Oracle® Communications Policy Management

Configuration Management Platform Wireless User's Guide

Release 9.9.2

E70987 Revision 01

May 2016

ORACLE

Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide,

Release 9.9.2

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

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:

- *Introduction* 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 Multimedia Policy Engine (MPE) device, which manages multiple network-based client sessions; the network in which the MPE device operates; policies; and the 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.
- *Managing Network Elements* describes how to manage network elements.
- *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).
- *Managing Policy Front End Devices* describes the Multi-Protocol Routing Agent (MRA), a standalone entity that supports MPE devices and is manageable by the CMP system.
- *Managing Mediation Servers* describes how the CMP system interacts with the mediation server.
- *About Subscriber Profile Repositories* describes how to manage subscriber profile repositories (SPRs).
- *Managing Subscribers* describes how to manage subscriber tiers, entitlements, and quota usage within the CMP system.
- *System-Wide Report* describes the reports available on the function of Policy Management systems in your network.
- *Upgrade Manager* describes the purpose of the Upgrade Manager GUI page and the elements found on that page.
- *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.

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

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information.

Other Publications

The following documents are useful for reference:

- Internet Engineering Task Force (IETF) Diameter-related RFCs:
  - RFC 3539: "Authentication, Authorization and Accounting (AAA) Transport Profile"
  - RFC 3588: "Diameter Base 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 ad 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"
- RFC 3164: "The BSD syslog Protocol"

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.
3. Under the Oracle Communications subheading, click the **`Oracle Communications documentation`** link.

The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The

emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

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

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

Chapter 2

Oracle Communications Policy Management System

Topics:

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.

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.

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.

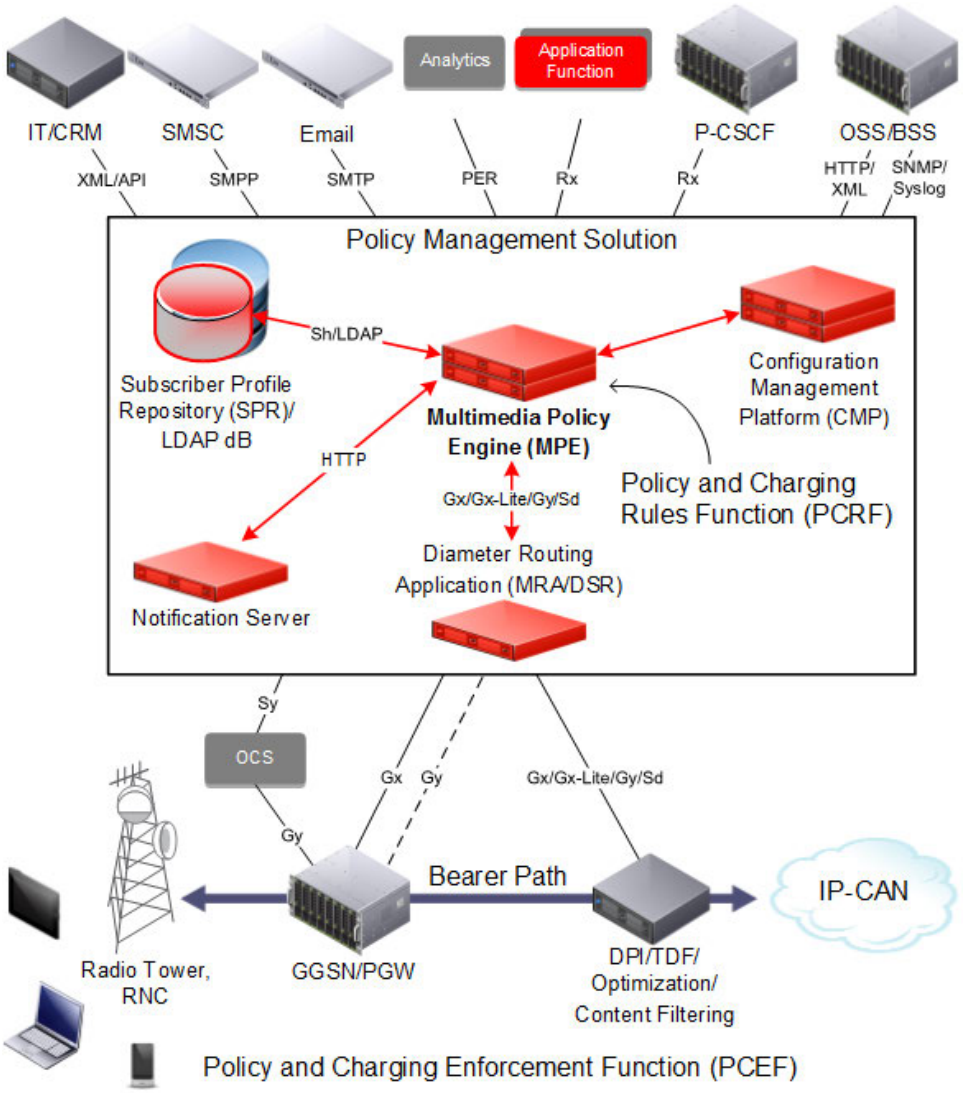


Figure 1: The Policy Management Solution and MPE Devices

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 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 Oracle Communications Policy Management 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

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

Figure 2: 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 BBEFs 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).
- 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; it can affect, in real time, the service rendered. MPE devices communicate with OCSs 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 OCSs, 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 Policy Front End (also referred to as the MRA) 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, see *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.

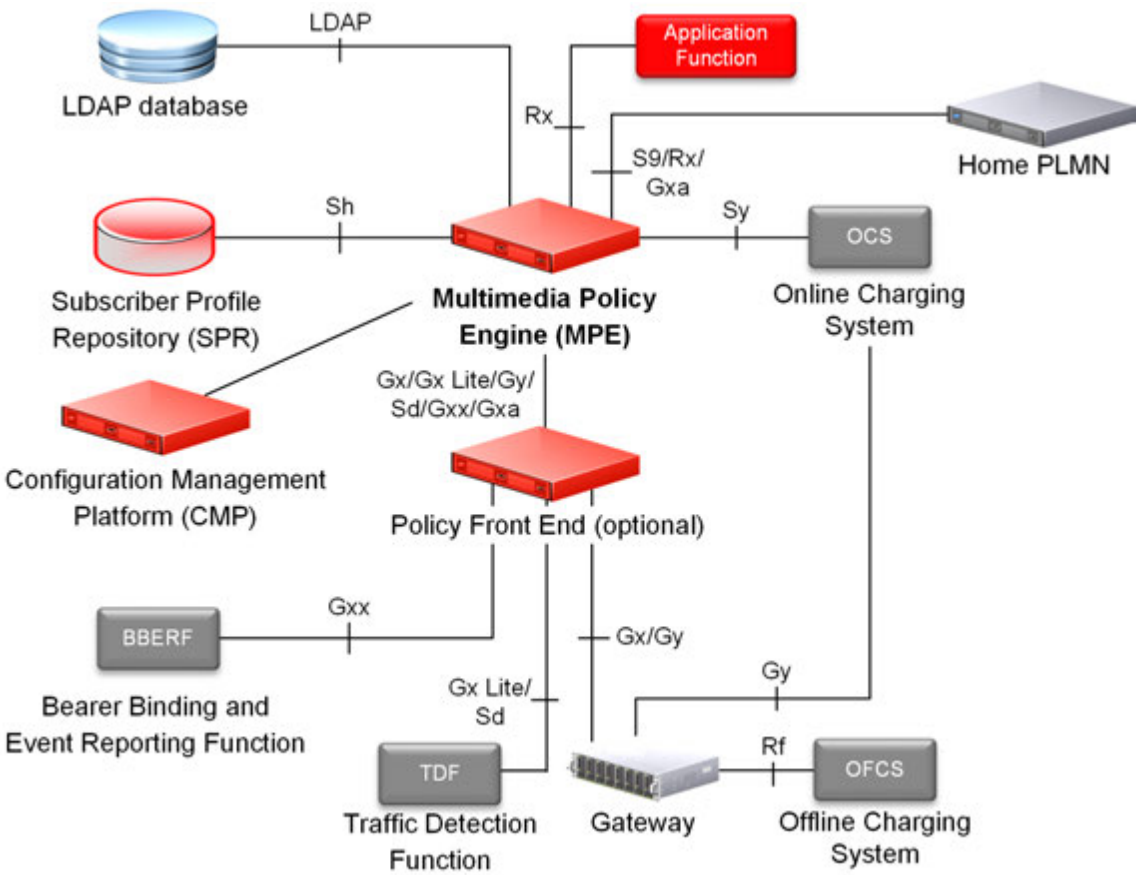


Figure 2: Interfaces to the MPE Device

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.

Notification Servers

Note: To support notification, the CMP system must be operating in SMPP or XML mode. See *CMP Modes* for details.

Within the Policy Management system, an MPE device configured for generic notifications connects to a notification server over HTTP. The notification server processes event notifications in response to policy actions for HTTP messages. These policy actions include the ability to:

- Send notifications using a dynamic URL

- Send notifications using a static URL

Refer to *Policy Wizard Reference* for details on managing notification servers.

The audit log records all notification server actions (create, modify, and delete), policy creation and modification, and associations (both policy servers and configuration templates).

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, 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.

For information about the MRA device and how to configure the device, see *Policy Front End Wireless User's Guide*.

