
23. Click **Continue Upgrade**.
You are prompted: Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)
24. Click **OK**.
The remaining CMP system is upgraded. When the alarm **CLUSTER_MIXED_VERSION** is cleared, the upgrade is complete.

The primary-site CMP cluster is upgraded. You must now upgrade the secondary (Site2) CMP cluster, if present, using the release 12.1 Upgrade Manager as described in this chapter, before you can upgrade any other Policy Management clusters. When all the CMP clusters are upgraded, you can upgrade the remaining clusters of the Policy Management network.

Upgrading a Primary-site CMP Cluster

You must upgrade the primary-site CMP cluster first in any Policy Management topology. This procedure describes the normal upgrade process.

Note: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.



Caution: After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

If you are upgrading from release 11.5, use the procedure described in [Upgrading a Release 11.5 Primary-site CMP Cluster](#) instead of this one.

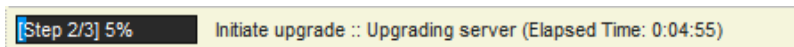
If you are installing a patch or patch set, use the procedure described in [Preparing to install a Patch or Patch Set](#).

If you are installing an upgrade to the current release, see [Preparing for an Upgrade](#) before starting this procedure.

To upgrade the primary-site CMP cluster:

1. Log in to the active CMP server as an administrator with upgrade privileges.
2. Click **Upgrade** in the navigation pane and then click **Upgrade Manager**.
The **Upgrade Manager** page opens.
3. Select an ISO file to use for the upgrade.
For more information, see [Selecting an ISO for Upgrade](#).
4. Select the primary CMP (Site1) cluster and click **Start Upgrade**.
You are prompted: Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)
5. Click **OK** to continue.

The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the standby server. The **Upgrade Operation** column displays the progress of the action; for example:



Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

When the standby server is upgraded, the **Upgrade Operation** column displays the message: Initiate upgrade Completed Successfully at *date_time*. and the following alarms are reported:

- 70500-System Mixed Version
- 70501-Cluster Mixed Version
- 70502-Cluster Replication Inhibited
- 70503-Server Forced Standby
- 70506-Upgrade Operation Failed
- 70507-Upgrade In Progress
- 70508-Server Is Zombie

Tip: Review alarms associated with each action before proceeding with the next action.

6. Log in to the active server of the primary-site CMP cluster as **root**.
The system displays the root-level prompt (#).
7. Enter the command `ls -l /var/camiant/iso` to verify that the correct CMP ISO is in the directory.
If the ISO is not present, enter the following commands:

```
rm -f /var/camiant/iso/*
cp /var/TKLC/upgrade/* /var/camiant/iso
```

 Upgrade files are copied to the target directory on the active server.
8. Enter the command `logout`.
You are logged out of the active server.
9. Log in to the active CMP server as an administrator with upgrade privileges.
You have access to the **Upgrade** menu in the navigation pane.
10. Select the cluster again and click **Continue Upgrade**.
You are prompted: Are you sure that you want to perform this action? Failover to new version *cluster_name* (next).
11. Click **OK** to continue.
If you stop an upgrade at a point of operator intervention, you can resume it later, or roll it back from there.
The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.
12. Select the cluster again and click **Continue Upgrade**.
You are prompted: Are you sure that you want to perform this action? Initiate upgrade *server_name* (next).
13. Click **OK**.
The remaining CMP server in the cluster is upgraded. When the Cluster Mixed Version alarm clears, the upgrade is complete.
Tip: You do not have to wait for the primary CMP cluster to be upgraded before beginning to upgrade the secondary CMP cluster.

The primary-site CMP cluster is upgraded. You must now upgrade the secondary (Site2) CMP cluster, if present, before you can upgrade any other Policy Management clusters. When all the CMP clusters are upgraded, you can upgrade the remaining clusters of the Policy Management network.

Upgrading a Georedundant Cluster

Before upgrading a cluster, see [Preparing for an Upgrade](#)

If you are adding a patch or patch set, see [Preparing to install a Patch or Patch Set](#).

If you are upgrading an entire Policy Management network, you must upgrade the primary-site CMP cluster first, then the secondary-site CMP cluster (if present).

The default, required sequence followed by the Upgrade Manager to upgrade a two-server cluster (including a CMP cluster) is as follows:

1. Upgrade the standby server.
2. Fail over to the standby server.
3. Reapply the configuration to the cluster.

4. Upgrade the remaining server.

The default, preferred sequence followed by the Upgrade Manager to upgrade a georedundant (three-server) cluster is as follows:

1. Upgrade the standby server.
2. Fail over to the standby server.
3. Reapply the configuration to the cluster.
4. Upgrade the remaining server in the primary site.
5. Upgrade the spare server.

An optional action lets you change this order if required. You can also upgrade the second and third server in the cluster simultaneously.

You can upgrade up to four MPE or MRA clusters in parallel. (This is the best practice.) You must manually start the process for each cluster.

You can roll back from an upgrade from any point of operator intervention. Whenever the action **Continue Upgrade** is available, the action **Start Rollback** is also available.



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. After you begin an upgrade, any changes to the configuration (such as creating or editing network elements or policies) may be lost.

To upgrade a georedundant cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
The **Upgrade Manager** page opens.
2. Select the cluster to be upgraded and click **Start Upgrade**.
You are prompted: Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)
3. Click **OK** to continue.
The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the standby server, in the primary site. The **Upgrade Operation** column displays the progress of the action; for example:

[Step 2/3] 5% Initiate upgrade :: Upgrading server (Elapsed Time: 0:04:55)

Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

When the standby server is upgraded, the **Upgrade Operation** column displays the message Initiate upgrade Completed Successfully at *date_time* and Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

Tip: Review alarms associated with each action before proceeding with the next action.

4. Select the cluster again and click **Continue Upgrade**.
You are prompted: Are you sure that you want to perform this action? Failover to new version *cluster_name* (next).
5. Click **OK** to continue.

If you stop an upgrade at a point of operator intervention, you can resume it later, or roll it back from there.

The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.

6. Reapply the configuration to the cluster:

- (For an MPE cluster) From the **Policy Server** section of the navigation pane, select **Configuration**, select the cluster, and in the **Policy Server Administration** page, click **Reapply Configuration**.
- (For an MRA cluster) From the **MRA** section of the navigation pane, select **Configuration**, select the cluster, and in the **MRA Administration** page, click **Reapply Configuration**.

The configuration information is synchronized.

7. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

The **Upgrade Manager** page opens.

8. Select the cluster again and click **Continue Upgrade**.

You are prompted: Are you sure that you want to perform this action? Initiate upgrade *server_name* (next).

9. Click **OK** to continue.

The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the second server in the primary site. The **Upgrade Operation** column displays the progress of the current action.

When the second server is upgraded, the **Upgrade Operation** column displays the message: Initiate upgrade Completed Successfully at *date_time*.

10. Select the cluster again and click **Continue Upgrade**.

You are prompted: Are you sure that you want to perform this action? Initiate upgrade *server_name* (next).

11. Click **OK** to continue.

The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the spare server, in the secondary site. The **Upgrade Operation** column displays the progress of the current action.

When the spare server is upgraded, the **Upgrade Operation** column displays the message: Initiate upgrade Completed Successfully at *date_time* and Alarm 70501 is cleared.

The georedundant cluster is upgraded. For each server, the **Prev Release** column displays the release installed before the upgrade, and the **Up to Date** column displays Y (yes).

If the upgrade fails, a diagnostic message describes the problem. Try the upgrade again; if it fails again, contact My Oracle Support.

Note: If the upgrade fails and also leaves a server in an unrecoverable state (designated **Zombie** in the **Upgrade Operation** column, plus Alarm 70508), the Upgrade Manager cannot resolve the issue. Contact My Oracle Support immediately.

Viewing the Upgrade Log

You can view the upgrade log for an individual cluster. The log includes both automatic and manual actions taken during an upgrade. To view the upgrade log:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
The **Upgrade Manager** window opens.

2. Select the cluster and then click **View Upgrade Log**.
The **Upgrade Log** window opens.

The upgrade log is displayed. *Figure 38: Sample Upgrade Log* shows a sample upgrade log.

You can click on a column heading to sort the log on that column. You can drag the end of a heading to resize the column. You can click **Filter** and filter the rows on a value in any column. You can click **Columns** and select which columns appear in the log.

Upgrade Log

Cluster Name: CMP Site1 Cluster
Last Update: 2/12/2015 15:40:18

Filter

Columns

ID	Parent ID	Action Name	Start Time	End Time	Duration	Scope	Hostname	Result	Mode	Description
1	0	Preflight Check	2/7/2015 19:05:38	2/7/2015 19:05:46	0:00:07	Server	CMP24-58	Success	Manual	User initiated action: upg...
2	1	Upgrading server	2/7/2015 19:05:46	2/7/2015 19:38:06	0:32:20	Server	CMP24-58	Success	Automatic	Automatic action initiate...
3	1	Modify the role/replication attrib...	2/7/2015 19:05:46	2/7/2015 19:05:48	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
4	1	Wait for replication to synchronize	2/7/2015 19:38:06	2/7/2015 19:38:16	0:00:10	Server	CMP24-58	Success	Automatic	Automatic action waitfo...
5	1	Modify the role/replication attrib...	2/7/2015 19:38:06	2/7/2015 19:38:09	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
72	0	Backing out server upgrade	2/10/2015 8:58:51	2/11/2015 15:44:21	30:45:29	Server	CMP24-62	Success	Manual	User initiated action: inli...
73	72	Modify the role/replication attrib...	2/10/2015 8:58:51	2/10/2015 8:58:53	0:00:01	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
75	0	Preflight Check	2/11/2015 16:01:19	2/11/2015 16:01:34	0:00:14	Server	CMP24-58	Success	Manual	User initiated action: upg...
76	75	Upgrading server	2/11/2015 16:01:34	2/11/2015 16:33:05	0:31:30	Server	CMP24-58	Success	Automatic	Automatic action initiate...
77	75	Modify the role/replication attrib...	2/11/2015 16:01:34	2/11/2015 16:01:36	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
78	75	Wait for replication to synchronize	2/11/2015 16:33:05	2/11/2015 16:33:15	0:00:09	Server	CMP24-58	Success	Automatic	Automatic action waitFo...
79	75	Modify the role/replication attrib...	2/11/2015 16:33:05	2/11/2015 16:33:07	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...

Figure 38: Sample Upgrade Log

Upgrade Manager Page Elements

On the **Upgrade** section of the navigation pane, **Upgrade Manager** is an option. All clusters and servers in the Policy Management network are listed in the table on this page. Servers display in groups by cluster; you can collapse or expand cluster information by clicking the [-] or [+] icons in the first column of the table. The table is updated every ten seconds.

Figure 39: Sample Upgrade Manager Page shows a sample.

Upgrade Manager						
Start Rollback		Start Upgrade		Current ISO: incremental-upgrade-12.1.0.0.0_15.1.0		
				View Upgrade Log Filter Columns Advanced		
Name	Alarm Sev...	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
CMP Site1 Cluster (2 Servers)						
CMP24-58	Major	Y	Standby	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
CMP24-62	Major	Y	Active	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate backup Completed Successfully at May 27, 2015 11:59:17.
CMP Site2 Cluster (2 Servers)						
CMP24-163	Minor	Y	Standby	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.
CMP24-162	Minor	Y	Active	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
MPE-1 (3 Servers)						
MPE24-165	Minor	Y	Standby	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
MPE24-164	Minor	Y	Active	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.
MPE24-115	Minor	Y	Spare	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
MPE-2 (2 Servers)						
MPE24-30	Minor	N	Active	10.5.0_1.1.0	11.5.2_1.1.0	n/a
MPE24-29	Minor	N	Standby	10.5.0_1.1.0	11.5.2_1.1.0	Failed to Complete Initiate upgrade at Feb 12, 2015 9:23:50. (Generic Failure)
MRA-1 (3 Servers)						
MRA24-114	Minor	Y	Spare	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.
MRA24-69	Minor	Y	Standby	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
MRA24-68	Minor	Y	Active	12.0.0.0_40.2.0	12.1.0.0_15.1.0	Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.

Figure 39: Sample Upgrade Manager Page

The Upgrade Manager page contains the following elements:

- (check boxes) to select clusters to upgrade or roll back
- Buttons (context-sensitive actions such as **Start Rollback** or **Start Upgrade**); **View Upgrade Log**; **Filter**; and the name of the current ISO
- The table of filtered clusters and servers
- Lists (**Columns** and **Advanced**) for changing what columns are in the table and for selecting optional advanced operations

[Table 42: Upgrade Manager Page Elements](#) describes these elements.

Table 42: Upgrade Manager Page Elements

Element	Description
■ (check box)	Use the ■ (check box) column to select the cluster on which an operation is to be performed. All servers in the selected cluster will be affected by the operation. Note: You must select a cluster before you can select an operation.
Name	Displays the name of each cluster and server. You can drag the edge of the heading to resize the column.
Alarm Severity	Displays the highest level severity of alarm, if any, on the server: Critical , Major , or Minor . This indicates that at least one alarm of this severity has been raised on the server (there may be more than one), but none at any higher level of severity. If there are no alarms for the server, the severity is blank. You can drag the edge of the heading to resize the column.

Element	Description
	Note: An upgrade typically triggers minor, major, and critical alarms as servers are taken out of service or failed over. This is normal and to be expected.
Up to Date	Displays whether a server is up to date, that is, running the most recent release of Policy Management software available: <ul style="list-style-type: none"> • Y — the server is running the most recent software • N — the server is running a previous release of software • n/a — the server cannot be updated, because either the current ISO file does not apply to the server, no ISO file is loaded, or there is a problem with the server
Server Role	Displays the server's role in the cluster. You can drag the edge of the heading to resize the column. <p>Note: Roles are changed automatically during the course of an upgrade or rollback.</p> <ul style="list-style-type: none"> • Active • Standby • Spare • OOS (out of service) — the server is in Standby mode, either because of operator action or as part of an upgrade
Prev Release	Displays the previous Policy Management software release of each server, if known. The Filter list lets you display a specific release only or All releases. You can drag the edge of the heading to resize the column.
Running Release	Displays the current Policy Management software release operating on each server. The Filter list lets you display servers running a specific release only or all releases. You can drag the edge of the heading to resize the column.
Upgrade Operation	Displays details of the last or current operation performed on each server. You can drag the edge of the heading to resize the column.
Upgrade Log	Includes a View button. Click to view the upgrade log for that cluster. By default, this column is not visible. You can drag the edge of the heading to resize the column.
View Upgrade Log	Displays an Upgrade Log window for the selected cluster.
Filter	Use the Filter button to list a subset of clusters or servers in the table. You can filter by columns: <ul style="list-style-type: none"> • Name • Alarm Severity • Up to Date • Server Role • Prev Release • Running Release

Element	Description
	These filters are initially set to filter out nothing.
Columns	Use the Columns list to change the columns in the table. By default, all columns except Upgrade Log are shown. To remove a column, uncheck it.
Current ISO	Displays the upgrade procedure available, or n/a if no ISO file is available. If multiple ISOs are available, click on the name to select a different ISO.
Advanced	<p>Use the Advanced list to select an optional advanced upgrade operation to perform at a point of operator intervention. You must select a cluster (in the first column of the table) before you can select an optional operation.</p> <p>Note: The operations available in this list dependent on the current release, the cluster selected, the state of the cluster, and the current state of an upgrade or rollback in progress. In some cases there may be no available options, in which case the list is disabled.</p> <p>As a protective feature, when you select an optional operation, you are prompted to confirm the operation. If you click OK, a progress bar displays the status of the operation. After you confirm an operation, it cannot be cancelled.</p>

The actions available are determined by the Upgrade Manager based on the current release, the cluster you select, the cluster's current state, and its upgrade status. Invalid actions are disabled (grayed out). For example, in [Figure 39: Sample Upgrade Manager Page](#), **Start Upgrade** is a valid action for the selected cluster, but **Start Rollback** is not.

Common actions include the following:

- **Start Upgrade** (after a new ISO file is available)
- **Continue Upgrade** (when the upgrade process has reached a point of user intervention)
- **Start Rollback** (after a system is upgraded)
- **Continue Rollback** (when the rollback process has reached a point of user intervention)

You should normally be able to complete an upgrade by clicking only **Start Upgrade** and **Continue Upgrade**.

About Rolling Back an Upgrade

It is possible to roll back, or back out, the Policy Management software to the previous release in a production environment. The overall sequence is the reverse of the upgrade sequence:

1. Roll back MPE and MRA clusters.
2. Roll back all CMP systems except for the last CMP server. (You cannot begin this operation until all MPE and MRA clusters are rolled back.)
3. If you are rolling back to Release 11.5, use the **System Maintenance** page to roll back the last CMP server.

In the same way that you can roll back from an upgrade from any point of operator intervention, you can also upgrade from a rollback from any point of operator intervention. Whenever the action **Continue Rollback** is available, the action **Resume Upgrade** is also available.

Rolling Back an Upgrade

The default, preferred sequence followed by the Upgrade Manager to roll back a georedundant (three-server) cluster is as follows:

1. Roll back the standby server.
2. Roll back the spare server.
3. Fail over to the standby server.
4. Reapply the configuration to the cluster.
5. Roll back the remaining server.

An optional advanced action lets you change this order if required. You can also roll back the second and third server in the cluster simultaneously.

The default, preferred sequence followed by the Upgrade Manager to roll back a two-server cluster is as follows:

1. Roll back the standby server.
2. Fail over to the standby server.
3. Reapply the configuration to the cluster.
4. Roll back the remaining server.

You can roll back up to four MPE or MRA clusters in parallel. (You must manually start the process for each cluster.)

To roll back a georedundant cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
The **Upgrade Manager** page opens.
2. Select the cluster to be rolled back and click **Start Rollback**.
You are prompted: *Are you sure that you want to perform this action? Initiate backout server_name (back).*
3. Click **OK** to continue.

The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the standby server, in the primary site. The **Upgrade Operation** column displays the progress of the current action.

Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

When the standby server is rolled back, the **Upgrade Operation** column displays the message *Initiate backout Completed Successfully at date_time* and Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

Tip: Review alarms associated with each action before proceeding with the next action.

4. Select the cluster again and click **Continue Rollback**.
You are prompted: *Are you sure that you want to perform this action? Initiate backout server_name (back).*
5. Click **OK** to continue.

If you stop a rollback at a point of operator intervention, you can continue it later, or resume upgrading it from there.

The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the spare server, in the secondary site. The **Upgrade Operation** column displays the progress of the current action. When the spare server is rolled back, the **Upgrade Operation** column displays the message `Initiate backout Completed Successfully at date_time`.

6. Select the cluster again and click **Continue Rollback**.

You are prompted: Are you sure that you want to perform this action? Failover to old version *cluster_name* (next).

7. Click **OK** to continue.

The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.

8. Reapply the configuration to the cluster:

- (For an MPE cluster) From the **Policy Server** section of the navigation pane, select **Configuration**, select the cluster, and in the **Policy Server Administration** page, click **Reapply Configuration**.
- (For an MRA cluster) From the **MRA** section of the navigation pane, select **Configuration**, select the cluster, and in the **MRA Administration** page, click **Reapply Configuration**.

The configuration information is synchronized.

9. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

The **Upgrade Manager** page opens.

10. Select the cluster again and click **Continue Rollback**.

You are prompted: Are you sure that you want to perform this action? Initiate backout *server_name* (back)

11. Click **OK** to continue.

The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then rolls back the remaining server, in the primary site. The **Upgrade Operation** column displays the progress of the current action.

When the remaining server is rolled back, the **Upgrade Operation** column displays the message `Initiate backout Completed Successfully at date_time` and Alarm 70501 is cleared.

The cluster is rolled back to the previous release. For each server, the **Running Release** column displays the release to which you rolled the system back, and the **Up to Date** column displays N (no).

If the rollback fails, a diagnostic message describes the problem. Try the rollback again; if it fails again, contact My Oracle Support.

Note: If the rollback fails and also leaves a server in an unrecoverable state (designated **Zombie** in the **Upgrade Operation** column, plus alarm 70508), the Upgrade Manager cannot resolve the issue. Contact My Oracle Support immediately.

Rolling Back a Release 11.5 Primary-site CMP Cluster

If you are rolling back an entire Policy Management network, you must roll back the primary-site CMP cluster (designated CMP Site1 cluster) last. If you are rolling back to release 11.5, this rollback procedure is different from the rollback procedure for other clusters because you must use the Upgrade Manager for release 11.5 to roll back the last release 12.1 CMP system.

To roll back the primary-site CMP cluster to release 11.5:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
The **Upgrade Manager** page opens.
2. Select the primary-site CMP cluster (the CMP Site1 cluster) and click **Start Rollback**.
You are prompted: Are you sure that you want to perform this action? Initiate backout *server_name* (back).
3. Click **OK** to continue.
The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the standby server. The **Upgrade Operation** column displays the progress of the current action.

Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

When the standby server is rolled back, the **Upgrade Operation** column displays the message Initiate backout Completed Successfully at *date_time* and Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

Tip: Review alarms associated with each action before proceeding with the next action.
4. Verify that all CMP servers except the active server are rolled back.
5. Select the cluster again and click **Continue Rollback**.
You are prompted: Are you sure that you want to perform this action? Failover to old version *cluster_name* (next).
6. Click **OK** to continue.
The confirmation window closes and the cluster fails over to the standby server, which becomes the active server. You are logged out of the CMP system.

Note: The active server will be running release 11.5.
7. Log in to the active CMP server as an administrator with upgrade privileges.
You have access to the **Upgrade Manager** menu in the navigation pane.
8. From the **Upgrade Manager** section of the navigation pane, select **System Maintenance**.
The **System Maintenance** page opens.
9. Select the last CMP server and from the **Operations** list, select **Other Operations** and then select **Backout**.
You are prompted: Are you sure you want to execute Backout?
10. Click **OK** to continue.
The last CMP server is backed out.
11. When the backout is marked complete, select the last CMP server and from the **Operations** list, select **Other Operations** the select **Cancel Force Standby**.
You are prompted: Are you sure you want to execute Cancel Force Standby?
12. Click **OK** to continue.
The confirmation window closes and the forced standby state is canceled. The **Server State** column displays the server state as Standby.

The CMP cluster is rolled back to release 11.5.

If the rollback fails, a diagnostic message describes the problem. Try the rollback again; if it fails again, contact My Oracle Support.

Note: If the rollback fails and also leaves a server in an unrecoverable state (designated Zombie in the **Upgrade Operation** column, plus Alarm 70508), the Upgrade Manager cannot resolve the issue. Contact My Oracle Support immediately.

ISO Maintenance Page Elements

On the **Upgrade** section of the navigation pane, **ISO Maintenance** is an option. All clusters and their constituent servers in the Policy Management network are in the table on this page. You can collapse or expand the display of servers by clicking the [-] or [+] icons in the first column of the table. The display is updated every ten seconds. *Figure 40: Sample ISO Maintenance Page* shows a sample **ISO Maintenance** page.

ISO Maintenance (Last Refresh :05/12/2015 11:28:42)

Save Layout Columns Filters Operations

		Name	Appl Type	Site	IP	Running Release	ISO
+	<input type="checkbox"/>	MPE-2	MPE				
-	<input type="checkbox"/>	MRA-1	MRA				
-	<input type="checkbox"/>	MRA24-68	MRA	Site-1	10.148.24.68	12.1.0.0.0_15.1.0	<input type="checkbox"/> mra-12.1.0.0.0_15.1.0-x86_64.iso
-	<input type="checkbox"/>	MRA24-69	MRA	Site-1	10.148.24.69	12.1.0.0.0_15.1.0	<input type="checkbox"/> mra-12.1.0.0.0_15.1.0-x86_64.iso
-	<input type="checkbox"/>	MRA24-114	MRA	Site-2	10.148.24.114	12.1.0.0.0_15.1.0	<input type="checkbox"/> mra-12.1.0.0.0_15.1.0-x86_64.iso
+	<input type="checkbox"/>	MPE-1	MPE				
-	<input type="checkbox"/>	CMP Site2 Cluster	CMP Site2 Cluster				
-	<input type="checkbox"/>	CMP24-162	CMP Site2 Cluster	Unspecified	10.148.24.162	12.1.0.0.0_15.1.0	<input type="checkbox"/> cmp-12.1.0.0.0_15.1.0-x86_64.iso
-	<input type="checkbox"/>	CMP24-163	CMP Site2 Cluster	Unspecified	10.148.24.163	12.1.0.0.0_15.1.0	<input type="checkbox"/> cmp-12.1.0.0.0_15.1.0-x86_64.iso
-	<input type="checkbox"/>	CMP Site1 Cluster	CMP Site1 Cluster				
-	<input type="checkbox"/>	CMP24-58	CMP Site1 Cluster	Unspecified	10.148.24.58	12.1.0.0.0_15.1.0	<input type="checkbox"/> cmp-12.1.0.0.0_15.1.0-x86_64.iso
-	<input type="checkbox"/>	CMP24-62	CMP Site1 Cluster	Unspecified	10.148.24.62	12.1.0.0.0_15.1.0	<input type="checkbox"/> cmp-12.1.0.0.0_15.1.0-x86_64.iso

Figure 40: Sample ISO Maintenance Page

The following types of elements display on the **ISO Maintenance** page:

- Check boxes to select clusters or servers on which to perform operations
- The table of filtered clusters and servers
- Lists (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for selecting operations

Table 43: ISO Maintenance Page Elements describes the elements on the **ISO Maintenance** page.

Table 43: ISO Maintenance Page Elements

Element	Description
<input type="checkbox"/> (checkbox)	Use this column to select the clusters or servers on which an operation is to be performed. If you select a cluster, all servers in that cluster are selected. Note: At least one cluster or server must be selected before you can select an operation from the Operations menu.
Name	Displays the names of all filtered clusters and servers. When a server is receiving an ISO file, a download icon displays next to the name. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.

Element	Description
Appl Type	Displays the type of application running on each server. The Filters list lets you select the application type: CMP Site1 Cluster , CMP Site2 Cluster , MPE , MRA , or All applications. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Site	Displays the site name, if any, that is associated with each server. The Filters list also lets you display Unspecified or All sites. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column. Note: This column is only shown for a georedundant Policy Management network.
IP	Displays the OAM server IP address of each server. The Filters list lets you filter on only a server with a specific IP address or display All servers. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Running Release	Displays the current Policy Management software release of each server. The Filters list lets you filter on only a specific major release only or display All releases. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
ISO	Displays the ISO files available on each server. Use the checkbox to select the ISO file to delete during the Delete ISO operation. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Columns	Use the Columns list to change the columns that are shown in this table. The Name column is mandatory. By default, all columns display. To change which columns display, uncheck the columns to be removed from the page.
Save Layout	Use the Save Layout button to save formatting changes to this page.
Filters	Use the Filters list to select a subset of clusters and servers to display on this page. On this menu are the following pulldown filter submenus: Appl Type , Site , IP , and Running Release . By default, the filters are set to All , and all servers are listed. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	Use the Operations list to select an ISO operation to perform. Note: You must select (in the first column of the table) the cluster(s) or server(s) on which the operation is being performed before you can select an operation. The operations listed are dependant on the state of the selected servers; that is, if you select more than one server, only the operations that are valid for all the selected servers display. Possible operations are Push Script , Upload ISO , and Delete ISO . As a protective feature, before Push Script or Delete ISO are executed, you are prompted whether you sure you want to execute the operation. If you click OK , the operation is performed. A progress bar displaying the status of the command execution displays in a window.

Element	Description
	Note: After an operation is confirmed, it cannot be cancelled.

Chapter 17

Global Configuration

Topics:

- [*Setting the Precedence Range.....320*](#)
- [*Setting UE-Initiated Procedures.....321*](#)
- [*Setting Stats Settings.....321*](#)
- [*Setting Quota Settings.....322*](#)
- [*Setting eMPS ARP Settings.....323*](#)
- [*Setting S9 Settings.....324*](#)
- [*Setting PDN APN Suffixes.....324*](#)
- [*Configuring the Activity Log.....325*](#)
- [*Configuring Custom APNs.....326*](#)
- [*About Emergency APNs Settings.....327*](#)

This section describes how to configure the global settings in the CMP system.