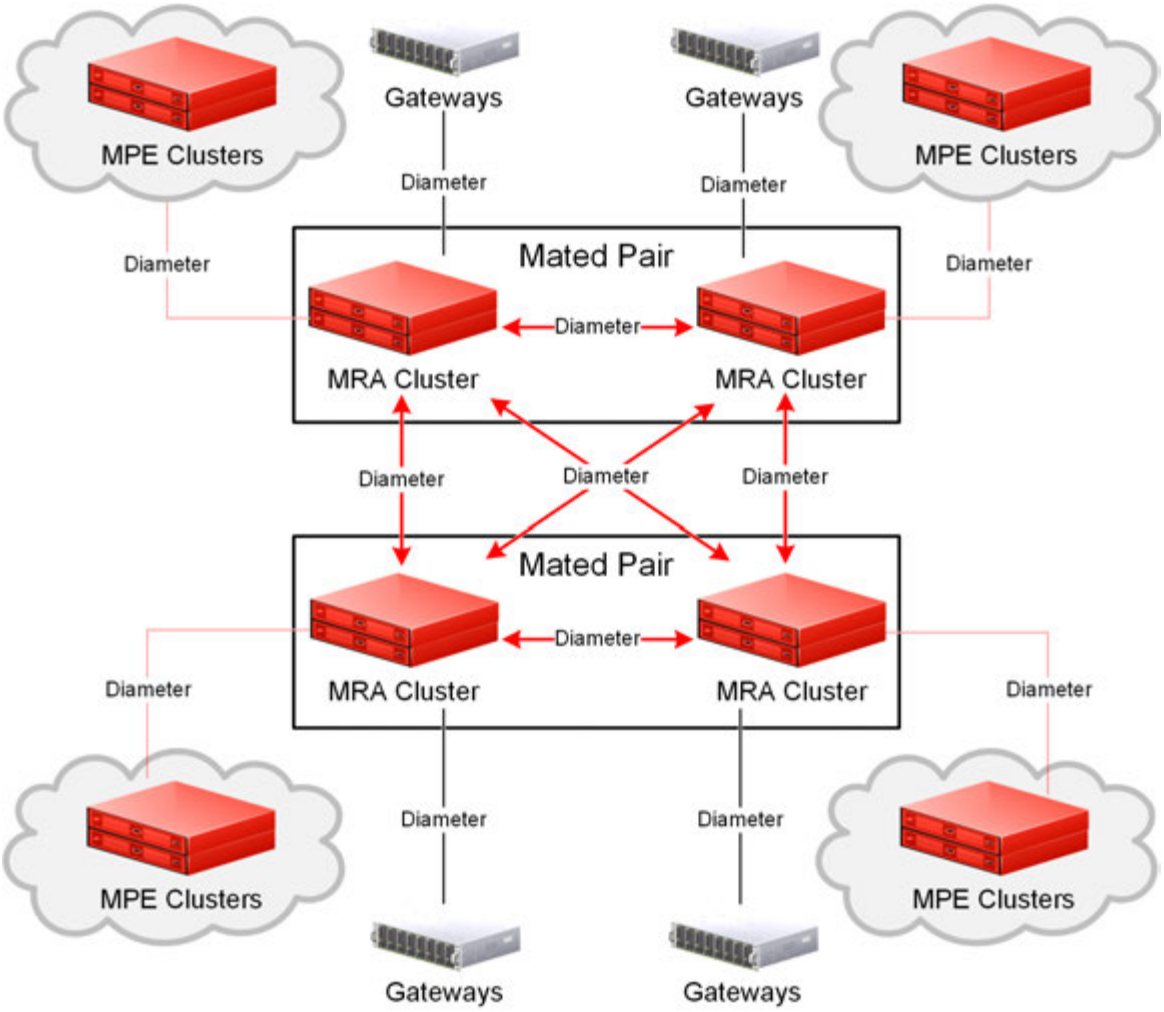


Figure 3: Typical MRA Network

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.

Examples of SPR systems are:

- 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 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 and management of mediation 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	• Mozilla Firefox® release 10.0 or later • Google Chrome version 20.0 or later
Monitor	Use a 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.

GUI Overview

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

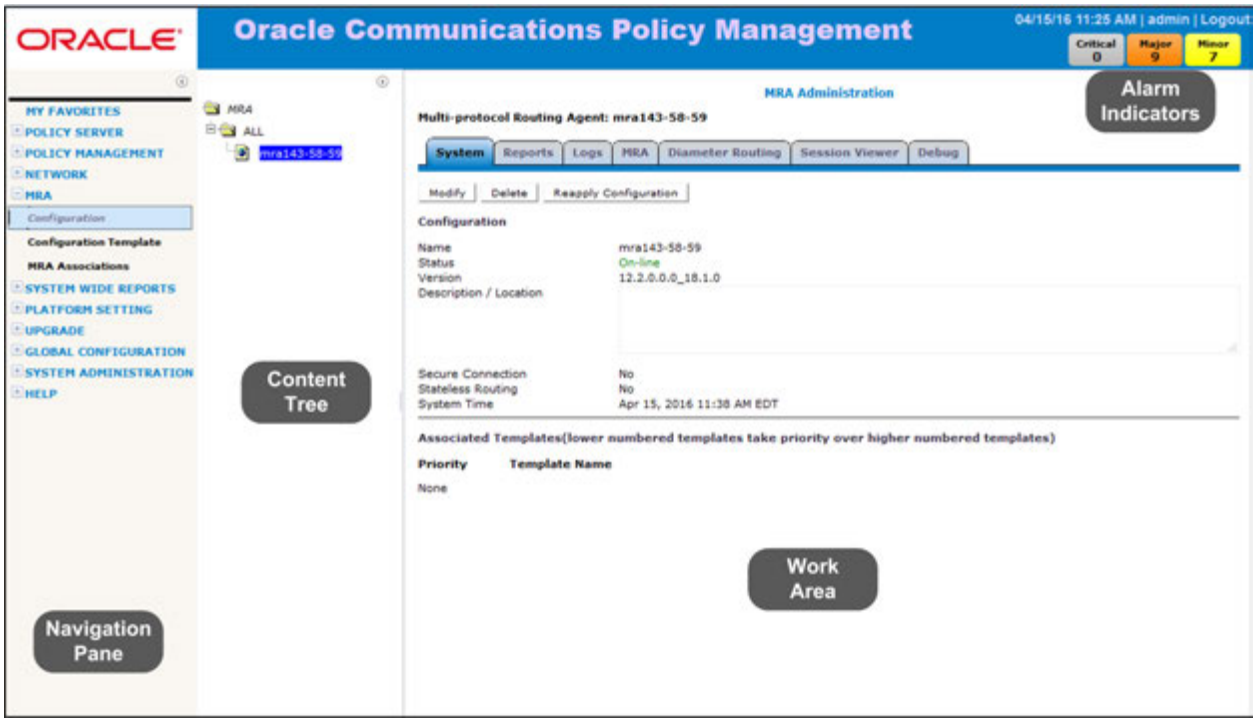


Figure 4: Layout of the CMP Window – Wireless Mode

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.
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 a 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.
View Cart	Displays the list of configurable objects selected for the **Export** action.

Changing a Password

The CMP GUI lets users change their password. Refer to the *CMP User's Guide* for details.

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*.

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 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*.
- Configure mediation servers, which are used to interface between the China Mobile Communications Corporation (CMCC) Business and Operation Support System (BOSS) and the subscriber profile repository (SPR). This task is described in *Managing Mediation Servers*.

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:

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

About the Policy Management Topology

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 that controls the Policy Management network

Figure 5: Policy Management Topology illustrates a Policy Management topology consisting of a primary (CMP Site 1) and secondary (CMP Site 2) CMP cluster, an MRA cluster, and two MPE clusters.

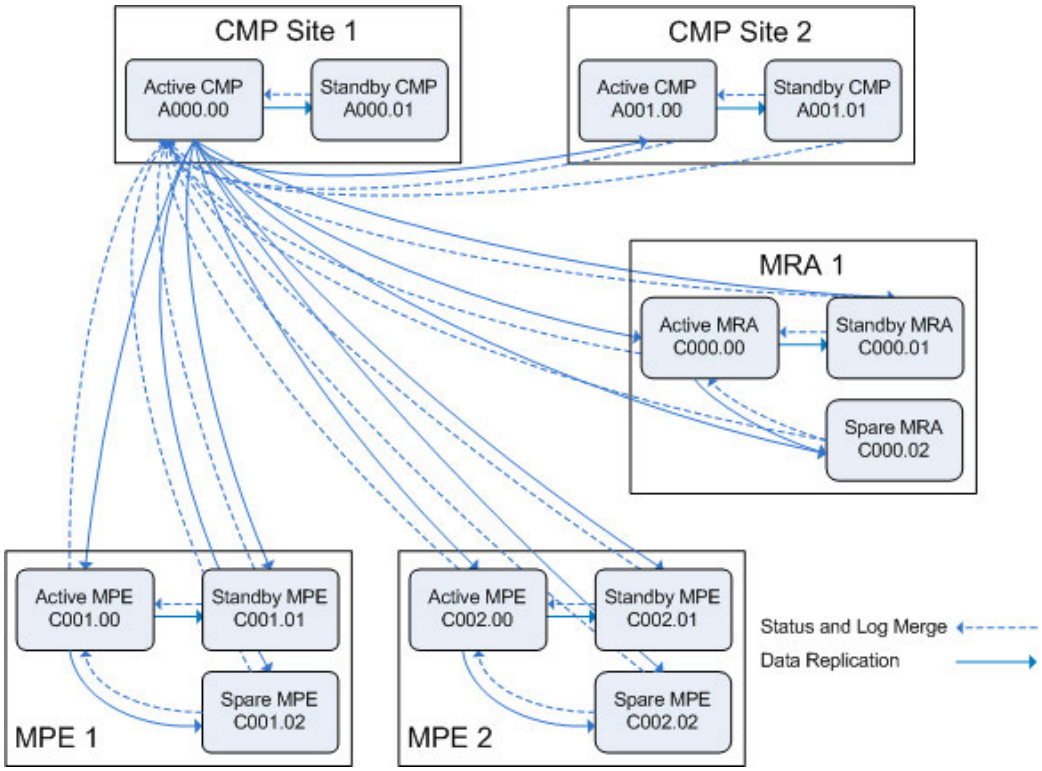


Figure 5: Policy Management Topology

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

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 6: 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.

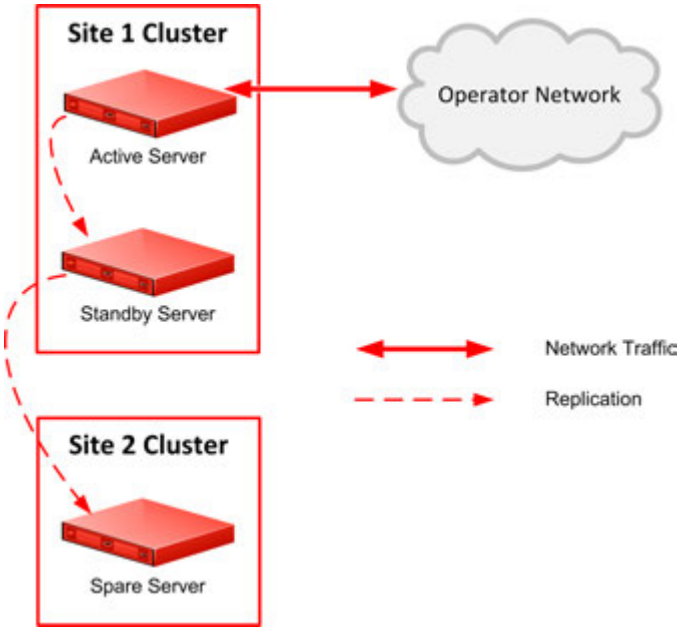


Figure 6: Clusters with Active, Standby, and Spare Servers

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 7: 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.

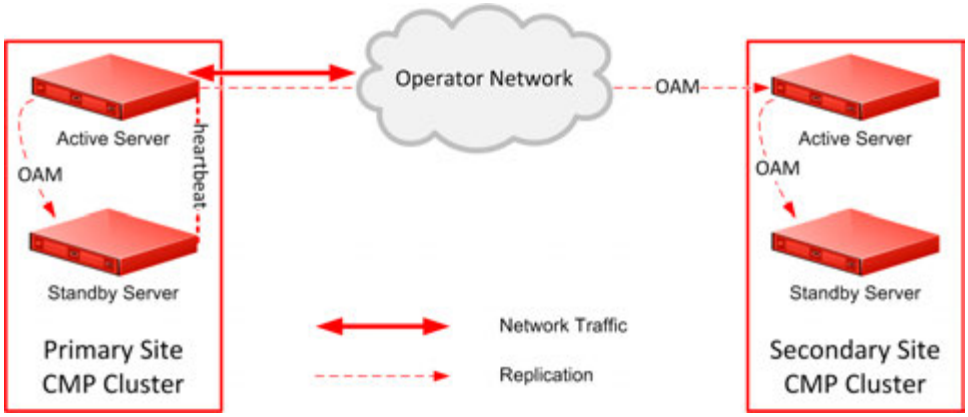


Figure 7: CMP Georedundancy

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 (HP ProLiant BL460G6c/G8c servers with a 1x4 mezzanine card) and Netra servers 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 8: 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.

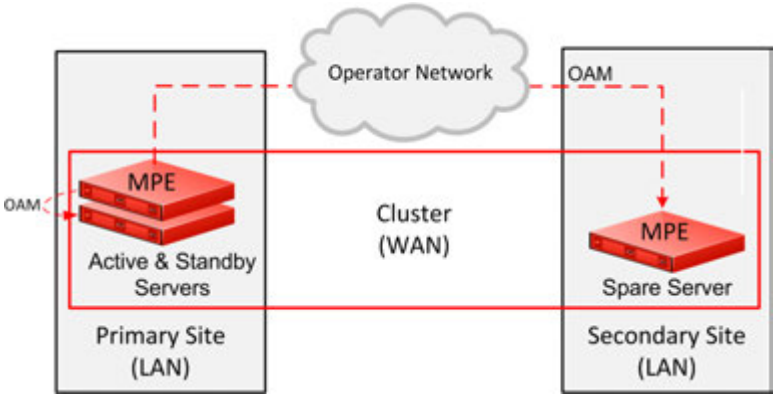


Figure 8: Non-CMP Georedundant Configuration

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.

Diameter signaling traffic is carried on a virtual LAN (VLAN) Signaling A (SIG-A) network or, optionally, a SIG-B network. Database replication and high-availability (HA) heartbeat traffic within a site (that is, between the active and standby servers) is sent on an Operation, Administration, and Management (OAM) VLAN network. You can configure the Policy Management topology to send

replication and HA heartbeat data between sites (that is, between the active and spare servers) using different VLANs. Replication data can be sent between sites on the OAM (default), SIG-A, SIG-B, or a dedicated replication (REP) network. (Replication traffic between CMP servers always uses the OAM network.) For information on configuring a REP network, see *Setting Up a Non-CMP Cluster*. In a georedundant topology, HP ProLiant BL460G6 servers (with a 1x4 mezzanine card) and Netra servers can communicate over a dedicated backup (BKUP) network. However, for Policy Management applications, only backup of CMP systems is typical.

Replication packets can be marked with a symbolic differentiated services code point (DSCP) value to determine per-hop behavior (PHB). The supported code points are class selector (CS), assured forwarding (AF), and expedited forwarding (EF). The available class selectors are CS1 through CS7. The following AF points are available:

Drop Probability	Class 1	Class 2	Class 3	Class 4
Low	AF11	AF21	AF31	AF41
Medium	AF12	AF22	AF32	AF42
High	AF13	AF23	AF33	AF43

A cluster can be configured to use a secondary HA heartbeat path between georedundant sites in case the primary HA heartbeat network fails. The secondary HA heartbeat path can be configured to use the OAM, SIG-A, SIG-B, or REP network. If the primary HA heartbeat network fails, then the secondary HA heartbeat path continues to send heartbeats between the active and spare servers.

The primary HA heartbeat path is the same as the replication path. The default primary HA heartbeat and replication path is the OAM network. If you configure a different network to carry replication traffic, then that network is also used as the primary HA heartbeat network. In this case, the OAM network could be configured as the secondary HA heartbeat network.

Replication traffic, including a threshold of outstanding updates to a standby or spare server (see *Configuring the Upsync Log Alarm Threshold*), is displayed in an MPE/MRA Replication Stats report (see *Viewing the MPE/MRA Replication Statistics Report*).

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 9: 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.

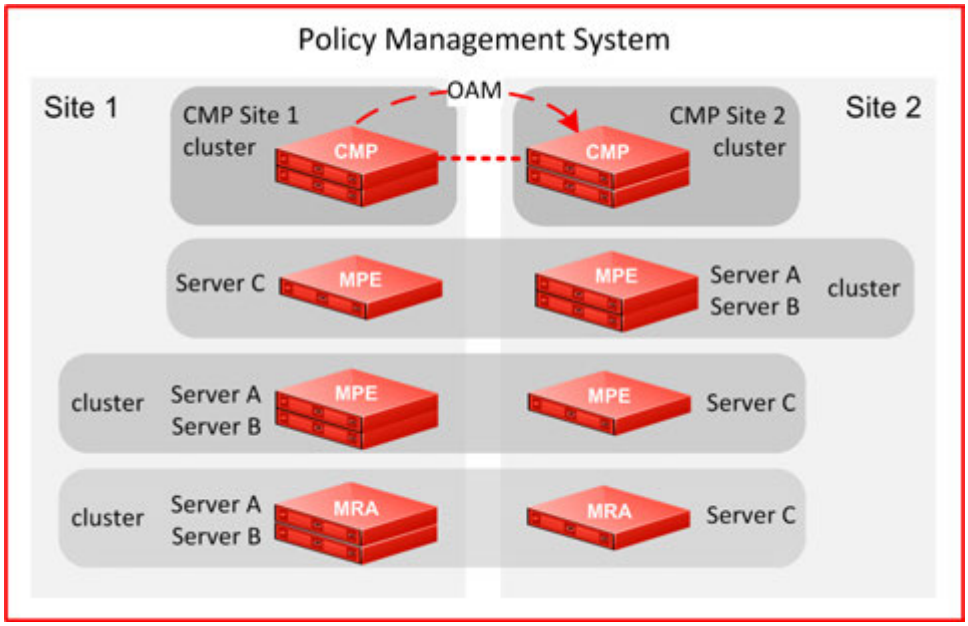


Figure 9: Example of Primary and Secondary Sites

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 10: 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 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.

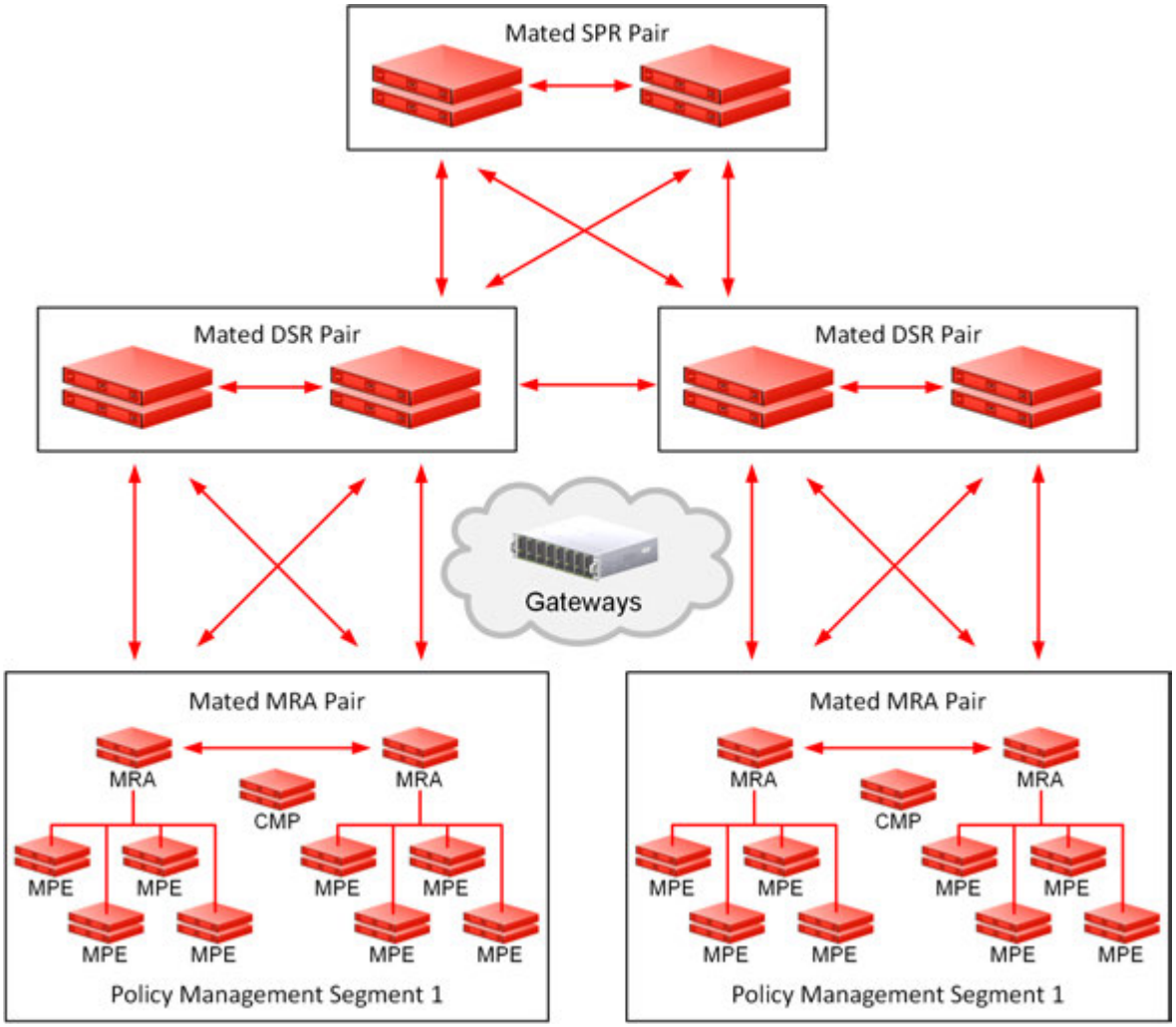


Figure 10: Segmented Policy Management Network

Policy Management Integration with CMCC

The CMP system and the subscriber profile repository (SPR) integrate with the CMCC system as shown in *Figure 11: CMCC General Architecture*.