Setting the Precedence Range

When overlapping policy and charging control (PCC) quality of service (QoS) rules apply to the same Gx or Gxx Diameter session, precedence is applied to determine which rule is installed on the gateway. In the case of an overlap, the rule with the lower precedence value is installed. Some vendor gateways require unique precedence, or else reject rules. You can configure MPE devices to maximize the probability that all rules have unique PCC rule precedences. This is a global configuration setting that affects all MPE devices managed by this CMP system.

Note: This does not guarantee rule precedence uniqueness. Operator-defined rules are not validated to ensure precedence uniqueness; if you define such rules, you must track their precedence values yourself.

To set the precedence range:

1. From the **Global Configuration** 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 **Precedence Range** group.
The **Precedence Range Configuration** page opens in the work area.
3. Click **Modify**.
The fields become editable.
4. Enter values for the configuration attributes:
 - a) **AF-Triggered** — Enter the minimum and maximum values for rules triggered by Rx requests. The default range is 400 to 899.
 - b) **UE-Triggered** — Enter the minimum and maximum values for rules triggered by user equipment-initiated resource requests. This range cannot overlap with the AF range. The default range is 1000 to 1999.
 - c) **Default Session** — If no other rules are installed when a Gx eHRPD, E-UTRAN, or GPRS session is established, a default rule is installed. Enter the default session precedence. The default precedence is 3000.
5. Click **Save**.

The reserved precedence ranges are configured.

Precedence values not set aside here are available for your use in defining rules. By default, you can use:

- 0–399
- 900–999
- 2000–2999
- 301–4,294,967,295

Note: Range changes do not automatically redeploy rule with new precedence values. Also, range changes do not automatically cause the validation of defined traffic profiles.

When traffic profiles are imported, they are imported regardless of their configured precedence values. The CMP system displays a message reminding you to check the precedence values of the imported traffic profiles.

Setting UE-Initiated Procedures

When enabled, this feature allows an MPE device to trap UE-Init resource modification requests and reject them using the specified parameters. This feature applies to Gx and Gxx (Gxa, Gxc) interfaces.

To enable or disable processing of UE-Initiated procedures or to change configuration attributes:

1. From the **Global Configuration** 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 **UE-Initiated Procedures**.
The **UE-Initiated Procedures** page opens in the work area group.
3. Click **Modify**.
The **Modify UE-Initiated Procedures** page opens.
4. Enter values for the configuration attributes:
 - a) **Reject UE-Initiating Request** — Select to enable this feature to reject UE-Initiated resource modification requests gracefully, or leave unchecked to process normally with no impact (by ignoring specific AVPs relevant to the UE-Initiated procedure request). The default is unchecked (disabled).
 - b) **Experimental Result Code** — Enter the numeric value that is returned in the Experimental-Result-Code AVP as part of the CCA message (if no configured code exists). Enter an integer between 0 and 2,147,483,647. The default value is 5144.
 - c) **Experimental Result Code Name** — Enter the description of the error that is returned in the Experimental-Result-Code AVP as part of the CCA message. Enter a string value up to 255 characters in length. The default name is `DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED`.
 - d) **Experimental Result Code Vender Id** — Enter the vender ID that is included in the Experimental-Result-Code AVP as part of the CCA message. Enter an integer between 0 and 2,147,483,647. The default ID is 10415.
 - e) **Experimental Result Code Vendor Name** — Enter the vender name that is included in the Experimental-Result-Code AVP as part of the CCA message. Enter a string value up to 255 characters in length. The default name is 3GPP.
5. Click **Save**.

The UE-initiated attributes are configured.

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 **Global Configuration** 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 area.

3. Click **Modify**.

The fields become editable.

4. Configure the **Stats Reset Configuration**.

- **Manual** (default)

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 after which stats are written to the Policy Management devices from the list. Options are minutes.

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

6. Click **Save**.

The Stats Settings attributes are configured.

Setting Quota Settings

This feature defines the quota pools.

To enable or disable processing of the Quota Settings procedures or to change configuration attributes, do the following:

1. From the **Global Configuration** 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 **Quota Settings** folder.

The **Quota Settings** page opens in the work area.

3. Click **Modify**.

The **Quota Settings** page refreshes with pooled quota settings editable.

4. Enter values for the configuration attributes:
 - a) **Enable subscriber pools** — The global configuration setting for a pooled quota is enabled if the box is checked.
 - b) **Enable pooled quota usage tracking** — This allows both individual quota usage tracking and pool quota usage tracking to occur simultaneously.
 - c) **Enable pooled entity state** — A defined policy which allows you to update individual entity states or pool entity states or both.

Note: A subscriber can only be associated with one pool.

 - d) **Enable pooled dynamic quota** — Enables pooled dynamic quotas for passes. The default is disabled.
 - e) **Enable Pass Expiration Extension** — Allows the expiration date and time value of a pass to be extended to match a later expiration date and time value of a pass that has the same name or is in the same pass group.

5. Click **Save**.

The Quota Setting attributes are configured.

Setting eMPS ARP Settings

The Enhanced Multimedia Priority Service (eMPS) feature allows prioritization of IMS-based calls. The feature allows National Security/Emergency Preparedness users to make calls over the public network when the network is congested by giving those calls/sessions priority in the network over other traffic.

The values configured through the CMP system, using the process below, are used as the default Allocation and Retention Policy (ARP) values for all MPE devices associated with the CMP system when a session is identified as Priority and the ARP values are not defined through policy.

To enable or disable prioritization of IMS-based calls:

1. From the **Global Configuration** 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 **eMPS ARP Settings** folder.
The **Priority Value** page opens in the work area.
3. Click **Modify**.
The **eMPS ARP Settings** page opens.
4. Enter values for the configuration attributes:
 - a) **Priority Value** — Defines the relative importance of a resource request. Enter a value from 1 to 15. The default is 1.
 - b) **Preemption Capability** — Defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. Select **Enable** or **Disable** from the list. The default is **Enable**.
 - c) **Preemption Vulnerability** — Defines whether a service data flow can lose the resources assigned to it so that a service data flow with a higher priority level can be admitted. Select **Enable** or **Disable** from the list. The default is **Disable**.

5. Click **Save**.

The eMPS ARP Settings attributes are configured.

Setting S9 Settings

To configure global S9 settings:

1. From the **Global Configuration** 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 **S9 Settings** folder.

The **S9 Settings** page opens in the work area.

3. Click **Modify**.

The **S9 Settings** page opens.

4. Click on each category title and enter values for the configuration attributes:

a) **APN Configuration** — Click **All** or click **List** and enter a comma-separated list of APNs for which an MPE device can accept a request when acting as a home PCRF (HPCRF).

b) **Acceptable Event Triggers** — Click **Select All** or select from the list of event triggers acceptable from the HPCRF when an MPE device acts as a visited PCRF (VPCRF).

To clear the list, click **Deselect All**.

c) **Report Specific Action Over S9** — Click **Select All** or select from the list of Rx-specific actions to filter the actions from being sent to the HPCRF from the VPCRF. For example, you can use this to prevent the action `INDICATION_OF_SUCCESSFUL_RESOURCE_ALLOCATION` from being reported to the HPCRF.

To clear the list, click **Deselect All**.

d) **Home MCC-MNC Lists** — Select a match list from the list of defined MCC-MNC match lists. Use these values to identify subscribers who are local for the MPE device. You can enter up to 500 MCC-MNC pairs.

See *Policy Wizard Reference* for more information on creating match lists of MCC-MNCs.

5. Click **Save**.

You have configured the S9 settings.

Setting PDN APN Suffixes

Access point name (APN) suffix matching on the MPE device is performed by reading the APN suffixes configured on the CMP system. An APN is considered a match based on the longest suffix it has in common after a case-insensitive comparison.

The MPE device dynamically creates a new stats object the first time it receives a new APN suffix match for a PDN connection. After it is created, each new PDN connection for that APN updates the current object. If a stats object has not been created for an APN suffix, the stats object is not displayed in the APN reports page.

If the MPE device receives a PDN connection without a configured APN suffix match, then the connection is added to a stats object called OtherAPN.

PDN connections per APN suffix are shown in the PDN APN suffix report. See [Viewing the PDN APN Suffix Report](#) for more information.

Up to 25 different APN suffixes can be configured. Each suffix is limited to 64 characters.

To configure PDN APN suffixes:

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 **PDN APN Suffixes** folder.
The **PDN APN Suffix Administration** page opens in the work area, listing the configured PDN APN suffixes.
3. Click **Create PDN APN Suffix**.
4. Enter the following values:
 - a) **Name** — Enter the name of the APN suffix.
 - b) **Value** — Enter a value for the APN suffix.
 - c) **Description** — Enter descriptive text.
5. Click **Save**.

The PDN APN suffix is created.

Configuring the Activity Log

The Activity Log allows the real-time tracing activity of Gx and Rx protocol messages to be performed for a specific subscriber from multiple MPE devices.

After activation, traces for subscriber protocol messages are merged from all MPE devices in the network to the CMP system. Messages are selected for tracing based on subscriber identification.

Up to 100 subscriber IDs can be configured in the subscriber configuration window with tracing enabled or disabled. Tracing can be enabled for up to 20 subscribers.

After tracing is enabled, the following associated tasks can be performed:

- Modify subscriber tracing configuration settings and add subscribers for tracing
- Activate and deactivate trace log backup
- View and export historical trace log data
- View and export real-time trace data for up to 10 subscribers

See [Subscriber Activity Log](#) for information on performing these tasks.

To enable subscriber tracing, do the following:

1. From the **Global Configuration** 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 **Activity Log Configuration**.
The **Activity Log Configuration** page opens in the work area.
3. Click **Modify**

The fields become editable.

4. Enter the number of subscribers for which tracing can be performed in the **Max Subscriber Trace Count** field. The subscriber trace count can be a value of 1 to 100. The default is 100.
5. Enter the number of active subscribers for which tracing can be performed in the **Max Active Subscriber Trace Count** field. The default is 20. Up to 20 subscribers can be enabled for tracing.
6. Click **Save**.

Subscriber tracing is enabled.

Configuring Custom APNs

Custom Access point name (APN) configuration on the MPE device, when the setting is set to true, overrides the behavior of the DIAMETER.ENF.AFDirectReply setting on a per APN basis.

When the DIAMETER.ENF.AFDirectReply setting is set to true, all Rx processing can be synchronous for specific APNs.

The **Custom APNs Configuration** display has three screens:

- **Synchronous APNs**
- **Session Recovery APNs**— allows a session recovery.
- **Session Synch APNs**—allows you to enable or disable Gx Session-Synch on a per APN per MPE basis.

To configure custom APNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Custom APNs Configuration** folder.
3. Click **Modify**.
4. To configure Synchronous APNs:
 - a) On the **Custom APNs Configuration** page, select the **Synchronous APNs** section.
 - b) Enter a **Synchronous APN** (for example, **xyz1.oracle.com**).
 - c) Click **Add** to add the new Synchronous APN to the list.
 - d) To delete an APN, select the APN in the list and click **Delete**.
 - e) Click **Save**.
5. To configure Session Recovery APNs:
 - a) On the **Custom APNs Configuration** page, select the **Session Recovery APNs** section.
 - b) Enter the name of the **Session Recovery APN**.
 - c) Click **Add** to add the Session Recovery APN.
 - d) To delete a Session Recovery APN, select the APN in the list and click **Delete**.
 - e) Click **Save**.
6. To configure a Session Synch APN:
 - a) On the **Custom APNs Configuration** page, select the **Session Synch APNs** section.
 - b) Enter a **Session Synch APN**.
 - c) Click **Add** to add the Session Synch APN.
 - d) To delete a Session Synch APN, select the APN in the list and click **Delete**.

- e) Click **Save**.

The custom APNs are configured.

About Emergency APNs Settings

The MPE determines if an IP-CAN Session requires an IMS emergency session based on the PDN-id. The MPE device stores a configurable list of Emergency APNs that are valid for the the MPE device. For emergency APNs, the IMSI cannot be present. The MPE device supports requests for PCC and QoS Rules that do not include an IMSI. See [Viewing the Audit Log](#).

The MPE device verifies the Service-URN if the IMS service information is associated with a UE IP address belonging to an emergency APN. The MPE device stores a configurable list of Service-URNs designated for emergency services. If the IMS service information does not contain an emergency-related indication and the UE IP address is associated with an emergency APN, the MPE rejects the IMS service information provided by the AF.

The **Emergency APNs Settings** display has two tabs:

- **Emergency APNs**
- **Emergency Service-URNs**

Adding Emergency APNs Settings

To add emergency APNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency APNs** section.
5. Enter an emergency APN.
6. Click **Add** to add the emergency APN to the list.
7. Click **Save**.

Deleting Emergency APNs Settings

To delete emergency APNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency APNs** section.
5. Select the emergency APN in the list.
6. Click **Delete**.
7. Click **Save**.

Adding Emergency Service-URNs Settings

To add emergency Service-URNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency Service-URNs** section.
5. Enter an emergency service-URNs.
6. Click **Add** to add the new emergency service-URN to the list.
7. Click **Save**.

Deleting Emergency Service-URNs

To delete emergency Service-URNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency Service-URNs** section.
5. Select the emergency service-URN in the list.
6. Click **Delete**.
7. Click **Save**.

Chapter 18

System Administration

Topics:

- [*Configuring System Settings.....330*](#)
- [*Importing and Exporting Configurable Objects.....332*](#)
- [*About the Manager Reports.....341*](#)
- [*Viewing the Trace Log.....342*](#)
- [*Viewing the Audit Log.....344*](#)
- [*Managing Scheduled Tasks.....347*](#)
- [*About Managing Users.....351*](#)
- [*Changing a Password.....367*](#)

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, after 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 enter a new password.)
 - h) **EMS Shared Secret** — Field provided to support third-party single sign-on architectures.
 - i) **Minimum Password Length** — The minimum allowable length in characters for a password, from 6 to 64 characters.
The default is six 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. You can enter up to 50 characters. You can select the font, size, and color of the text.

- l) **Allow policy checkpoint and restore (copies; 0=disallow)** — The number of checkpoints allowed in the system. Valid value range is 0 to 10. If set to 0, the Policy Checkpoint/Restore option is turned off and is no longer visible under the Policy Management heading on the navigation panel. The default value is 0.
4. In the **Invalid Login Threshold** settings section, define the following:
 - a) **Enable** — Enables login threshold control.
By default, this feature is enabled; deselect 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 or IPv6 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 non-alphabetic 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**.
7. To refresh the CMP system, log out and log back in.