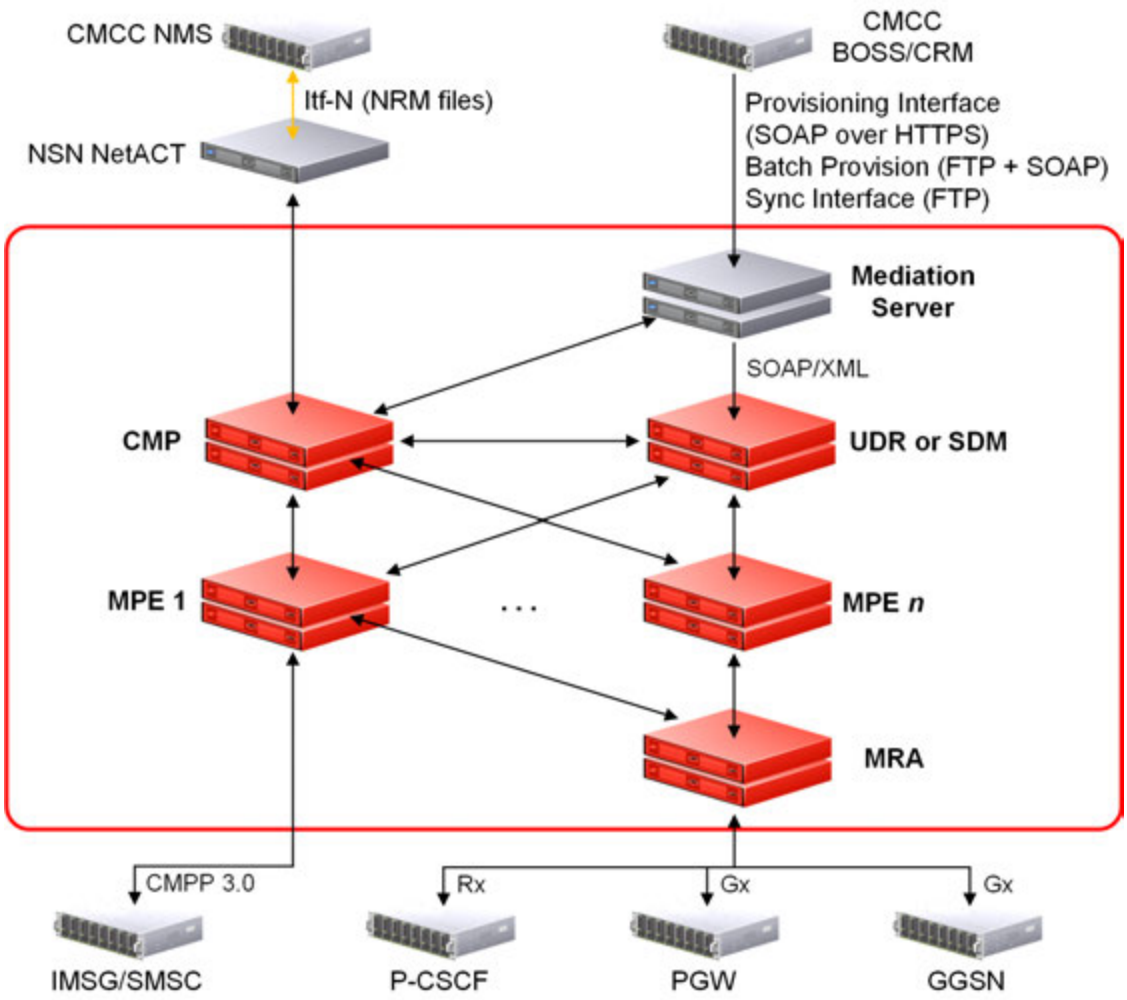


Figure 11: CMCC General Architecture

Integration with the CMCC Network Management System

The CMP system integrates with the CMCC Network Management System (NMS) through the Nokia Siemens Network (NSN) NMS, referred to as NetAct.

The CMP/NetAct integration is used for:

- Performance Management — The CMP system generates performance statistics and sends the statistics files to NetAct using FTP.
- Fault Management — The CMP system relays alarm information from the SPR and hardware.
- Configuration Management — The CMP system generates and supports static and dynamic information for Network Resource Management (NRM) and uploads the NRM statistics files to NetAct using FTP.

Integration with the CMCC BOSS System

The SPR (server) integrates with the CMCC Business and Operation Support System (BOSS) (client) through a mediation server to manage subscriber data. The mediation server uses the SOAP over

HTTP/HTTPS protocol to process subscriber profile and service subscription data. The mediation server provides:

- Initial SPR data provisioning — The mediation server processes the initial subscriber data provisioning file issued by the CMCC BOSS system.
- SPR provisioning — The mediation server processes the request and response between the CMCC BOSS system and either the Oracle Communications User Data Repository (UDR) or the Oracle Communications Subscriber Database Management (SDM) system.
- Data consistency checking — The mediation server processes data consistency checks between the CMCC BOSS and SDM systems. After the check is complete, the mediation server generates full or incremental SPR data by time frame or MSISDN prefix and sends the SPR data file to the BOSS system using FTP. The BOSS system compares the data and returns a conflict results file. The mediation server can resolve the conflict by modifying the SDM.

The mediation server is configured using the CMP GUI. See *Managing Mediation Servers* for more information.

Interaction with the Short Message Service Center

The China Mobile Peer to Peer (CMPP) interface can be used when submitting short messages to the subscriber through the Short Message Service Center (SMSC).

Messages over 140 characters are automatically segmented by the Multimedia Policy Engine (MPE) device and re-assembled by the receiving device. The maximum segmentation length is 255 characters.

The CMPP mode is set from the Mode page of the CMP system. See *The Mode Settings Page*. The CMP system is then used to create the CMPP profile and push the profile to the SMS Relay (SMSR). The SMSR uses the CMPP profile to establish a connection to the SMSC. See *Configuring a CMPP Client-based SMSR* for information on creating a CMPP profile and setting the SMSR and CMPP logs.

CMPP policies are pushed to the MPE devices and are used to trigger requests for submitting short messages when executed. The SMSR configuration is also pushed to the MPE devices and is used as the destination of the requests in MPE devices. The SMSR, in communication with the SMSC, constructs and sends the submit messages to the SMSC and receives the delivered messages from the SMSC following the CMPP specification.

A CMPP client is configured on the CMP system and added to the SMSR. The CMPP client can connect to the SMSC and send and receive CMPP messages. CMPP messages of greater than 160 octets are sliced when being sent to the SMSC and re-formed into one message at the SMSC.

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.

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. Configure the secondary CMP cluster (optional):
   a. Use the primary CMP cluster to configure a secondary, or Site 2, CMP cluster.
   b. A secondary CMP cluster can provide georedundancy.
3. To configure MPE and MRA clusters, 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.
   3. Active servers communicate with spare servers using WAN connections over the OAM, SIG-A, SIG-B, or REP network.
   4. Active and standby servers share a virtual IP (VIP) cluster address to support automatic failover.
   5. If present, the spare server has a unique VIP address.
   6. 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. For georedundancy (optional), 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** – Oracle Netra Server X3-2 or Oracle Sun Server X4-2
   - **RMS** (rack-mounted server) – HP ProLiant DL360G6/G8 or HP ProLiant DL380 G6/G8 server
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** IPv4 address and **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.

   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) 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.

   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.

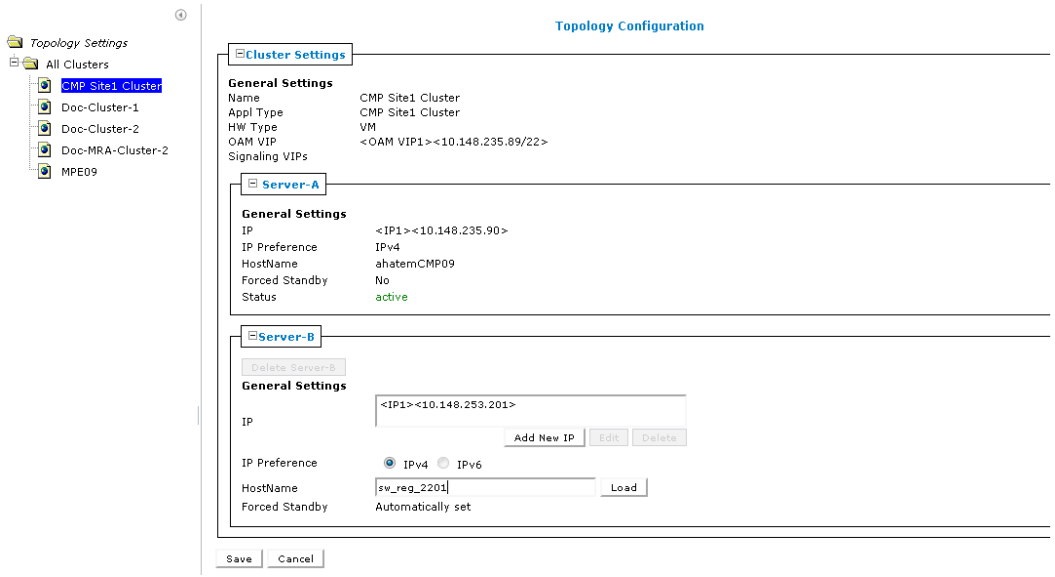


Figure 12: Cluster Settings Page for CMP Cluster

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.

      Use the IPv4 standard dot-formatted IP address string.

   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 secondary (Site 2) 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/Mediation**.
   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**
      - **Mediation**
   c) Select the **Degrade on failure of** settings.

This is the signaling network that, if it fails, the server status changes to Degraded. Available options are:

- OAM
- SIG-A
- SIG-B
- Both SIG-A and SIG-B

d) 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** – Oracle Netra Server X3-2 or Oracle Sun Server X4-2
- **RMS** (rack-mounted server) – HP ProLiant DL360G6/G8 or HP ProLiant DL380 G6/G8 server

e) (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** IPv4 address and **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.

2. Click **Save**.

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

f) If needed, repeat the process for the second OAM VIP.

g) (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. 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.

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.

h) Repeat the process for any remaining Signaling VIPs.

i) 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.

j) 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 IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

   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.

   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 13: 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.

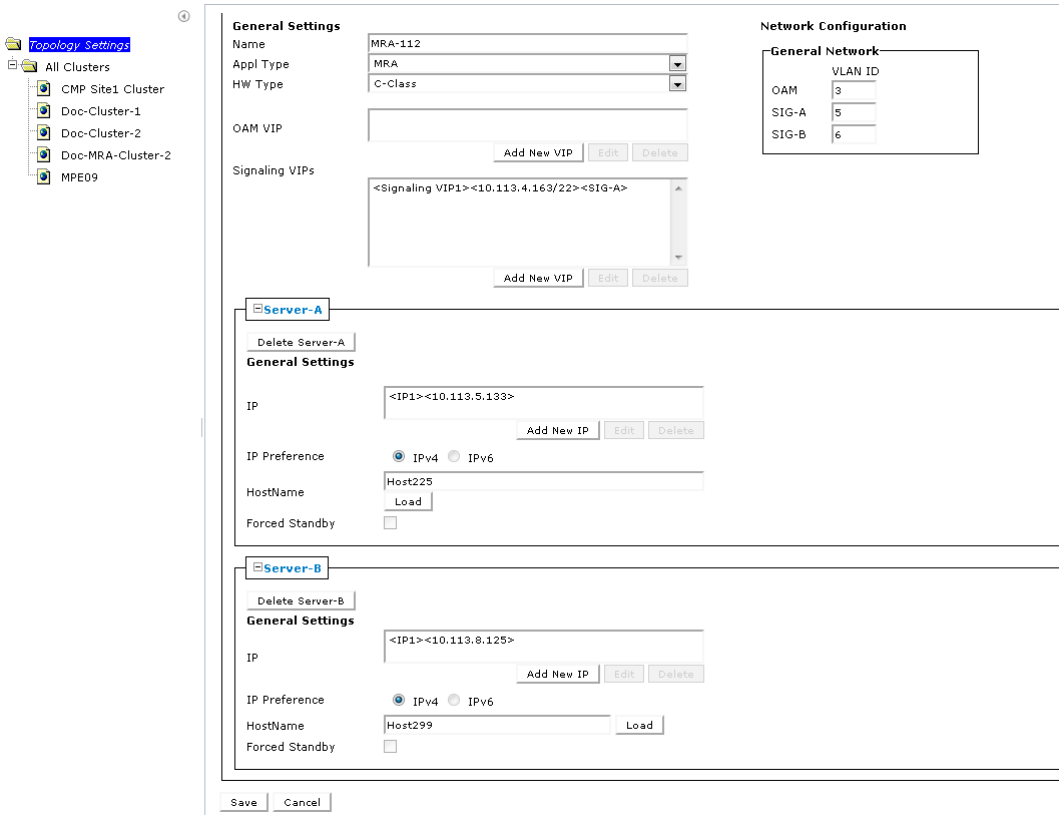


Figure 13: Sample MRA Cluster Topology Configuration

Setting Up a Georedundant Site

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

Georedundant sites can contain one or more MPE or MRA clusters.

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)

7. 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. See *CMP Modes* for more information.

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
- Mediation

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/Mediation 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**
      - **Mediation**

c) Select the **Site Preference**.

Available options are **Normal** (default) or **Reverse**. See *Georedundant Site Preferences* for more information.

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

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

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**

Note: When saving a configuration using **SIG-C**, a dialog opens stating, `If you configure SIG-C interface, the HW type cannot be set to RMS. Do you want to continue?` Click **OK**. The **RMS** option for **HW Type** shall be removed until all configured Signaling C VIPs or **SIG-C** interfaces in static IP are removed.

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.

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** – Oracle Netra Server X3-2 or Oracle Netra Server X5-2
- **RMS** (rack-mounted server) – HP ProLiant DL360G6/G8 or HP ProLiant DL380 G6/G8 server

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** IPv4 address and **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.

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. 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.

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 IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

      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.

   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 IPv4 address of the server. Enter the standard IP dot-formatted IPv4 address string.

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.

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.

   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.

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 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 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 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)

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 *The Mode Settings Page*.

   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.

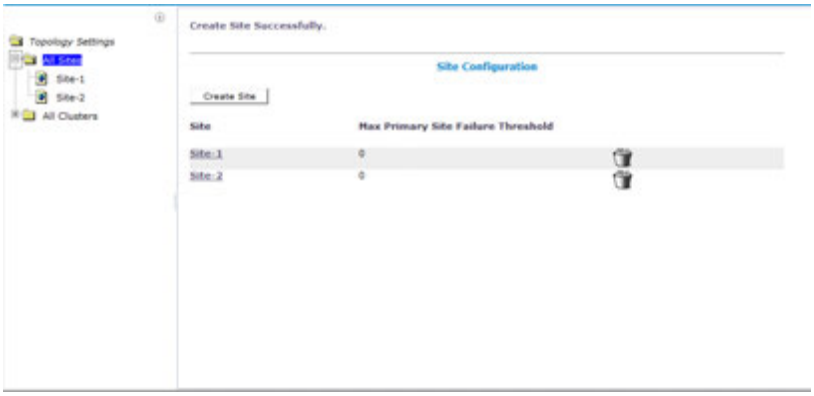


Figure 14: Site Configuration

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:

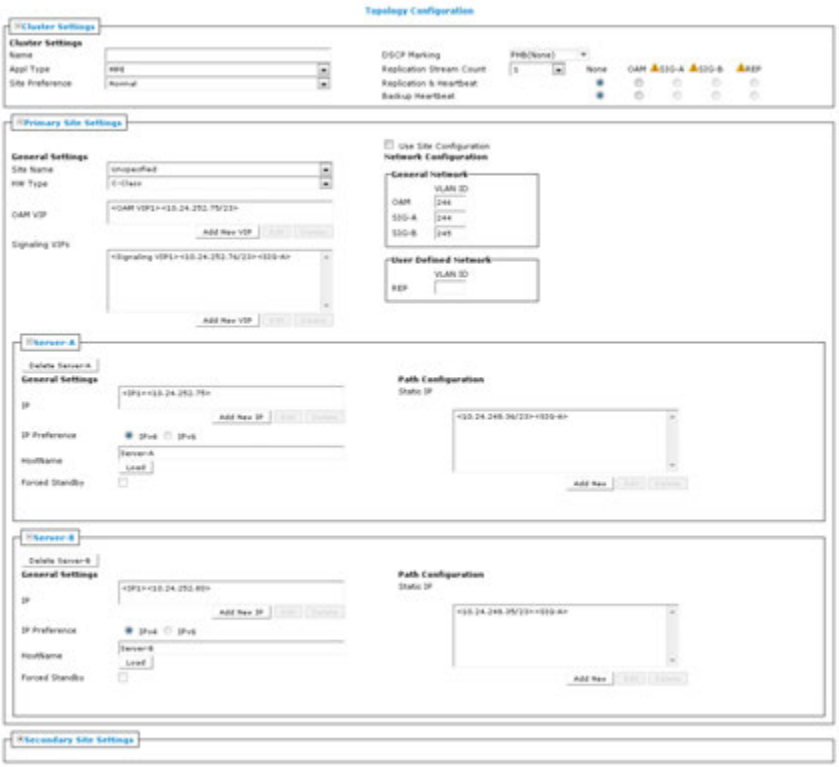


Figure 15: Example of Primary Site Settings

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:
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:
    a) If DSCP marking is used, in the **DSCP Marking** field, select the type of marking.

b) If replication streams are used, in the **Replication Stream Count** field, select the number of streams.
c) In the **Replication & Heartbeat** field, select the network used (or **None** to return to the system default).
d) 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. See *Georedundant Site Preferences* for more information.

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.

   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.

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**.

Chapter 4

Managing Multimedia Policy Engine Devices

Topics:

This chapter describes how to use the Oracle Communications Policy Management 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*
- *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. 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*.

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.

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.

   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*
   - *Diameter AF Default Profiles Configuration Options*
   - *Default Charging Servers Configuration Options*
   - *CMPP Configuration Options*
   - *SMPP Configuration Options*
   - *Primary SMSC Host Configuration Options*
   - *Secondary SMSC Host Configuration Options*
   - *SMTP Configuration Options*
   - *Generic Notification 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 *Policy Wizard Reference*.
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

Attribute	Description
	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 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

Attribute	Description
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, see *Policy Wizard Reference*.
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	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. **Note:** If the time zone was never provided for the user equipment, system local time is applied.
Enable Pro Rate	If **false** or **undefined**, the full monthly quota for subscribers is granted for the billing cycle following a quota reset.

Attribute	Description
	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.)

Billing Date Effective Name	Enter the name of the custom field in subscriber profiles to use for the SPR variable *NewBillingDateEffective*. The default is null. This is a global setting affecting all subscribers.
	• To specify a local time in the SPR, the field must be in the format:
	`yyyy-mm-ddThh:mm:ss`
	• To specify a time zone (UTC offset), the field must be in the format:
	`yyyy-mm-ddThh:mm:ssZ`
	For example: **`2011-10-30T00:00:00-5:00`**

Track Usage for Unknown Users	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.
Subscribe For Unknown Users	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. **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.
Use Single Lookup	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*). If **false**, separate lookups are used.
Use Combined Writes	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.
Cache Quota Usage	If **true**, the MPE device caches the quota usage objects locally for as long as the user session exists. 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.

Attribute	Description
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.
Diameter Identity	The fully qualified domain name (FQDN) or the valid routable domain address (formatted as described in 3GPP TS 23.003) 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).

Attribute	Description
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 *Policy Wizard Reference* 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: • **Username** • **NAI** • **E.164 (MSISDN)** • **IMSI**

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	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.
Audio	The profile for the audio.
Video	The profile for the video.
Data	The profile for data.
Application	The profile for application.
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.

Attribute	Description
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.