The system settings are configured.

Figure 41: 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 3

☐ Require at least lower-case letter(s) (1-64) 0

☒ Require at least upper-case letter(s) (1-64) 1

☒ Require at least numeral(s) (1-64) 1

☒ Require at least non-alphanumeric character(s) (1-64) 0

☒ Force users with weak password to change password at their next login

Figure 41: Sample Password Strength Policy

Importing and Exporting Configurable Objects

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.

You can export configuration information as a single ZIP file. This ZIP file contains an inner ZIP file of XML files, an MD5 checksum file for data verification, and an `exportResults.txt` file containing export result messages. You can use these exported XML or ZIP files to update configurable objects in a CMP system or to configure a new system.

Note: For CMP systems in network mode, the **Import/Export** action is only available for NW-CMP servers. S-CMP servers do not show this action.

User Privileges and Import/Export

Note: Releases of CMP earlier than 12.1 include the user role of **Policy Management Privileges** for **Policy Import/Export**. With release 12.1, the **Policy Import/Export** privilege changes to the **Policy Checkpoint** privilege. If you had a user role that included the **Policy Import/Export** privilege and upgraded to release 12.1, you must update your user role to include **Policy Checkpoint** to ensure you can use the **Perform checkpoint before importing** option.

To use the **Import/Export** action, you must have a role that includes the **System Administrator Privileges Import / Export** privilege.

Note: If the you have a role with the **Import / Export** privilege, then top-level objects are available for importing and exporting even though you may not have specific privileges to view the objects (that is, the specific object is hidden to your role).

See [Creating a Role](#) for details on roles and privileges.

If the you are expected to perform checkpoint operations during an import action, you must have a role that includes **Policy Management Privileges** with **Read-Write** access to **Policy Checkpoint**. See [Checkpoint and Importing Objects](#) for more information.

About Importing Configuration Objects

The CMP system exports configurable objects to a ZIP file. This ZIP file consists of an inner ZIP file, `export.zip`, containing XML files of configuration data (by object type), an MD5 checksum file (`md5.txt`), and an `exportResults.txt` message file. By default, during an import, the CMP system uses the MD5 file to verify the integrity of the import file.

The Import function provides a method for importing either XML or ZIP configuration data files. In this way, the CMP configurable objects in a system can be restored to a prior configuration or a new CMP system created and configured.

Another import option allows the CMP system to use the Checkpoint function to save a snapshot of all existing configuration objects. If necessary, this snapshot can be used to restore the system to its previous configuration. See [Checkpoint and Importing Objects](#) for more information. Refer to the *Policy Wizard Reference* for details on managing policy checkpoints.

See [About Adding Objects for Export](#) for details on exporting configuration objects.

Checkpoint and Importing Objects

Attention: To use the checkpoint option, the **Allow policy checkpoint and restore** setting must be configured in **System Settings**. See [Configuring System Settings](#).

During an import action, the CMP system includes the **Perform checkpoint before importing** option. This is a protective measure that uses the Checkpoint function to save a snapshot of all the configuration objects that exist in the system. See the *Policy Wizard Reference* for more checkpoint details. Included in the checkpoint output file are:

- Configurable objects such as policies, policy groups, policy templates, policy tables, traffic profiles, match lists, retry profiles, applications, policy counter IDs, MPE configuration templates, and traffic profile groups, RADIUS CoA templates
- All MPE templates
- Associations between virtual MPE templates and real MPE templates
- Associations between MPEs and virtual MPE templates
- Associations between virtual MPE templates and other configuration objects (for example, policies)

Enabling the checkpoint option ensures that if a newly reconfigured system fails to function as expected, a checkpoint XML file exists that returns the system to the state prior to the import action. An additional benefit is that the checkpoint output file is saved in the CMP database and is accessible using **Policy Checkpoint/Restore** under the **Policy Management** section. Refer to the *Policy Wizard Reference* for details on managing checkpoint files.

In a networked CMP system, the checkpoint function is limited to the NW-CMP server. The **Perform checkpoint before importing** option is not available for S-CMP servers. After a restoration from a checkpoint onto a NW-CMP server, the NW-CMP server pushes the restoration data to all S-CMP servers. The MPE and virtual MPE templates are not updated. Real MPE templates and related associations are restored on the S-CMP servers, so that the policies can be restored to MPE through the virtual template.

The **Checkpoint** function differs from the **Export All** function in the following ways:

- The output file is an XML file that is saved in the CMP database.
- MPE template associations are saved.

See [Exporting All Configuration Objects](#) for details on exporting all configurable objects.

Importing Configuration Object Files

To import XML or ZIP files, use the following file naming conventions:

- If you are importing a ZIP file, the filename for the inner ZIP file must be `export.zip`.
- If you are importing a series of XML files, the recommended file naming convention is `obj_type + Export[sequence_number] + *.xml`. For example:
 - `networkelementExport1_20150501.xml`
 - `networkelementExport2_20150501.xml`
 - `networkelementExport3_20150501.xml`

Note: If there are multiple files of one type, the sequence number is necessary. Any object groups for import should be included in the last file of the sequence.

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Import**.
The import file upload form and options appear.
3. Click **Browse** to locate the file to be imported.
4. Select a processing option to use to **Handle collisions between imported items and existing items**:
 - **Delete all before importing** — CMP system deletes all objects for each object type matching the import file before importing the object type XML file.

Attention: This import strategy can result in object inconsistency. For example, if you import a ZIP file that only contains traffic profiles, all the traffic profiles are deleted first. However, if existing policies depend on the existing traffic profiles, and the import file does not contain them, the policies can become invalid.
 - **Overwrite with imported version** — For each object in the import file, if the object exists in the CMP system, the import updates the object with the configuration contained in the import file. If an object does not exist, the CMP system adds the object to the system.
 - **Reject any that already exist** — For objects that already exist in CMP system, the import action does nothing. For objects that do not exist in the CMP system, the import adds the objects to the system.
 - **Any collisions prevent all importing** — The CMP system compares all objects in the import file with objects in the system. If any object exists, the entire import is canceled.
 - **Validate without importing** — If an MD5 file (part of the ZIP file) is present, the CMP system performs an MD5 checksum on the ZIP file and compares the hash value with that in the MD5 file. If the hash values match, the system validates each XML file contained in the inner ZIP file. The CMP system then performs a collision check between the system and the XML files and indicates if any exists.
5. Select one or more **Options**:
 - **Skip checksum** — If unselected and an MD5 file (part of the ZIP file) is present, the CMP system performs a checksum on the inner ZIP file and compares the hash value with that of the MD5 file from the ZIP file. If the values do not match, the import action is canceled.

If selected, the CMP system does not perform a checksum and proceeds with the import.

- **Perform checkpoint before importing** — If selected, the CMP system uses the **Checkpoint** function to save a file with all the configuration objects that exist in the system. The checkpoint file is saved in the CMP database. See [Checkpoint and Importing Objects](#) for more information.

6. Click **Import**.

The configuration objects and their configuration settings are imported into CMP. After the import is complete, the window reports the results for each XML file contained in the ZIP file. Results include whether a file was successfully imported or the number of objects successfully updated. Any problems during the import action appear in red text.

Note: As the result of memory limitations, the CMP system displays the top 2000 characters for each import type file.

The checkpoint file and the checkpoint management functions are accessed using **Policy Checkpoint/Restore** under the **Policy Management** section. Refer to the *Policy Wizard Reference* for details on managing policy checkpoint files.

About Exporting Configuration Objects

The Export action provides a method for exporting CMP configuration information as a ZIP file. Using this file, the configurable objects can be restored to a prior configuration or a new system can be created and configured.

As part of the export action, the CMP system performs the following actions:

1. Exports the configuration objects as individual XML files by object type.

Note: Network Element, Policy, and Policy Counter ID objects will be exported into multiple XML files. Network Element files contain a maximum of 500 objects per file. Policy files contain a maximum of 10000 objects per file. Policy Counter ID files contain a maximum of 10000 objects per file.

2. Compresses the XML files into a ZIP file named `export.zip`.
3. Creates the `exportResults.txt` file containing export result messages.
4. Calculates MD5 checksum number for `export.zip` and creates an `md5.txt` file containing the MD5 number.
5. Compresses the `md5.txt`, `exportResults.txt`, and `export.zip` files into another ZIP file named `CMP_export__yyyyMMddhhmmss.zip`.
6. Downloads the `CMP_exportZIP` file to the local computer.

To restore or configure a CMP system, see [Importing Configuration Object Files](#).

Export Window Overview

The **Bulk Export** window is divided into three areas.

- Object List

The left pane lists all of the configurable object types in CMP that are available for export. The top pane contains the **View Cart** link and a counter for the total number of objects in the cart.

- Work Area

The work area lists all of the configured objects for the selected object type. Objects are listed by Name in ascending alphabetical order. A maximum of 50 objects per page are shown.

- Navigation Area

Page navigation links appear at the top left of the work area. A **Search** text box appears at the top right of the work area. You can search the entire list of objects for specific strings and numbers. The **Search** text box accepts the wildcard (%) and underscore (_) characters.

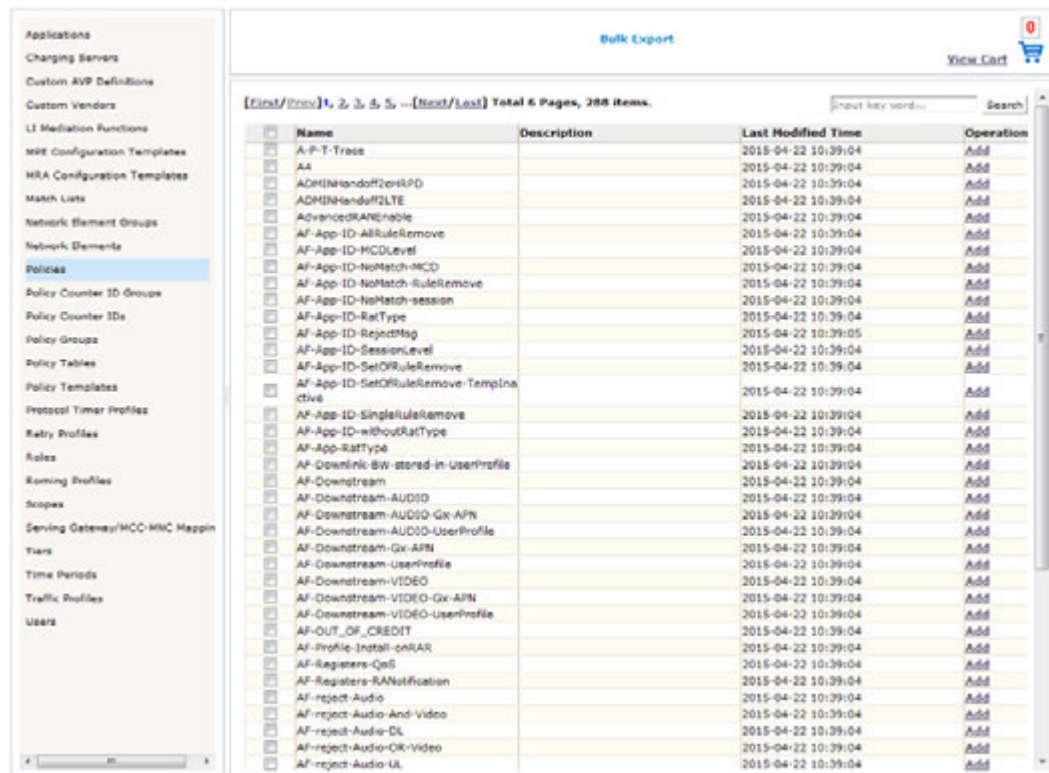


Figure 42: Bulk Export Window

About Adding Objects for Export

The Export action has different methods for selecting export objects:

- **Add**
Adds a single object to the export cart. See [Exporting a Configuration Object](#).
- **Add selected items**
Adds selected objects to the export cart. See [Exporting Multiple Selected Objects](#).
- **Add filtered items**
Adds the results of a search to the export cart. See [Exporting Multiple Filtered Objects](#)

After configuration objects have been added to the export cart, they are ready for export.

See [Exporting All Configuration Objects](#) for details on exporting all configurable objects.

Exporting a Configuration Object

To export a configuration object:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.

2. Select **Export**.

The **Bulk Export** page opens with a listing of exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the object type from the left pane (for example, **Policies**).

A list of configured objects for the specified type displays in the work area.


4. To include dependent objects in the export file, select **Include Dependencies**.

Any object dependencies for the selected objects will also be selected for export.

5. Use the pagination links at the top left of the work area to locate the object for export.

6. Click **Add** for the object to export.

A message displays indicating the named object has been successfully added to the cart.

7. Click  to close the message.

Note: If **Include Dependencies** is checked, the total number of items in the export cart may exceed the number of items checked in the list.

8. Click **View Cart** or  to continue with the export.

The **Check out Page** opens.

9. To remove an object from the listing, use any of the following methods:

- Click **Remove** next to the named object.
- Select the check box next to the named object and click **Remove selected items**.
- Use the **Search** tool to search the list for a specific string to remove and click **Remove filtered items**.

10. After the export list of objects is complete, click **Export Cart**.

A warning message displays verifying that you want to export the select item in the shopping cart.

11. Click **OK** to proceed with the export.

12. Click **Clear Cart**.

The contents of the export cart are removed.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention:
CMP_export_YYYYMMddhhmmss.zip.

Exporting Multiple Selected Objects

To export multiple selected objects:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.

2. Select **Export**.

The **Bulk Export** page opens with a list of the exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the object type from the left pane (for example, **Policies**).



A list of configured objects of the specified type displays in the work area.

4. To select all objects on the page for export:

- a) Select the check box next to the Name heading of the table.

All objects listed on the page are selected.

Note: Your selections only apply to the current page. Objects on other pages are not selected.