CMPP Configuration Options

Attribute	Description
CMPP Enabled	Enables the CMPP client to establish a connection with the SMSC. If this box is not checked, all CMPP messages to the SMSC are dropped. The default value is *Disabled*.
SMSC Host	The host name of the CMPP client that the SMSC will connect to. The default is to leave the field blank.
SMSC Port	The port number of the CMPP client that the SMSC will connect to. The default value is 7890.
Source Address	The source address of the CMPP client. The default value is to leave the field blank.
Shared Secret	The name of the shared secret, which is used to generate the authenticator source. The default value is to leave the field blank.
Registered Delivery	Requests an SMSC delivery receipt or SME originated acknowledgments. Valid values are: • **No Delivery Receipt** (default) • **Delivery Receipt**
Service ID	The service ID. Enter a string value with a 10-character length. The default value is to leave the field blank.
Message Format	The format of the message encoding. Valid values are: • **ASCII Encoding** • **Message Write Card Operation** • **Binary Message** • **UCS2 Encoding** (default) • **GBK Encoding** **Note:** To support a Chinese character set in the message content, the format should be **UCS2** or **GBK**.

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.
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: • **Segmentation and Reassembly (SAR)** (default) • **Message Payload**

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	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. **Note:** The secondary SMSC server is used if the secondary server fails.

Attribute	Description
SMSC Port	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.
ESME System ID	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. **Note:** This value must be configured on the secondary SMPP server.
ESME Password	Enter the password of the secondary 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 secondary ESME password for verification.
ESME Source Address	Enter the source address for a SUBMIT_SM operation in SMPP Protocol V3.4. The default is none.
ESME Source Address TON	Select the source address Type of Number (TON) from the list: • **UNKNOWN** (default) • **INTERNATIONAL** • **NATIONAL** • **NETWORK SPECIFIC** • **SUBSCRIBER NUMBER** • **ALPHANUMERIC** • **ABBREVIATED**
ESME Source Address NPI	Select the source address Number Plan Indicator (NPI) from the list: • **UNKNOWN** (default) • **ISDN (E163/E164)** • **DATA (X.121)** • **TELEX (F.69)** • **LAND MOBILE (E.212)** • **NATIONAL** • **PRIVATE** • **ERMES** • **INTERNET (IP)** • **WAP CLIENT ID**
Character Encoding Scheme	Select the character-set encoding for SMS messages from the list: • **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)**

Attribute	Description
	• **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: • **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). **Note:** There is no delivery receipt for the SMTP messages sent from the SMSR, only confirmation that it reached the configured MTA.
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. **Note:** This value must be configured on the MTA.
MTA Password	Enter the password of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. **Note:** This value must be configured on the MTA.
Confirm MTA Password	Re-enter the password for verification. **Note:** This is a new configuration setting for the SMTP connection.
Default From Address(es)	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. **Note:** The total number of To, CC, and BCC addresses is limited to five.
SMTP Connections	The number of SMTP connections. Enter a number from 1–10. **Note:** SMTP connections can be increased to support a higher throughput. Contact *My Oracle Support (MOS)* for more information.

Attribute	Description
Default Reply-To Address(es)	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. The default is none.
Default CC Address(es)	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. **Note:** The total number of To, CC, and BCC addresses is limited to five.
Default BCC Address(es)	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. **Note:** The total number of To, CC, and BCC addresses is limited to five.
Default Signature	Enter the text that should appear as the signature in an SMTP message. The default is none.

Generic Notification Configuration Options

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

Configuring MPE Advanced Settings

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

The MPE Advanced Settings page is used for the following:

- *Configuring Session Clean Up Options*
- *Configuring a Configuration Key*
- *Configuring Load Shedding Rules*

Configuring Session Clean Up Options

Session cleanup options are used to configure the methods used for cleaning up stale sessions and how often cleanup occurs.

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.

3. Select the **Policy Server** tab.
   The configuration settings for the policy server are displayed.
4. Click **Advanced**.
   Advanced configuration settings, including the session clean up options, are displayed and can be edited.

Table 2: Session Clean Up Options

Attribute	Description
Enable Session Clean Up	Select to turn on session clean up. The default is enabled.
Max Session Cleanup Rate (sessions/sec)	The rate at which the cleanup task attempts to clean stale sessions. The default is 50 sessions/sec. Valid range is 1–50 sessions/sec. Do not modify this setting without consulting My Oracle Support.
Max Session Iteration Rate (sessions/sec)	The maximum rate at which the cleanup task iterates through the sessions database. Default value is 1000. Valid range is 1–1000. Do not modify this setting without consulting My Oracle Support.
Max Duration For Session Iteration (hours)	The maximum duration to iterate through the sessions. Default value is 2 hours. Valid range is 1–2 hours. Do not modify this setting without consulting My Oracle Support.
Session Cleanup Start Time	The time of day when the cleanup task occurs. Click the associated radio button and enter a value or select a value from the menu. No default value is defined.
Session Cleanup Interval (hours)	The interval at which the cleanup task occurs. Click the associated radio button and enter a value. The default is 6 hours. A value of 0 disables cleanup. Do not modify this setting without consulting My Oracle Support.
Session Validity Time (hours)	The amount of time after which all sessions except Rx sessions are declared as stale. The default is 24 hours.
Max Session Validity Time (hours)	The maximum amount of time after which the session is cleaned up after an error. The default is 48 hours. Valid range is 1–48.
Override Cleanup Audit	Select to turn override clean up audit on. When selected, the cleanup task bypasses the audit process and deletes all sessions that are stale for the session validity time. The default is deselected.
Sy Session Audit Enabled	Select to turn on auditing for the Sy session. When selected, the Sy session is checked for the association with at least one IP-CAN session. If there is not an IP-CAN session association, the Sy session is removed and an STR message is sent to the OCS. If there is at least one IP-CAN session associated with the Sy session, an SLR (INTERMEDIATE) message is sent to audit stale Sy sessions.

Attribute	Description
	If this option is deselected (the default), the Sy session is checked for IP-CAN session associations. If there is an association, the Sy session is deemed active; otherwise, it is removed and an STR message is sent to the OCS.
Sy Session Validity Time (Hours)	The amount of time after which an Sy session is declared as stale. The default is 10 hours.
Sy Session Max Validity Time (Hours)	The amount of time used to validate an Sy session after it is declared stale (inactive). If it is not validated, the session is removed and the MPE device attempts to create a new Sy session for the subscriber. The default is 48 hours.
Enable Audit for Auth Lifetime	Select to enable the feature maximum and minimum times for AAR-I messages of Rx sessions that contain the Supported Feature AVP with the Support of Rx Subscription Expiry bit set (the Authorization-Lifetime AVP in the AAR-I is optional).
Auth Lifetime (sec)	The maximum lifetime for an Rx session.
Min Auth Lifetime (sec)	The minimum lifetime for an Rx session.
Enable Grace Period of Subscription Expiry	Select to allow a grace period, which specifies how aggressively Rx sessions are purged.
Grace Period of Subscription Expiry (sec)	The amount of time between an Rx session reaching its Auth Lifetime value and the session being deleted.
Cleanup Stale Rx Sessions	Determines whether the DiameterSessionCleanUp task should clean up Rx sessions. The default is true.
Audit Rx Sessions	Determines whether the DiameterSessionCleanUp task should audit Rx sessions before purging them from the database. The default is false.
Rx Session Validity Time (hours)	The amount of time after which an Rx session is declared as stale. The default is 24 hours.

5. Click **Save**.

The settings are applied to the selected MPE device.

Configuring a Configuration Key

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 Other Advanced Configuration Settings section of the Advanced configuration page.

To configure a configuration key:

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.
3. Select the **Policy Server** tab.
   The configuration settings for the policy server are displayed.
4. Click **Advanced**.
   The advanced configuration displays.
5. Configuration key changes are made using the Other Advanced Configuration Settings section.

   - **To add a key to the table** — 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.

     Enter the following values:

     - **Configuration Key** — The attribute to set
     - **Value** — The attribute value (up to 255 characters)

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

   - **To clone a key in the table** — Select an existing key in the table and click **Clone**; the Clone Configuration Key Value window opens with that key's information filled in. Make changes as required. Click **Save**.
   - **To edit a key in the table** — Select an existing key in the table and click **Edit**; the Edit Configuration Key Value window opens with that key's information. Make changes as required. Click **Save**.
   - **To delete a key from the table** — Select an existing key in the table and click **Delete**; you are prompted with a confirmation message. Click **Delete** to remove the key.

   The following figure shows an example configuration key.

   Other Advanced Configuration Settings

   Add | Clone | Edit | Delete | Up | Down

Configuration Key	Value	Default Value	Change Log
PCMM.Cleanup.CleanupStalePcmmSessions	false	true	
KPI.Capacity.Session	1	1	

6. Click **Save**.

The configuration key is configured and the settings are applied to the selected MPE device.

Configuring Load Shedding Rules

You can configure load shedding rules to determine how an device reacts to a processing backlog. This state is called "busyness." By default there are three levels of busyness, from Level 1, the least busy, to Level 3, the most busy. With each successive level, the device becomes more aggressive in rejecting or discarding messages in an attempt to prevent the main queue from become full. At any level of busyness, requests that have been queued longer than a configurable time are silently discarded

without further processing, since the originator would have already given up on that request. The following table shows the default load-shedding rules for an device.

Note: Default Device Busyness Level 1 applies to both MPE and MRA devices, all other levels apply to MPE devices only.

Table 3: Default Device Busyness Level 1

Rule Name	Actions
Default Device Busyness Level 1	
DefaultRule1	Reject Gx CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule2	Reject Gxx CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule3	Reject Gy CCR-I messages with DIAMETER_TOO_BUSY

Use the **Load Shedding Configuration** section of the **Advanced Configuration** page to edit, reorder, or add new rules at each of the three levels 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 pre-defined 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:

- Reject new messages with a specific result code (the default is DIAMETER_TOO_BUSY).
- Drop the message.

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. Configure the rules for the busyness levels:
   a) Click ▶ (right arrow) next to the level to expand the level.
   b) Click **Add**.
      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 **Gx**, **Gy**, **Gxx**, **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.
      - **Action** — Select the action to be taken if the criteria are met for the busyness level. You can select **Drop** (drop the message); **Answer With** (select a code from the drop-down list), or **Answer With Code** (enter a code) and **Vendor ID** (enter a vendor ID).
   d) Click **OK**.

The rule is displayed in the table.

2. Once a rule is defined, you can clone, edit, or delete it by selecting the rule and clicking the appropriate button.
3. Click **Save**.

The settings are applied to the selected device.

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. 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

1. **Admin State** — Select to enable this data source.
   Selected by default.
2. **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).

3. 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
4. **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.
5. **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.
6. **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.
7. 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

1. **Common** (information common to all configured Sy servers):
   a) **Admin State** — Select to enable this data source.
   b) **Connect SCTP** — Indicates whether the Sy data sources support the SCTP protocol. If checked, the MPE device can communicate with the Sy data sources using SCTP. The default is to use the TCP protocol.
   c) **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.
   d) **Realm** (required) — Defines the Diameter realm of the primary and optional secondary servers; for example, `galactel.com`.
   e) **Unique Name** (required) — Name to identify this group of servers in the CMP database.
   f) 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 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 (see *Policy Server Reports* 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.

CMPprovides 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

The device is synchronized with the CMP system.

Reapplying the Configuration to a Group of Devices

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

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

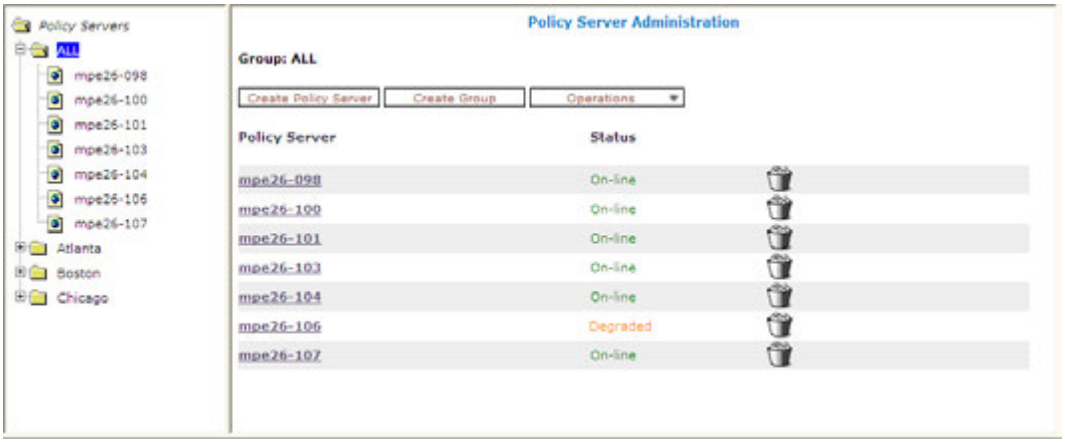


Figure 16: Group View

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	Rediscovers the cluster, deleting any failed servers that have been removed from service.
Pause/Resume	Stops or restarts automatic refreshing of displayed information. The refresh period is 10 seconds.
Cancel	Returns to previous page.

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

Cluster Information Report Information about the cluster.

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 • 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.

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 Session Clean Up Options*.

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.

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 17: 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 Sy Statistics	0	0 / 0	0
RADIUS			
RADIUS Stats		0 / 0	N/A

Figure 17: 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 *Other Publications*).

Note:

1. Statistical information is returned from the MPE device as a series of running peg counts. To arrive at interval rate information, such as session success and failure counts, two intervals are needed to perform the difference calculation. Also, statistical information, such as session activation counts, is kept in memory and is therefore not persisted across the cluster. After a failover, non-persistent metrics must be repopulated based on a sampling from the newly active primary server. Therefore, when an MPE device is brought 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.

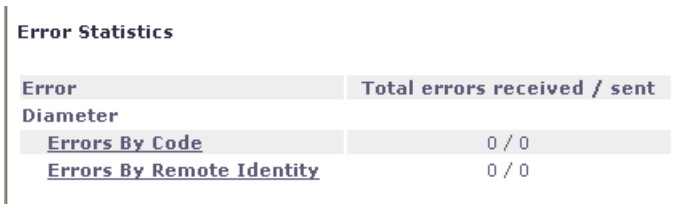
Event Trigger Statistics

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 18: 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 18: 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**
- **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**
- **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**
- **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 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.
   - **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 (calendar icon), select the starting date and time, then click **Enter**.
   - **End Date/Time** — Click (calendar icon), select the ending date and time, then click **Enter**.
   - **Trace Codes** — Enter one or a comma-separated list of trace code IDs. Trace code IDs are integer strings up to 10 digits long.
   - **Use timezone of remote server for Start Date/Time** — Select to use the time of a remote server (if it is in a different time zone) instead of the time of the CMP server.
   - **Severity** — Filter by severity level. Events with the selected severity and higher are displayed. For example, if the severity selected is **Warning**, the trace log displays events with the severity level **`Warning`** and higher.
   - **Contains** — Enter a text string to search for. For example, if you enter **`connection`**, all events containing the word **`connection`** 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 CMPP Log

The CMPP log contains all China Mobile Peer to Peer (CMPP) messages sent and received on the CMPP client, including state report if **Delivery Receipt** is enabled. This log records details about each message and tracks the success or failure of sending that message to a configured Short Message Service Center (SMSC). If messages are dropped by the short message relay (SMSR) application, then that action is logged so that all triggered messages can be tracked.

You can configure filter notifications by severity level.

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.

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

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

7. 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

   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 CMPP Log Settings** section of the page configure the **CMPP Log Level**.

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

12. 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.

13. 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:

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 MRAdevices support Diameter Rx, Gq, Ty, Gxx, Gx,Gy, 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. The content tree displays a list of policy server or MRA groups.
2. 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.

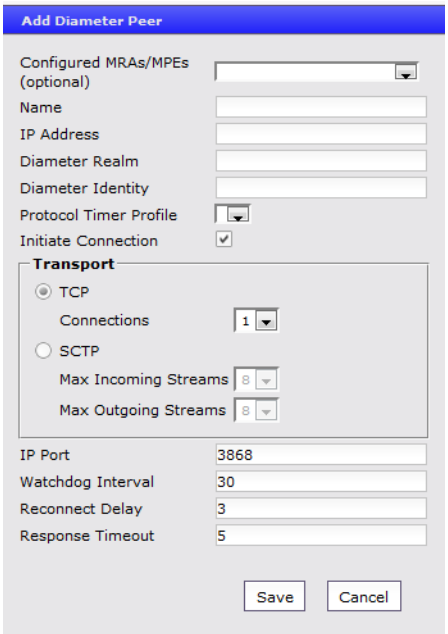


Figure 19: Add Diameter Peer

   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`**).

c) Click **Save**.

6. 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`**.
   - **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)`

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 6

Managing Network Elements

Topics:

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 form 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 form 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) **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 form 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 form 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) **FQDN** — Customer-specific fully qualified domain name of the network element.
   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 form 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 form 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 form 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 form 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:

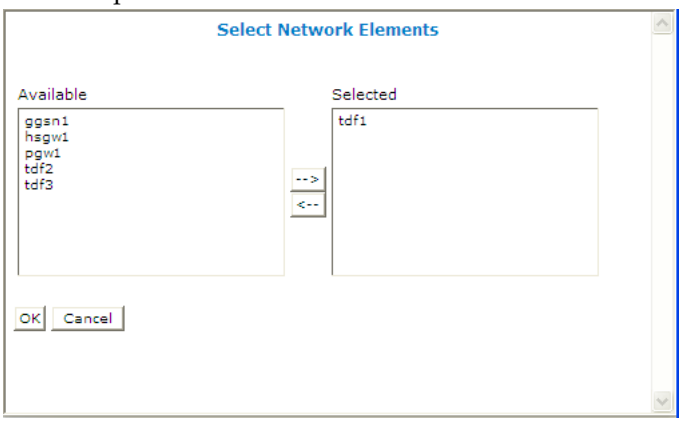


   Figure 20: Select Network Elements

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/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 7

Managing Charging Servers

Topics:

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. Enter information as appropriate for the charging server:
   a) **Name** (required) — The name you assign to the charging server.

      The name can be up to 255 characters long and must not contain colons (:), quotation marks ("), or commas (,).

   b) **Description/Location** — Free-form text that identifies the charging server within the network.

      Enter up to 250 characters.

   c) **Host Name** (required) — Fully qualified domain name assigned to the charging server.
   d) **Port** — The port number on which the charging server is listening for messages.
      If left blank, port 3868 is used.
   e) **Transport** — The transport protocol used to communicate with the charging server:

      - **tcp** — Transmission Control Protocol
      - **udp** — User Datagram Protocol
      - **sctp** — Stream Control Transmission Protocol

   f) **Protocol** — Specifies the AAA protocol used to communicate with the charging server.

      - **diameter**
      - **radius**
      - **tacacs+**

      Note: If you configure the **Transport** protocol as **udp**, you cannot configure the **Protocol** as **diameter**.

   g) **Security** — Select if transport security is used to communicate with the charging server.

5. 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, listing the defined charging servers.

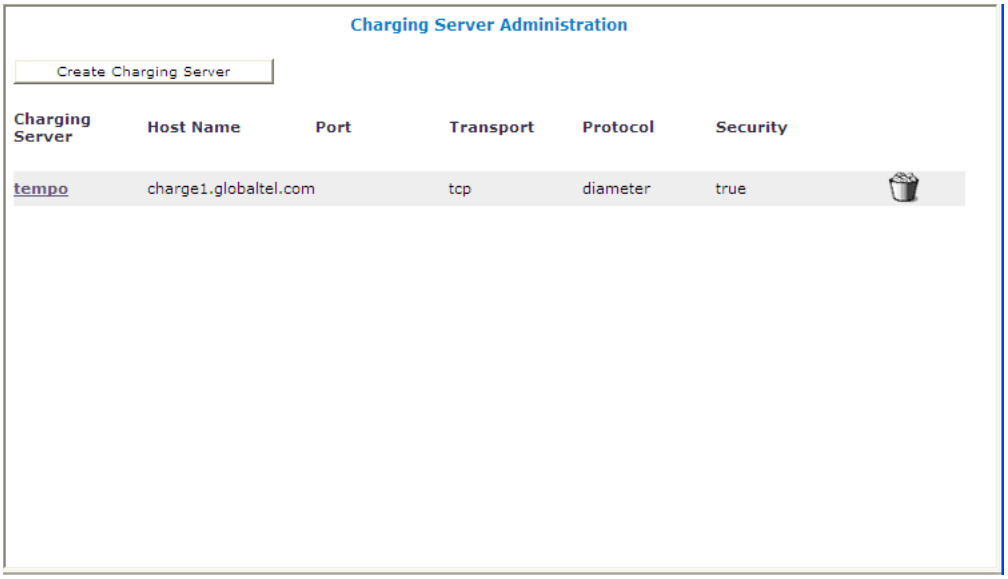


Figure 21: Charging Server Administration

2. Delete the charging server using one of the following methods:
   - From the work area, click **Delete** (), located to the right of the charging server.
   - From the content tree, select the charging server 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 policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server.
   The **Policy Server Administration** page opens in the work area.
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 8