- b) Click **Add selected items** to add all objects in the filtered list to the export cart.
A message displays indicating the objects has been successfully added to the export cart.
5. To select several objects from multiple pages for export:
 - a) Use the pagination links at the top left of the work area to locate the first page of objects for export.
 - b) Select the check box next to the name of each of the objects to be exported.
 - c) Click **Add selected items** to add the selected objects to the export cart.
 - d) Use the pagination links at the top left of the work area to locate the next page of objects for export.
 - e) Select the check box next to the name of each of the objects to be exported.
 - f) Click **Add selected items** to add the selected objects to the export cart.
A message displays indicating the objects has been successfully added to the export cart.
6. Click the  to the right of the message to close the message.
7. Click **View Cart** or  to continue with the export.
The **Check out Page** opens.
8. Review the listing of objects.
9. To remove an object from the listing, use one of the following methods:
 - Click **Remove** next to the named object.
 - Select the check box next to the named object and click **Remove selected items**.
 - Use the **Search** tool to search the list for a specific string and click **Remove filtered items**.

Note: Any checked items will become unchecked if you change pages.

10. To view a filtered list of export objects by object type:

- a) Click the **Type** list and select the object types.
- b) Click **Search**.

All of the selected object types display in the list.

Note: The remaining object types are still in the export cart. To view the entire contents, select **All** from the **Type** list and click **Search**.

11. When the list of objects is ready, click **Export Cart**.

A warning message displays verifying that you want to export the select items in the shopping cart.

12. Click **OK** to proceed with the export.

13. Click **Clear Cart**.

The contents of the export cart are removed and you can proceed with another export.



A ZIP file is downloaded to your local computer. The filename uses the following naming convention:
CMP_export_YYYYMMddhhmmss.zip.

Exporting Multiple Filtered Objects

To export multiple filtered objects:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export**.

The **Bulk Export** page opens with a listing of exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the object type from the left pane (for example, **Policies**).
A list of configured objects of the specified type displays in the work area.
4. To include dependent objects in the export file, select **Include Dependencies**.
Any object dependencies for selected objects will also be selected for export.
5. To export a subset of objects, use the **Search** tool to search the list.
Note: The text box accepts the wildcard (%) and underscore (_) characters.
The list of objects is filtered to a subset of objects matching the search criteria.
6. Click **Add filtered items** to add all objects in the filtered list to the export cart.
A message displays indicating the objects has been successfully added to the export cart.
7. Repeat the search for other filter criteria.
8. Click the  to the right of the message to close the message.
9. Click **View Cart** or  to continue with the export.
The **Check out Page** opens.
10. Review the listing of objects.
11. To remove an object from the listing, use one of the following methods:
 - Click **Remove** next to the named object.
 - Select the check box next to the named object and click **Remove selected items**.
 - Use the **Search** tool to search the list for a specific string and click **Remove filtered items**.

Note: Any checked items will become unchecked if you change pages.

12. To view a filtered list of export objects by object type, click the **Type** list, select the object types, and click **Search**.
All of the selected object types are shown in the list.

Note: The remaining object types are still in the export cart. To view the entire contents, select **All** from the **Type** list and click **Search**.

13. After the export list of objects is complete, click **Export Cart**.
A warning message displays verifying that you want to export the select items in the shopping cart.
14. Click **OK** to proceed with the export.
15. Click **Clear Cart**.

The contents of the export cart are removed and you can proceed with another export.


A ZIP file is downloaded to your local computer. The filename uses the following naming convention:
CMP_export_YYYYMMddhhmmss.zip.

Exporting Configuration Object Groups


To export configuration object groups:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export**.
The **Bulk Export** page opens with a listing of exportable CMP object types in the left pane and a work area for selecting objects for export on the right.
3. Select the group object type from the left pane (for example, **Network Element Groups**).

A list of object groups are shown in the work area.

4. To include dependent objects in the export file, select **Include Dependencies**.
Any object dependencies for the selected group will also be selected for export.
5. For each group you want to export, click the check box next to the group Name.
6. Click **Add selected items** to add the selected groups to the export cart.
A message displays indicating the objects has been successfully added to the export cart.
7. Click the  to the right of the message to close the message.

Note: If **Include Dependencies** is checked, the total number of items in the export cart may exceed the number of items checked in the list.

8. Click **View Cart** or  to continue with the export.
The **Check out Page** opens.
9. Review the listing of objects.
10. To remove an object from the listing, use one of the following methods:
 - Click **Remove** next to the named object.
 - Select the check box next to the named object and click **Remove selected items**.
 - Use the **Search** tool to search the list for a specific string and click **Remove filtered items**.

11. To view a filtered list of export objects by object type, click the **Type** list, select the object types, and click **Search**.
All of the selected object types are shown in the list.

Note: The remaining object types are still in the export cart. To view the entire contents, select **All** from the **Type** list and click **Search**.

12. After the list of objects is ready, click **Export Cart**.
A warning message displays verifying that you want to export the select items in the shopping cart.
13. Click **OK** to proceed with the export.
14. Click **Clear Cart**.
The contents of the export cart are removed and you can proceed with another export.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention:
CMP_export_yyyyMMddhhmmss.zip.

Exporting All Configuration Objects

The **Export All** function exports a ZIP file to the local computer that contains all of the exportable types of configuration objects.

Note: **Export All** does not include associations between policies and MPE templates.

To export all configuration objects:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export All**.
The **Bulk Export** page appears.
3. Click **Export All**.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention:
CMP_export_yyyyMMddhhmmss.zip.

About the Manager Reports

The Manager Reports provides information about the CMP cluster itself. This information is similar to the Cluster Information Report for MPE and MRA clusters. The display is refreshed every ten seconds.

Viewing Manager Reports

To view Manager Reports:

1. From the **System Administration** section of the navigation pane, select **Reports**.
The **Manager Reports** page opens in the work area.
2. To manage the reports:
 - To pause refreshing the display, click **Pause**.
The report does not update every 10 seconds.
 - To resume refreshing the display, click **Resume**.
The report refreshes every 10 seconds.
 - To reset the display counters, such as blade failures, click **Reset All Counters**.
The counters in the report are reset to zero.

The fields that are displayed in the Manager Reports include the following:

- **Cluster Name and Designation** — The name of the cluster and whether it is the primary (**P**) or secondary (**S**) site.
- **Mode** — The status of the cluster:
 - **Active** – The cluster is managing the Policy Management network.
 - **Standby** – The cluster is not currently managing the Policy Management network.
 - **Paused** – The report is paused. Click **Resume** to return the **Mode** to **Active**.
- **Cluster Status** — The status of the servers within the cluster:
 - **On-line** – If one server, it is active; if two servers, one is active and one is standby.
 - **Degraded** – One server is active, but the other server is not available.
 - **Out-Of-Service** – Neither server is active.
 - **No Data** – The CMP system cannot reach the server.

Also within the Manager Reports is a listing of the **Blades** (that is, the servers) contained within the cluster. A symbol (➡) indicates which server currently has the external connection (that is, the active server). The report also lists the following server-specific information:

- **Overall** section — Displays the current topology:
 - **State** – (Active, Standby, or Forced Standby)
 - **Blade Failures** – counters
 - **Uptime** – the time providing active or standby service For the definitions of these states, see [Server Status](#).

- **Utilization** – Displays the current usage statistics:
 - **Disk** – percentage utilization of disk (of the `/var/camiant` file system)
 - **CPU** – average value for the CPU utilization
 - **Memory** – average value for Memory use

The **Actions** links let you **Restart** the CMP software on the server or **Reboot** the server.

Viewing the Trace Log

To view the Trace Log :

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* displays.

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** — When 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** — When 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. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search**.
The trace log for the selected server displays.
 4. To filter the log, see [Filtering the Trace Log](#).
 5. Click **Close**.

Filtering the Trace Log

The Trace Log can contain a large number of messages. To reduce the number, the log can be filtered using several criteria.

To filter the trace log information:

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 the data is being retrieved, the a progress message displays.
3. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search**.
The trace log for the selected server displays.
4. Specify the filtering parameters using any of the following fields.
 - **Start Date/Time** — Click , specify a date and time, and then click **Enter**.
 - **End Date/Time** — Click , specify a date and time, and then click **Enter**.
 - **Trace Codes** — Enter one or a comma-separated list of trace code IDs. Trace code IDs are integers 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.
 - **Contains** — Enter a text string to search. For example, if you enter **connection**, all events containing the word **connection** display. This field does not use wildcards and is not case specific.

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 in events last month and this month, only results from this month are listed.
5. Click **Search**.
The filtered log displays.
6. Click **Close**.
The **Trace Log Viewer** window closes.

Configuring the Trace Log

You can configure the trace log severity message levels for the CMP system.

To configure the trace log:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
The **Trace Log** page opens in the work area.
2. Click **Modify**.
The **Modify Trace Log Settings** page opens.
3. 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. 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** (default) — 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 log level setting from its default value (for example, from **Warn** to **Info**) causes more notifications to be recorded in the log and can adversely affect performance. Similarly, raising the log level setting (for example, from **Warn** to **Alert**) causes fewer notifications to be recorded in the log and may cause you to miss important notifications.

4. Click **Save**.

The trace log is configured.

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

The CMP lets you track and view configuration changes within the 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 view 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 43: Audit Log* shows an example.)

Audit Log

124 items found, displaying 1 to 20.
[First/Prev] 1, 2, 3, 4, 5, 6, 7 [Next/Last]

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 12:48:20	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	172.31.251.25	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	MRA - Reapply Config	MRA: mpe21-32 (10.15.20.150) - configuration was reloaded
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 reloaded
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: martin 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.

Refine Search

Figure 43: Audit Log

For a detailed description of an item, click the underlined description. The details of the event display. (*Figure 44: 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 - Q2 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 - Q2 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: mmospn.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmospn.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 44: Audit Log Details

Searching for Audit Log Entries

To search for the Audit Log entries:

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** — Click  (calendar icon), specify a date and time then click **Enter**.
 - **Action by User Name(s)** — Enter the **User Name** of the user or users to audit.
 - **Action on Policy Server(s)** — Enter the name of the Policy Management device to audit.
 - **Audit Log Items to Show** — Specifies the category of items to audit:
 1. When you select some categories, a **Name** field displays, which lets you enter a search string.
 2. Leave the **Name** field blank to include all items.
 3. When you select a category, an **Actions** link displays, 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 audit log item category.

- **Results Forms** — Specifies the number of items per page to display, including which data to display (most recent or oldest items).

4. Click **Search**.
The Audit Log displays search results.


Exporting or Purging Audit Log Data

You can export the audit log to a text file; the default file name is `AuditLogExport.txt`.

Exporting Audit Log Data

You can export audit log data to a text file. The file name is `AuditLogExport.txt`.


To export audit log data:

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. 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. 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,

reschedule, enable or disable 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 \(MOS\)](#) before changing the order of task execution.

The tasks include:

- | | |
|--|--|
| Alert Aging | Ensures that alerts age out and are eventually removed from the CMP database. (The valid range is 1 to 365 days.) |
| Stats Files Synchronization #1, 2, 3, 4 | <p>Synchronizes stats files to defined remote server. Up to four synchronization tasks can be defined, and they are scheduled independently. Statistics files are generated and synchronized to external systems only from the active CMP system. This task retries when the remote server is unreachable. The default number of retries is three times in each one minute interval. The maximum number of retries in one minute is five times. If a transfer period is missed, the next time the remote server is reached any files from the missed transfer periods are transferred. Remote server information that must be defined before this task runs is: Host Name/IP address, Remote repository path, and SSH user login and password.</p> <p>Note: An external system must be configured before beginning this task. If no external system is configured in any of the Stats File Synchronization tasks, no stats files are generated.</p> <p>Note: If access to configuration is restricted to Read-Only, you will not be able to configure this task.</p> |
| Health Checker | Periodically checks the MPE devices to ensure that they are online. |
| OM Statistics | <p>Periodically retrieves Operational Measurement (OM) statistics from all MPE devices. The Operational Measurements XML interface retrieves operational counters from the system. The OM interface requires that the OM Statistics scheduled task be running on the CMP system. After the specified Stats Collection Period, this task collects the operational counters from the Policy Management devices in the network and records them in the CMP database; the data is then available for query via the OM XML interface. You can configure the task to poll at intervals between 5 minutes and 24 hours, with a default value of 15 minutes; the system keeps the data available for query for 1 to 30 days, with a default value of 7 days. The recommended settings for this task will vary depending on the volume of data you are collecting.</p> <p>When you request OM statistics, the data for the response is taken from the information that has been collected by this task. You must gather data using the OM Statistics scheduled task if you want data available for subsequent OM queries. Most values returned as part of the response are presented as the positive change between the start time and end time. To calculate a response, you must have a minimum of two recorded values available; thus you must run the OM Statistics task at least twice in a given time period before you can obtain any statistical data from the OSSI XML interface. <i>OSSI XML Interface Definitions Reference</i> describes the OM Interface and the OM Statistics in detail.</p> <p>Stats File Generator Generates statistics files by extracting the data from the CMP database using the OSSI XML interface. This task is also responsible for cleaning up the statistics files. The available settings for this task are:</p> |

Local Repository directory (the default is `/var/camiant/stats_export`); Maximum age to keep files, in hours (default is 72 hours); File Format, either XML (default) or CSV; and Stats Type, which lets you select the statistics groups to extract. For information on the individual statistics in each available group, see *OSSI XML Interface Definitions Reference*.

Legacy OM Statistics	Periodically retrieves OM statistics from MPE devices executing the previous release of Policy Management software. This task should be run only during migration between software releases.
Replication Statistics	Generates replication statistics for MPE and MRA servers. Note: The run interval should be the same as the Stats Collection Period. For more information, see Setting Stats Settings .

Configuring a Scheduled 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 showing the settings for the available scheduled tasks.
2. Click **Refresh** to update the page.
3. To configure a scheduled task, click the task name. The page displays the current settings and status for the selected scheduled task.
4. Click **Settings**.

Note: The **Health Checker** task has no configurable settings.

5. To configure a **Stats File Synchronizations** task (maximum of 4) for CMP to store copies of stats files to a remote external system:
 - a) Enter the **Host Name / IP Address** for the remote server.
You can use either the FQDN or IP address (either IPv4 or IPv6 format).
 - b) Enter the **SSH User Name** required to access the remote server.
 - c) Enter the **SSH Password**.
 - d) Enter the **Path of Remote Repository** for storing the stats files.
 - e) Enter the **Retry Limit** for the number of times to retry synchronizing the stats files (default is 3 with a maximum of 5) if the remote server is unreachable.
6. To configure the **OM Statistics** or **Replication Statistics** task:
 - a) Enter the **Number of days to keep statistical data**.
This is the number of days to retain the specified statistics file. The valid range is from 1 to 30 days with a default of seven days.
7. To configure the **Stats Files Generator**:
 - a) Enter the path for the **Local Repository**.
This is the path on the external server where stats files are replicated. The default repository's root directory is `/var/camiant/stats_export`. Two levels of subdirectories will be created under this root directory. An MPE or MRA cluster will have a corresponding first level

subdirectory. Each stats file type will have its own subdirectory under the cluster-level directory. All the stats files will be created under the stats type subdirectory.

- b) Enter the **Maximum age to keep files (hours)**.

The default is 72 hours.

- c) Select the **File Format** from the list.

Available formats are **CSV** or **XML** (default).

- d) Select the **Stats Type** from the list:

See [Generated Statistics](#) for a list of available statistics.

- Click **Select All** to have the generator collect statistics for all stats types.
- Click **Inverse All** to deselect any selected stats types and select any unselected stats types.
- Select each individual stats types.

8. Click **Save**.

The scheduled task is configured.

Rescheduling a Task

To reschedule a scheduled task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.
The **Scheduled Task Administration** page opens showing the settings for the available scheduled tasks.
2. To configure a scheduled task, click the task name.
The page displays the current settings and status for the selected scheduled task.
3. Click **Reschedule**.
The reschedule configuration settings appear.
4. To **Schedule by Interval**:
 - a) Select the date and time for the **Next Run Time**.
 - b) For the Run Interval, select the **Hours** or **Minutes**.
Valid intervals are from 0 to 24 hours in 5-minute increments.
5. To schedule the task **Following Another Task**, select the **Task to Follow** from the list.
6. Click **Save**.

The scheduled task is rescheduled.

Enabling or Disabling a Scheduled Task

To enable or disable an individual task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.
The **Scheduled Task Administration** page opens showing the settings for the available scheduled tasks.
2. To configure a scheduled task, click the task name.
The page displays the current settings and status for the selected scheduled task.
3. To disable an enabled task, click **Disable**.

The scheduled task is disabled and the button text changes to **Enable**.

4. To enable a disabled task, click **Enable**.

The scheduled task is enabled and statistics files will be generated based on the task's configuration settings. The button text changes to **Disable**.

5. Click **OK** to acknowledge the change.

The specified task is disabled or enabled.

About Managing Users

The CMP system lets you configure the following user attributes:

Roles	Determines the actions (and the access level) a user can perform within the CMP system. See About User Roles for details.
Scopes	Determines the network element groups and Policy Management device groups a user can perform actions on and providing a context for a role. See About User Scopes for details.
Users	After you define roles and scopes, you can assign them to user profiles. See About User Profiles for details.
External Authentication	Enables the CMP system to authenticate users using either RADIUS or SANE Authentication. These users must match the RADIUS Server account information before access is permitted. See About External Authentication for details.

Creating a Customer User Management System Profile

To support identity management (IDM), the CMP system can accept HTTP or HTTPS connection requests from an external Customer User Management system to create, update, query, and delete user profiles. Requests and responses consist of XML documents.

For more information on the XML application programming interface, see *OSSI XML Interface Definitions Reference*.

To create a user profile for an external Customer User Management system:

1. Create a user profile as described in [Creating a User Profile](#).
2. Assign the user profile a **Role** that includes the following privileges:
 - **Show** access for **Import/Export** privilege
 - **Read-Write** access for **User Management** privilege
3. Assign the user profile to the default **Global** scope.
4. Click **Save**.

The user profile for the Customer User Management System is saved.

About User Roles

The CMP system uses roles to configure what a user can do within the CMP system. Assigning roles to the various users that access the CMP system lets you control who can configure and access features within the CMP system. The default roles are:

Administrator	Permits full read/write access to all functions. You cannot delete the Administrator role.
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 Management .
Viewer	Permits read-only access to functions associated with Policy Management device management and configuration. Full access is also permitted to some of the system administration functions, such as Change Password.

The CMP system allows you to perform the following role management actions:

- [Creating a Role](#)
- [Modifying a Role](#)
- [Deleting a 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.
3. Click **Create Role**.
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).
The **New Role** page opens.
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**
 - **Configuration Template**
 - **Applications**
 - **Match Lists**
 - **Quota Profiles & Conventions**
 - **Services & Rating Groups**

- Policy Counter ID
 - Traffic Profiles
 - Roaming Profile
 - Protocol Timer Profile
 - Retry Profiles
 - Charging Servers
 - Time Periods
 - Monitoring Key
 - Serving Gateway/MCC-MNC Mapping
 - Custom AVP Definitions
 - Custom VSA Definitions
 - Customer Vendor
 - Notification Server
 - Global Configuration Settings
 - Bulk Operation
7. **Subscriber Privileges** — Defines access to the subscriber functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
 - Entitlements
 - Tiers
 - Quota Usage
 8. **SPR Privileges** — Defines access to the SPR functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
 - Subscriber Data
 9. **Network Privileges** — Defines access to the network management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
 - Network Elements
 - Topology (not supported)
 10. **MRA Privileges** — Defines access to the MRA Configuration functions:
 - Configuration (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - Bulk Operations (with the access **Hide** or **Show**)
 - Configuration Template
 11. **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**)
 - Policy Checkpoint (with the access **Hide**, **Read-Only**, or **Read-Write**)
 12. **System Wide Reports Privileges** — Defines access to the system-wide reports functions:
 - System Wide Reports Configuration (with the access **Hide**, **Read-Only**, or **Read-Write**)
 13. **Platform Setting Privileges** — Defines access to the platform setting functions:

- **Platform Configuration Setting** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **Topology Settings** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **SNMP Settings** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **Server Operation** (with the access **Hide** or **Read-Write**)
14. **Upgrade Manager Privileges** — Defines access to software upgrade functions:
- **ISO Maintenance** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **Upgrade Manager** (with the access **Hide**, **Read-Only**, or **Read-Write**)
15. **System Administration Privileges** — Defines access to system administration functions:
- **Import / Export** (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 CMP** (with the access **Hide**, **Read-Only**, or **Read-Write**)
 - **Subscriber Activity Log** (with the access **Hide**, **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**)

New tasks are created to synchronize stats files. These tasks perform a retry if a remote server is unreachable. The following fields are displayed for the Stats Files Synchronization setting:

- **Remove Server Information**
 - **Host Name/IP Address**
 - **User Name**
 - **Password**
 - **Path of Remote Repository**
- **Retry Limit** — You have a limit of three retries in one-minute intervals.

16. Click **Save**.

The role is created.

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.
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

Note: You can delete any role except the **Administrator** role.

You cannot delete a role that is in use. You must remove any users assigned to the role before deleting it.

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.
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.

About User Scopes

The CMP system uses scopes to define the network element groups and Policy Management device groups that a user can access which provides operational context for a role.

Note: You can assign a user more than one scope.

The CMP system allows you to perform the following scope management actions:

- [Creating a Scope for CMP Servers](#)
- [Creating a Scope for Multilevel CMP Servers](#)
- [Modifying a Scope](#)
- [Deleting a Scope](#)

Creating a Scope for CMP Servers

Note: This procedure applies to non-tiered CMP servers. See [Creating a Scope for Multilevel CMP Servers](#)

Scopes allow you to control what areas or devices in a network a user can manage. The default scope, **Global**, contains all items defined within the CMP database. After you define a scope you can assign it to users.

To create 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, select **Scopes**.
The **Scope Administration** page opens in the work area.
3. Click **Create Scope**.
The **New Scope** page opens.
4. Enter the **Name**
The name for the scope can contain 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. Select the **MRA Groups** included in this scope.
9. Click **Save**.

The scope is created.

Creating a Scope for Multilevel CMP Servers

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, select **Scopes**.
The **Scope Administration** page opens in the work area.
3. Select the scope you want to modify.
The scope configuration appears.
4. Click **Modify**.
The **Modify Scope** page opens.

Note: See [Creating a Scope for CMP Servers](#) for descriptions of the fields on this page.
5. Modify the scope as needed.
6. Click **Save**.


The scope is modified.

Deleting a Scope

Note: You cannot delete the **Global** scope.

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, select **Scopes**.
The **Scope Administration** page opens in the work area.
3. Delete the scope using one of the following methods:
 - From the work area, click  (Delete icon) located to the right of the scope you want to delete.
 - From the content tree, select the scope to delete and click **Delete**.

A confirmation message appears.
4. Click **OK**.
The scope is deleted.

About User Profiles

The User Management functions include the tools necessary to create, modify, or delete user profiles. A user profile defines a user with a role and one or more scopes.

The CMP system is configured initially with the following default user profiles and passwords:

- **admin/policies** (you cannot delete this profile)

Note: Oracle recommends changing the password after your first log in to the CMP system.

- **operator/policies**
- **viewer/policies**

The **admin** user is the only profile that cannot be deleted or have its username modified. The **admin** user is the only user who can create, modify, or delete other users, as well as log off all users.

Note: When logging in, the username is not case sensitive; however, the password is case sensitive.

The CMP system allows you to perform the following user management actions:

- [Creating a User Profile](#)
- [Modifying a User Profile](#)
- [Deleting a User Profile](#)

Creating a User Profile

Note: See [Creating a Customer User Management System Profile](#) for details on creating a user profile for a Customer User Management System.

To create 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, select **Users**.
The **User Administration** page opens in the work area.
Note: The **Log Out All Users** button is visible only to the **admin** user.
4. Click **Create User**.
The **New User** page opens.
5. Enter the **Username**.

The name can use up to 64 characters.

Note: This value is not case sensitive.

6. Enter a **Description/Location** (optional).
Free-form text.
7. Enter the **Password**.
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. See [Changing a Password](#) for details on configuring password strength rules.
8. Enter to **Confirm Password** the **Password**.
9. Enter the number of days for the **Password Expiration Period(days; 0=never)**.
Enter a value from **7** to **365**, or **0** to indicate that the password never expires. The default value is the system setting.

Note: This setting overrides the system setting. See [Changing a Password](#) for details on configuring password system settings.
10. Select to **Force to Change Password**.
If selected, this user must change passwords during the next log in. The default value is enabled.
11. Select a **Role** from the list.
12. Select one or more **Scopes** to assign to the user profile.
13. Click **Save**.

The user profile is created.

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, select **Users**.
The **User Administration** page opens in the work area.
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

Note: You cannot delete the **admin** user profile.

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, select **Users**.
The **User Administration** page opens in the work area.
4. Delete the user profile using one of the following methods:
 - From the work area, select  (Delete icon) located to the right of the profile.
 - From the content tree, select the user profile and click **Delete**.

A confirmation message displays.

5. Click **OK**.

The user profile is deleted.

About Locking and Unlocking User Profiles

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** user cannot lock the **admin** user.

The CMP system allows you to perform the following actions:

- [Locking a User](#)
- [Unlocking a User](#)

Locking a User

To lock 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, select **Users**.
The **User Administration** page opens in the work area.
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 user profile 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 a User

To unlock 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, select **Users**.
The **User Administration** page opens in the work area.
4. Select the user profile from the content tree.
The **User Administration** page opens.
5. Click **Unlock**.
A confirmation message appears.
6. Click **OK**.
 - The user profile 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`.

Logging Out All Users

Note: Only the **admin** user can log out all users that are currently logged in to the CMP system. The **admin** user will not be logged out.

To log out all users:

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, select **Users**.
The **User Administration** page opens in the work area.
4. Click **Log Out All Users**.
A confirmation message appears.
5. Click **OK**.

Logged in users are logged out from the CMP system.

About External Authentication

In addition to the built-in authentication functions, you can configure external authentication, RADIUS authentication, and SANE authentication of CMP users.

In the CMP system, you can manage the RADIUS Authentication and Account or the SANE Authentication external authentication method.

RADIUS Authentication and Accounting

The CMP system supports RADIUS authentication and accounting. You can configure the CMP system to operate in a network environment including multiple authentication servers, one authentication server, or no servers. If both primary and secondary authentication servers are defined, the authentication process is as follows:

1. The CMP system contacts the primary RADIUS server.
If it responds with Accept or Reject, that action is followed.
2. If the primary server does not respond within a specified number of retries or before a timeout value, the CMP system contacts the secondary RADIUS server (if defined).
If it responds with Accept or Reject, that action is followed.
3. If the secondary server does not respond, the CMP system authenticates against its local database (if enabled).
4. If local authentication is not enabled, authentication fails.
5. The user **admin** is always authenticated locally, regardless of configuration settings.

This process provides a fail-safe mechanism for accessing the CMP system even in the face of misconfiguration or network problems that cause the RADIUS servers to become inaccessible.

RADIUS configuration involves three steps:

1. [About Configuring the RADIUS Server](#) to accept authentication (and accounting, if used)
2. [About Defining CMP Users to the RADIUS Server](#) and [Associating Roles and Scopes](#) on the CMP system
3. [About Defining the CMP System as a RADIUS Client](#) to work with RADIUS

About Configuring the RADIUS Server

The RADIUS servers must be configured to authenticate clients and users on the CMP system. Some of the configuration values must be consistent with configuration parameters on the CMP system. (The RADIUS administrator is aware of the names and locations of the configuration files.)

See [Enabling and Configuring RADIUS on the CMP System](#) for details.

About Defining the CMP System as a RADIUS Client

The client file identifies the systems that use the RADIUS server to authenticate user access. A client should be defined as a single device. For example:

```
client 10.0.10.22 {
    secret = example
    shortname = MPE5
}
client 10.0.10.23 {
    secret = example
    shortname = CMP56
}
```

The best practice is to define IP addresses rather than FQDNs. If a netmask is not given, the default is /32. The shared `secret` (in this example, **example**) must be defined on both the RADIUS server and entered into the CMP configuration (see [Enabling and Configuring RADIUS on the CMP System](#)). The `shortname` is used as an alias.

If multiple IP addresses are configured on the CMP system (such as SIG-A and SIG-B), use the IP address that would be used as the Source IP address of RADIUS requests sent to the RADIUS server.

About Defining CMP Users to the RADIUS Server

The RADIUS server can use either a database or a simple flat file as its repository of user information. The following example uses a flat file to demonstrate a minimum user configuration. The users file contains authentication and configuration information for each user. It begins with the username and

the authentication (that is, the password) that is required from the user. The user/password line is followed by indented lines that are attributes to be passed back to the requesting server.

```
Jeff      Cleartext-Password:="garbage"
          Class="Administrator",
          Oracle-MI-role="Administrator",
          Oracle-MI-scope="Global"

Paul      Cleartext-Password:="apr6279"
          Class="Viewer",
          Oracle-MI-role="Viewer",
          Oracle-MI-scope="Global"
```

Figure 45: Sample RADIUS User Information Flat File

When the RADIUS server has authenticated a user, it sends back various attributes with the authentication acceptance message. The CMP system uses these attributes to determine what actions the user can perform.

The best practice is to use a vendor-specific attribute (VSA) dictionary file to define what attributes to send back to the client. [Figure 46: Sample VSA Dictionary File For RADIUS](#) shows a sample file. The local RADIUS administrator is responsible for incorporating the VSA dictionary file onto the RADIUS server.

```
===== dictionary.oracle =====
# Oracle Communications VSA's, from RFC 2548
# The filename given here should be an absolute path.
#
# Place additional attributes or $INCLUDEs here.

VENDOR Oracle 21274
BEGIN-VENDOR Oracle
ATTRIBUTE Oracle-MI-role 1 string
ATTRIBUTE Oracle-MI-scope 3 string
END-VENDOR Oracle
=====
```

Figure 46: Sample VSA Dictionary File For RADIUS

The attributes **Oracle-MI-role** and **Oracle-MI-scope** are for access to the CMP system. Both a scope and a role are associated with a user. The responses sent back from the RADIUS server should match what is configured in the CMP system. The defaults for the role, in ascending order of capability, are **Viewer**, **Operator**, and **Administrator**, but the system administrator can create other roles or remove any role except that of **Administrator**.

The default scope is **Global**, and the administrator can create other scopes within the CMP system.

Associating Roles and Scopes

The CMP system assigns two attributes to a user, a role and a scope. Users that authenticate against a RADIUS server are assigned roles and scopes by matching against the attribute values returned by the RADIUS server.

It is easiest to provide role and scope values using the VSA dictionary, by defining the attributes **Oracle-MI-role** and **Oracle-MI-scope**. The flexibility of roles and scopes can be supported by RADIUS if the VSA dictionary is integrated.

The following example defines users who have access at different role levels:

```
Jeff      Cleartext-Password:="garbage"
          Class="Administrator",
          Oracle-MI-role="Administrator",
          Oracle-MI-scope="Global"

Paul      Cleartext-Password:="apr6279"
          Class="Viewer",
          Oracle-MI-role="Viewer",
          Oracle-MI-scope="Global"
```

However, if Oracle VSAs are not included in the RADIUS dictionary, then they cannot be defined in the user file, and only a **Class** attribute can be returned on a RADIUS authentication. The CMP system can use the Class attribute for RADIUS authentication.

To accept the Class attribute for CMP login, define a scope and a role that matches what the RADIUS server returns as the Class attribute. The CMP system uses the Class attribute for both required credentials. For example, consider this user defined in RADIUS:

```
Dawn      Cleartext-Password:="kkmk4813"
          Class="Viewer"
```

Dawn can get access to the CMP system if you have defined both a role named Viewer and a scope named Viewer; the GUI matches the one returned value to both of the required credentials.

Enabling and Configuring RADIUS on the CMP System

By default, RADIUS Authentication is disabled in the CMP system. Enabling authentication requires admin privileges. The **admin** user is always authenticated against the local database record; thus, the **admin** user is best suited to setting up RADIUS authentication (see [Creating a User Profile](#)).

Two configuration parameters must match with the configuration that was put on the RADIUS server:

- **Source of User Credentials** must match up with the user configuration in the RADIUS server, but this will also depend on what is configured in the next parameter.
- If **Action if missing credentials** is set to **Use following defaults**, then a user will be authenticated as long as the password is correct. This user could log in even though the Class is not valid:

Figure 47: Sample User for RADIUS Server

```
test      Cleartext-Password := "2931txy"
          Class = "noone"
```

- If **Action if missing credentials** is set to **Reject**, then the configuration of the user will depend on the configuration of **Source of User Credentials**.

To enable RADIUS authentication and accounting:

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. From the content tree, select **External Authentication**. The **External Authentication** page opens. By default, external authentication is disabled.

4. Click **Modify**.
The **External Authentication** page becomes editable.
5. In the **Configuration** section, select **Enable RADIUS Authentication**.
Configuration and RADIUS Services configuration fields appear.
6. Select to **Enable RADIUS Accounting**.
This feature is disabled by default. When enabled, the CMP system sends an Accounting-Start message to the accounting server when a user logs in, and an Accounting-Stop message when the user logs out. These messages contain a session ID attribute that uniquely identifies the user session so that it can be matched between Start and Stop.
7. Select the **Destination for Accounting Messages** from the list.
Available options include:
 - **Both Primary and Secondary** (default) — Specifies that accounting messages generated for each user session are sent to both the primary and (when configured) secondary RADIUS servers.
 - **Primary (Secondary on error)** — Accounting messages are sent only to the primary server, as long as it is reachable. If the primary accounting server is unreachable, messages are sent to the secondary accounting server.
8. Enter the **NAS IP Address** (required).
The IP address, in IPv4 or IPv6 format, of the network access server. By default, this is the local host address.
9. Select when to **Use local authentication** from the list.
Available options include:
 - **When RADIUS servers timeout** (default)
 - **When both RADIUS servers timeout or reject**
 - **Never**

Note: Fallback to local authentication is never used. However, the **admin** user is always authenticated locally.
10. Select the **Source of User Credentials** from the list.
Available options include:
 - **RADIUS Class** — The value of the `Class` attribute returned by the server determines both the role and scope.
 - **Oracle VSAs** — The value of Oracle VSAs returned by the server determines the role and scope.
11. Select an **Action if Missing Credentials**.
Available options include:
 - **Reject** — If you select this option, a user whose login credentials are missing is not logged in.
 - **Use following defaults** — Select a setting for each of the following attributes:
 - **Default Role** — The role assigned if the user credentials are missing or mismatched. The default role is **Viewer**.
 - **Default Scope** — The scope assigned if the user credentials are missing or mismatched. The default scope is **Global**.
12. In the **RADIUS Services** section, edit the following fields:

a) Configure the **Primary RADIUS Authentication Server**:

- **Server** — The FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary authentication server.

Note: To disable the primary server, delete its IP address.

- **Port** — The IP port number of the primary server. The default value is port 1812.
- **Timeout (seconds)** — The length of time the CMP system waits for a response from the server. The default value is 3 seconds.
- **Retries** — The number of times the CMP system tries to send a message to the server. The default value is 3 times.
- **Shared Secret** — A password-like string that must exactly match between the CMP system and the `secret` attribute configured in the entry for this CMP system in the `clients.conf` file in the RADIUS server.

Note: If the two values do not match, the server ignores all messages from the CMP system.

b) Configure the **Secondary RADIUS Authentication Server**:

If configured, the secondary authentication server uses the same fields as the primary authentication server.

c) Configure the **Primary RADIUS Accounting Server**:

- **Server** — The FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary accounting server.
- **Port** — The IP port number of the Primary RADIUS Accounting server. The default value is port 1813.
- **Timeout (seconds)** — The length of time the CMP system waits for a response from the server. The default value is 3 seconds.
- **Retries** — The number of times the CMP system tries to send a message to the server. The default value is 3 times.
- **Shared Secret** — A password-like string that must exactly match between the CMP system and the `secret` attribute configured in the entry for this CMP system in the `clients.conf` file in the RADIUS server.

Note: If the two values do not match, the server ignores all messages from the CMP system.

d) **Secondary RADIUS Accounting Server**

If configured, the secondary accounting server uses the same fields as the primary accounting server.

13. Click Save.

RADIUS Authentication and Accounting is configured.

SANE Authentication

The CMP system supports Secure Access to Network Elements (SANE) authentication and authorization. You can configure the CMP system to operate in a SANE network environment such that a user elsewhere in the network can gain single sign-on (SSO) access. When the CMP system is configured to authenticate using SANE, users can log in using a SANE client. (Usage of a SANE client is outside the scope of this document.) See [Enabling SANE Authentication on the CMP System](#) for details.

The **admin** account is treated separately. An admin user enters the CMP URL in any supported browser to log in.

The authentication process is as follows:

1. From a SANE client GUI, the user selects the CMP system. A web browser session is launched. An encrypted SANE authentication artifact is sent to the CMP system through the browser.
2. The CMP system forwards the artifact to a SANE server (the SANE responder).
3. If the SANE server verifies the artifact, it returns an assigned role and scope for the user, and the CMP system allows the user to log in accordingly. Otherwise, the CMP system rejects the login request.
4. The user **admin** is always authenticated locally, regardless of configuration settings. (That user clicks on the **Login** link.)

Enabling SANE Authentication on the CMP System

By default, SANE Authentication is disabled in the CMP system. Enabling authentication requires **admin** privileges. The user **admin** is always authenticated against the local database account; thus, the **admin** user is best suited to setting up SANE authentication (see [Creating a User Profile](#)).

To enable SANE authentication:

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. From the content tree, select **External Authentication**. The **External Authentication** page opens, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**. The **External Authentication** page becomes editable.
5. In the **Configuration** section, select **Enable SANE Authentication**. Configuration and SANE Servers configuration fields appear.
6. Enter the **Artifact Parameter Name**. The name of the artifact parameter. Enter an alphanumeric string. The default value is **artifact**.
7. Select the **Verification for Account** setting from the list. Available options are:
 - **On login only** (default) — The CMP system authenticates the user once on login. The user is considered authenticated until logout.
 - **On each request** — The CMP system authenticates the user on login, and then for each HTTP or HTTPS request. If any request is not authenticated, the user is immediately logged out.
8. Select the **Action if Missing Credentials**. The available options are:
 - **Reject** — If you select this option, a user login is rejected even if the authentication is successful.
 - **Use following defaults** — If you select this option, a user with missing credentials is allowed to log in, but the system assigns a default role and scope:
 - **Default Role** — Default role assigned to the user. The default role is **Viewer**.
 - **Default Scope** — Default scope assigned to the user. The default scope is **Global**.

9. In the **SANE Servers** section, enter the **SAML Service Name**.

The name of the Security Assertion Markup Language service registered with the UDDI server.
Enter an alphanumeric string.

10. Enter the **UDDI Inquiry URL**.

The Universal Description, Discovery and Integration URL, in HTTP or HTTPS format, for the inquiry.

11. Click **Save**.

SANE authentication is enabled.

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.

If the system administrator has configured your account for password expiration, you will receive a warning when you log in that you must change your password.

Note: To reset the administrator password, contact [My Oracle Support \(MOS\)](#).

To change a 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 your **Current Password**.
3. Enter your **New Password**.
4. Re-enter your new password to **Confirm Password**.

Note: If your new password does not conform to the password strength rules, a validation error message appears that includes valid password criteria. Enter and confirm another password that conforms to the criteria.

5. Click **Change Password**.

Your password is changed.

Appendix

A

CMP Modes

Topics:

- [About Mode Settings.....369](#)

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.

About Mode Settings

When you use a web browser to connect to a CMP system after the software is first installed, the **Mode Settings** page opens ([Figure 48: Mode Settings Page](#)). Select the needed modes, functions, and management options for your installation 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.

Restriction



Important: Options marked as **Restricted** are for use within specific environments and should not be enabled without authorization. For more information about the restricted function or feature, call My Oracle Support.

Modes and Functions

The following modes and functions available are:

Cable Enables support of a cable carrier environment.

Note: If Cable Mode is enabled, you must also enable **Manage Direct Link**.

Functions are described in the *Configuration Management Platform Cable User's Guide*.

Cable functions include:

PCMM Supports PacketCable MultiMedia functions.

DQOS Supports Dynamic Quality of Service functions.

Note: This function is restricted. See [Restriction](#) for more information.

Diameter AF Supports Diameter AF functions.

Wireless Enables support of a wireless carrier environment.

Wireless functions include:

Diameter 3GPP Supports Diameter 3GPP protocol.

Diameter 3GPP2 Supports Diameter 3GPP2 protocol.

Note: This function is restricted. See [Restriction](#) for more information.

PCC Extensions Supports Policy and Charging Control functions.

Note: This function is restricted. See [Restriction](#) for more information.

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.

Note: This function is restricted. See [Restriction](#) for more information.

LI	Supports Lawful Intercept functions. Described in the <i>Configuring Lawful Intercept Application Note</i> . Note: This function is restricted. See Restriction for more information.
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. Note: This function is restricted. See Restriction for more information.
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. Note: This function is restricted. See Restriction for more information.
Cisco Gx	Supports the Cisco Gx protocol. Note: This function is restricted. See Restriction for more information.
DSR	Supports Policy Management network segmentation using a Oracle Communications Diameter Signaling Router (DSR). Note: This function is restricted. See Restriction for more information.
SMS	Enables support of SMS servers.. SMS Mode functions include: SMPP Supports SMS using SMPP protocol. XML Supports SMS using XML. Note: This function is restricted. See Restriction for more information.
SPR	Enables support of subscriber database management. Select only one sub-mode. Functions are described in the Subscriber Data Management documentation. SPR Mode functions include: Subscriber Profiles Supports subscriber profile functions. Note: This function is restricted. See Restriction for more information. Quota Supports subscriber quotas. Note: This function is restricted. See Restriction for more information.
Wireline	Enables support of a wireline carrier environment. Functions are described in the <i>Configuration Management Platform Wireline User's Guide</i> . Note: This function is restricted. See Restriction for more information.
SPC	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> .

Note: This function is restricted. See [Restriction](#) for more information.

RADIUS Enables support of RADIUS Authentication, Authorization, and Accounting (AAA).

Note: This function is restricted. See [Restriction](#) for more information.

BoD Mode Enables the Bandwidth on Demand Application Manager (BoD-AM), which support video on demand (VoD) servers. Functions are described in the *Bandwidth on Demand Application Manager Cable User's Guide*.

PCMM Supports a network creating PacketCable Multimedia (PCMM) sessions.

Diameter Supports a network creating Diameter sessions.

Note: This function is restricted. See [Restriction](#) for more information.

RDR Supports a network containing Service Control Engine (SCE) devices transmitting Raw Data Records (RDRs).

Note: This function is restricted. See [Restriction](#) for more information.

Server Management Options

The management options for servers are:

Manage Policy Servers	Manages MPE devices.
Manage MA Servers	Manages Management Agent servers.
Manage Policies	Enables the Policy Wizard.
Manage MRAs	Manages Multi-Protocol Routing Agent servers.
Manage SPR Subscriber Data	Manages Subscriber Profile Repository servers.
Manage Geo-Redundant MPE/MRA/BoD	Manages georedundant MPE, MRA, or BoD clusters.
Manager is HA (clustered)	Enables High Availability features.
Manage Analytic Data	Enables output of policy event records.
Manage Direct Link	If enabled, all replication and HA transmissions go through the backplane interface; if disabled, all replication and HA transmissions go through the OAM interface. Note: This function is restricted. See Restriction for more information.
Manager is NW-CMP	Enable Network mode in a tiered CMP system. See Network Configuration Management Platform for more information. Note: This function is restricted. See Restriction for more information.
Manager is S-CMP	Enable System mode in a tiered CMP system. See Network Configuration Management Platform for more information. Note: This function is restricted. See Restriction for more information.

Mode Settings

Important: Options marked as **Restricted are for use within specific environments and should not be enabled without authorization.#**

Mode

Cable		
PCMM		<input type="checkbox"/>
DQOS (Restricted)		<input type="checkbox"/>
Diameter AF		<input type="checkbox"/>
Wireless		
Diameter 3GPP		<input checked="" type="checkbox"/>
Diameter 3GPP2 (Restricted)		<input type="checkbox"/>
PCC Extensions (Restricted)		<input type="checkbox"/>
Quotas Gx		<input checked="" type="checkbox"/>
Quotas Gy (Restricted)		<input checked="" type="checkbox"/>
LI (Restricted)		<input type="checkbox"/>
SCE-Gx (Restricted)		<input type="checkbox"/>
Gx-Lite (Restricted)		<input checked="" type="checkbox"/>
Cisco Gx (Restricted)		<input type="checkbox"/>
DSR (Restricted)		<input type="checkbox"/>
SMS		
SMPP		<input checked="" type="checkbox"/>
XML (Restricted)		<input type="checkbox"/>
SPR		
Subscriber Profiles (Restricted)		<input type="checkbox"/>
Quota (Restricted)		<input type="checkbox"/>
Wireline (Restricted)		<input type="checkbox"/>
SPC (Restricted)		<input type="checkbox"/>
RADIUS (Restricted)		<input checked="" type="checkbox"/>
BoD		
PCMM		<input type="checkbox"/>
Diameter (Restricted)		<input type="checkbox"/>
RDR (Restricted)		<input type="checkbox"/>

Manage Policy Servers	<input checked="" type="checkbox"/>
Manage MA Servers	<input type="checkbox"/>
Manage Policies	<input checked="" type="checkbox"/>
Manage MRAs	<input checked="" type="checkbox"/>
Manage BoDs	<input type="checkbox"/>
Manage SPR Subscriber Data	<input checked="" type="checkbox"/>
Manage Geo-Redundant MPE/MRA/BoD	<input type="checkbox"/>
Manager is HA (clustered)	<input checked="" type="checkbox"/>
Manage Analytic Data	<input checked="" type="checkbox"/>
Manage Direct Link	<input type="checkbox"/>
Manager is NW-CMP (Restricted)	<input type="checkbox"/>
Manager is S-CMP (Restricted)	<input type="checkbox"/>

Figure 48: Mode Settings Page

Appendix B

Generated Statistics

Topics:

- [List of Generated Statistics.....374](#)

This appendix lists the available statistics for generated scheduled tasks.

List of Generated Statistics

The following is a list of generated statistics available for scheduled tasks:

- DiameterPcefStats
- DiameterPcefPeerStats
- DiameterCTFStats
- DiameterCTFPeerStats
- DiameterBberfStats
- DiameterBberfPeerStats
- DiameterAfStats
- DiameterAfPeerStats
- DiameterShStats
- DiameterShPeerStats
- DiameterSyStats
- DiameterSyPeerStats
- DiameterTdfStats
- DiameterTdfPeerStats
- DiameterDrmaStats
- DiameterDrmaPeerStats
- DiameterPcefLatencyStats
- DiameterPcefPeerLatencyStats
- DiameterBberfLatencyStats
- DiameterBberfPeerLatencyStats
- DiameterAfLatencyStats
- DiameterAfPeerLatencyStats
- DiameterShLatencyStats
- DiameterShPeerLatencyStats
- DiameterSyLatencyStats
- DiameterSyPeerLatencyStats
- DiameterTdfLatencyStats
- DiameterTdfPeerLatencyStats
- DiameterDrmaLatencyStats
- DiameterDrmaPeerLatencyStats
- DiameterVzrStats
- ProtocolErrorStats
- ConnectionErrorStats
- DiameterEventTriggerStats
- DiameterConnectionEventTriggerStats
- IntervalStats
- TrafficProfileStats
- StaleSessionStats
- SyReconciliationStats
- QuotaProfileStats
- SgwFailureStats

- PolicyStats
- TopologyUpdateStats
- PolicyServerStats
- KpiStats
- LdapDataSourceStats
- ShDataSourceStats
- SprDataSourceStats
- RadiusAccountingStats
- RadiusAccountingNetworkElementStats
- DiameterMrnPcefStats
- DiameterMrnPcefPeerStats
- DiameterMrAfStats
- DiameterMrAfPeerStats
- DiameterMrBberfStats
- DiameterMrBberfPeerStats
- DiameterMrCtfStats
- DiameterMrCtfPeerStats
- DiameterMrDrmaStats
- DiameterMrDrmaPeerStats
- DiameterMrDraStats
- DiameterMrTdfStats
- DiameterMrTdfPeerStats
- DiameterMrAfLatencyStats
- DiameterMrAfPeerLatencyStats
- DiameterMrPcefLatencyStats
- DiameterMrPcefPeerLatencyStats
- DiameterMrBberfLatencyStats
- DiameterMrBberfPeerLatencyStats
- DiameterMrDrmaLatencyStats
- DiameterMrDrmaPeerLatencyStats
- DiameterMrTdfLatencyStats
- DiameterMrTdfPeerLatencyStats
- DiameterMrVzrStats
- KpiMrStats
- IntervalMrStats
- ProtocolMrErrorStats
- ConnectionMrErrorStats

#

3GPP 3rd Generation Partnership Project
The standards body for wireless communications.

3GPP2 3rd Generation Partnership Project
2

A

ADC Application Detection and Control
Policy rules that enable detection and control of application traffic and associated enforcement action.

ADS Analytics Data Stream
A data feed containing real-time analytic data generated from one or more MPE devices by events that occur in the Policy Management system.

APN Access Point Name
The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.

C

charging server An application that calculates billing charges for a wireless subscriber

CID Connection ID

C

CMP	<p>Configuration Management Platform</p> <p>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.</p>
CMTS	<p>Cable Modem Termination System</p> <p>An edge device connecting to subscribers' cable modems in a broadband network. A CMTS device can function as a PCEF device; see PCEF.</p> <p>Equipment used by cable companies to provide high speed data services to cable subscribers.</p>
COMCOL	<p>Communications Core Object Library</p> <p>A suite of re-usable C++ libraries, as well as processes and procedures available for use in Oracle products. Many of its features are focused toward the communications area of software developments, although its purpose is not intended to restrict its functionality to any particular area.</p>
COPS	<p>Common Open Policy Service</p> <p>A protocol that is part of the internet protocol suite as defined by the IETF's RFC 2748. COPS specifies a simple client/server model for supporting policy control over Quality of Service (QoS) signaling protocols (for example, RSVP).</p>

C

CPU

Central Processing Unit

D

DEA

Diameter Edge Agent

Device through which LTE roaming signaling traffic is funneled to protect network element addresses from being exposed to third parties.

Diameter

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.

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

DPI

Deep Packet Inspection is a form of packet filtering that examines the data and/or header part of a packet as it passes an inspection point. The MPE device uses DPI to recognize the application for establishing QoS or managing quota. See also packet inspection.

DSCP

Differentiated Services Code Point

Provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated

D

services are realized by mapping the code point contained in a field in the IP packet header to a particular forwarding treatment or per-hop behavior (PHB). Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

DSR

Diameter Signaling Router

A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

E

E.164

The international public telecommunication numbering plan developed by the International Telecommunication Union.

ESME

External Short Message Entity

The remote-destination entities on the IP network that is connected to using SMPP protocol.

ESPR

Enhanced Subscriber Profile Repository - Oracle Communications' database system that provides the storage and management of subscriber policy control data for PCRF nodes.

E

event In Policy Management, an expected incident that is logged. Events can be used for debugging purposes.

F

FABR Full Address Based Resolution
Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.

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.

FQDN Fully Qualified Domain Name
The complete domain name for a specific computer on the Internet (for example, www.oracle.com).
A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GPRS General Packet Radio Service
A mobile data service for users of GSM mobile phones.

GUI Graphical User Interface

G

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.

Gx

The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.

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.

High Availability

See HA.

HTTP

Hypertext Transfer Protocol

I

IMSI

International Mobile Subscriber Identity

A unique internal network ID identifying a mobile subscriber.

IP-CAN

Internet Protocol Connectivity Access Network

Collection of network entities and interfaces that provide the underlying IP transport connectivity between the user

I

equipment (UE) and the core network or backbone entities. An example IP-CAN is GPRS. An IP-CAN session can incorporate one or more IP-CAN bearers.

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).

IPv6

Internet Protocol version 6

Identifies an Internet Protocol version 6 address composed of 8 groups of colon-separated 4 hexadecimal digits.

K

KPI

Key Performance Indicator

L

LDAP

Lightweight Directory Access Protocol

A protocol for providing and receiving directory information in a TCP/IP network.

Lightweight Directory Access Protocol

See LDAP.

M

MCC

Mobile Country Code

A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies

M

a particular subscriber. See also MNC, IMSI.

MNC

Mobile Network Code

A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.

MPE

Multimedia Policy Engine

A high-performance, high-availability platform for operators to deliver and manage differentiated services over 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.

MRA

Multi-Protocol Routing Agent - Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.

MTA

Mail Transfer Agent (or Message Transfer Agent)

Email server software that transfers electronic mail messages from one computer to another.

N

N

network topology	A map of physical equipment or logical entities in a network.
NFV	<p>Network Functions Virtualization</p> <p>Applying IT virtualization technologies to virtualize network functions for telecommunications carriers.</p> <p>Principle of separating network functions from the hardware they run on by using virtual hardware abstraction.</p>
NW-CMP	<p>Network Configuration Management Platform</p> <p>The NW-CMP server configures Network tier objects. Examples of Network tier objects are policies, network elements, and configuration templates.</p>

O

OCS	<p>Online Charging System</p> <p>A system allowing a Communications Service Provider to charge customers in real time based on service usage.</p>
OFCS	Offline Charging Server
OM	Operational Measurement

P

packet inspection	Packet inspection (or shallow packet inspection) is a form of packet filtering that checks the header portion of a packet. See also deep packet inspection.
-------------------	---

P

PCC	<p>Policy and Charging Control</p> <p>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.</p>
PCEF	<p>Policy and charging enforcement function</p> <p>A system responsible for enforcing policies on network subscriber authentication, authorization, accounting, and mobility. A PCEF device, such as a CMTS or GGSN, communicates with a PCRF device, such as a policy server.</p>
PCMM	<p>PacketCable MultiMedia</p>
PCRF	<p>Policy and Charging Rules Function</p> <p>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.</p> <p>Software node designated in real-time to determine policy rules in a multimedia network.</p>
PDN	<p>Packet Data Network</p> <p>A digital network technology that divides a message into packets for transmission.</p>

P

PER	<p>Policy Event Record</p> <p>A Policy Management-related message in the Analytics Data Stream.</p>
PGW	<p>PDN Gateway</p>
PUR	<p>Profile Update Request on Sh Interface</p> <p>The Command sent by a Diameter client to a Diameter server to update user data in the server.</p>

Q

QoS	<p>Quality of Service</p> <p>Control mechanisms that guarantee a certain level of performance to a data flow.</p>
-----	---

R

RADIUS	<p>Remote Authentication Dial-In User Service</p> <p>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.</p>
realm	<p>A fundamental element in Diameter is the realm, which is loosely referred to as domain. Realm IDs are owned by service providers and are used by Diameter nodes for message routing.</p>

S

SANE	<p>Secure Access to Network Elements</p> <p>Verizon Wireless's central authentication and authorization system for network elements. It provides single-sign-on capability to network elements, for user of the SANE GUI client, and it allows network element vendors to use open-source, open-protocol methodologies to integrate clients into the Verizon Wireless security infrastructure.</p>
S-CMP	<p>System Configuration Management Platform</p> <p>The S-CMP servers configure System tier objects. System tier objects are MPE and MRA devices.</p>
SCTP	<p>The transport layer for all standard IETF-SIGTRAN protocols.</p> <p>SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.</p>
Secure Access to Network Elements	See SANE.
server	<p>In Policy Management, a computer running Policy Management software, or a computer providing data to a Policy Management system.</p>

S

session	A Diameter session between the MPE and an external device (for example, a Gx, Gxa, Gx-Lite or Rx session). Subscribers can maintain multiple sessions at any given time.
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
Short Message Service	See SMS.
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
SMSR	SMS Relay Application An interface between the MPE and SMSC or other specific SMS web service(s).
SMTP	Simple Mail Transfer Protocol

S

SPR	Subscriber Profile Repository
	A logical entity that may be a standalone database or integrated into an existing subscriber database such as a Home Subscriber Server (HSS). It includes information such as entitlements, rate plans, and so on. The PCRF and SPR functionality is provided through an ecosystem of partnerships.

SSO	Single Sign-On
-----	----------------

Subscriber Profile Repository	See SPR.
-------------------------------	----------

T

TLV	Type/Length/Value
-----	-------------------

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.

U

UE	User Equipment
----	----------------

V

VIP	Virtual IP Address
	Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more

V

IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

X

XML

eXtensible Markup Language

A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.