Mapping Serving Gateways to MCCs/MNCs

Topics:

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 9

Managing Policy Front End Devices

Topics:

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 it's 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 (see *Defining a Network Element* to add network elements), 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:

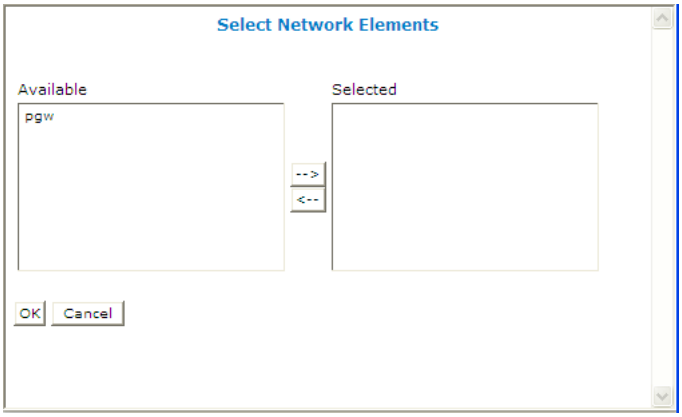


Figure 22: Select Network Elements

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.

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.

Deleting an MRA Cluster Profile from an MRA Group

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. Removing an MRA cluster profile from the ALL group removes it from all other groups.

To delete an MRA cluster profile from an MRA group (other than ALL):

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 MRA group.
   The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.
3. Remove the MRA cluster profile using one of the following methods:
   - On the **MRA Administration** page, click (scissors icon), located to the right of the MRA cluster profile you want to remove.
   - From the content tree, select the MRA cluster profile; the **MRA Administration** page opens. 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.

Configuring 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 23: Enabling Stateless Routing* shows an example).

The stateful MRA configuration is hidden.

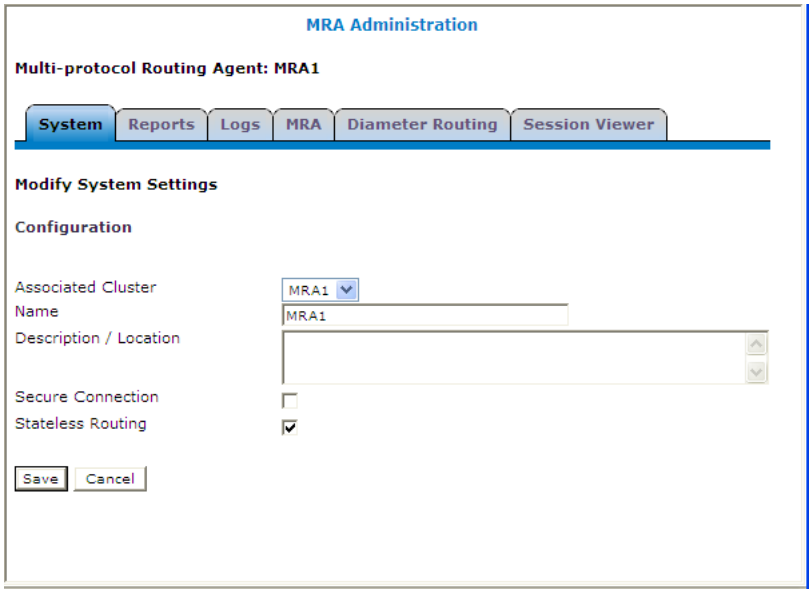


Figure 23: Enabling Stateless Routing

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.

Chapter 10

Managing Mediation Servers

Topics:

This chapter describes how to configure mediation servers and mediation server groups. The mediation server is used to interface between the China Mobile Communications Corporation (CMCC) Business and Operation Support System (BOSS) and the subscriber profile repository (SPR).

About Mediation Servers

The mediation server is used to interface between the SPR (either UDR or SDM) and the BOSS to manage subscriber data. See *Policy Management Integration with CMCC* for more information about the mediation server's role in the CMCC system.

The mediation server uses the SOAP over HTTP/HTTPS protocol to process subscriber profile and service subscription data. The mediation server provides:

- Initial SPR data provisioning — The mediation server processes the initial subscriber data provisioning file issued by the CMCC system.
- SPR provisioning — The mediation server processes the request and response between the CMCC BOSS system and either the UDR or the SDM system.
- SPR data consistency checking — The mediation server ensures data consistency between the BOSS and UDR or the SDM systems. After the check is complete, the mediation server generates full or incremental SPR data by time frame or MSISDN prefix and sends the SPR data file to the BOSS system using FTP. The BOSS system compares the data and returns a conflict results file. The mediation server can resolve the conflict by modifying the UDR or the SDM system.

Mediation Server Profiles

A mediation server profile contains the configuration information for a mediation server. The CMP system stores mediation server profiles in a configuration database. After you define profiles, you deploy them to mediation servers across the network.

The following sections describe how to manage mediation server profiles:

- *Creating a Mediation Server Profile*
- *Modifying a Mediation Server Profile*
- *Deleting a Mediation Server Profile*

Creating a Mediation Server Profile

To create a mediation server profile:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Mediation Server Administration** page opens in the work area.
3. Click **Create Mediation Server**.
   The **New Mediation Server** page opens.
4. Enter values for the configuration attributes:
   a) **Associated Cluster** (required) — Select the cluster to associate with this mediation server.
   b) **Name** — Name of this mediation server. The default is the associated cluster name. A name is subject to the following rules:
      - Is case insensitive (that is, uppercase and lowercase are treated as the same)

- Must be no longer than 255 characters
- Must not contain quotation marks (") or commas (,)

c) **Description / Location** (optional) — Information that defines the function or location of this mediation server.

d) **Secure Connection** — Designates whether or not to use the HTTPS protocol.

5. Click **Save**.

You have created a mediation server profile and the mediation server appears in the list of mediation servers.

Modifying a Mediation Server Profile

To configure or modify a mediation server profile:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the mediation server profile that you want to modify.

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

   The page contains the following tabs:

   - **System** — Defines the system information associated with this mediation server, including the name, status, version, and whether or not the mediation server uses a secure connection to any management system (such as the CMP system).
   - **Reports** — Displays various statistics and counters related to the physical hardware of the cluster, policy execution, and network protocol operation. Reports cannot be modified.
   - **Logs** — Displays the Trace Log configurations.
   - **Settings** — Lets you configure the SOAP and Data Sync Interface settings. You can also enable Load Shedding from this tab.
   - **Data Sources** — Lets you configure interfaces to the UDR or the SDM information associated with the mediation server.
   - **Profile Viewer** — Displays the Profile Viewer.
   - **Batch Task Status**—Displays the status of batch tasks.
   - **Sync** — Lets you apply synchronization settings.
3. Select the tab that contains the information you want to modify and click **Modify**.
4. Make the needed changes.
5. Click **Save**.

Deleting a Mediation Server Profile

Deleting a mediation server from the ALL group also deletes it from any associated group.

To delete a mediation server profile:

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

The **Mediation Server Administration** page opens in the work area, displaying a list of all defined mediation servers.

3. Use one of the following methods to delete a mediation server:
   - From the work area, click the **Delete** icon located next to the mediation server you want to delete.
   - From the mediation server group tree, select the mediation server. The **Mediation Server Administration** page opens. Click the **System** tab, and click **Delete**.

   A confirmation message displays.
4. Click **OK** to delete the mediation server.

The mediation server profile is deleted.

Configuring Mediation Server Interface Settings

To configure SOAP and Data Sync settings and enable Load Shedding Configuration for a mediation server:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the desired mediation server.
   The **Mediation Server Administration** page opens.
3. Select the **Settings** tab.
   The current settings are displayed.
4. Click **Modify** and define options as necessary.
   - *Table 4: Mediation Server Soap Interface Options*
   - *Table 5: Mediation Server Load Shedding Options*

Table 4: Mediation Server Soap Interface Options

Attribute	Description
Soap User Name	User name for authenticating the SOAP request.
Soap Password	Password for authenticating the SOAP request.
Enable HTTP Service	Enable to use the HTTP server. The HTTP Service and/or the HTTPS Service should be enabled.
HTTP Port	The port number of the HTTP server.
Enable HTTPS Service	Enable to use the HTTPS server. The HTTP Service and/or the HTTPS Service should be enabled.
HTTPS Port	The port number of the HTTPS server.
Equipment Serial No	The serial number of the equipment.

Table 5: Mediation Server Load Shedding Options

Attribute	Description
Enabled	Click to enable Load Shedding. The default value is enabled.

5. Click **Save**.

The mediation server's interface options are configured.

Configuring Mediation Server Advanced Settings

The Advanced configuration page is used to modify the configuration keys for the mediation server.

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

To configure an advanced setting on a mediation server:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the desired mediation server.
   The **Mediation Server Administration** page opens.
3. Select the **Settings** tab.
   The mediation server interface settings are displayed.
4. Click **Advanced**.
   The **Advanced Configuration Settings** page opens.
5. Add a configuration key to the table.
   a) Click **Add**. The Add Configuration Key Value window opens.
   b) Enter the name of the attribute to set in the **Configuration Key** field.
   c) Enter the value for the attribute in the **Value** field.
   d) Click **Save**.

Caution: The CMP server does not perform input validation on the configuration key name or value. If you overwrite a setting that is already configurable using the CMP interface, the value used by the mediation server is undetermined.

6. (Optional) Add, modify or delete keys 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.

7. Click **Save**.

The settings are applied to the selected mediation server.

Reapplying the Configuration to a Mediation Server

The CMP system lets you reapply the configuration to each mediation server. When you reapply the configuration, the CMP system completely reconfigures the mediation server with topology information, ensuring that the server configuration matches the data in the CMP database. This action is not needed during normal operation but is useful in the following situations:

- When the mediation 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 the failed servers' status.
- After upgrading the software on a mediation server, it is recommended that you reapply the configuration from the CMP system to ensure that the upgraded servers and the CMP database are synchronized.
- There are situations in which it is possible for mediation server configuration to go out of synchronization with the CMP system; for example, when a break in the network causes communication to fail between the CMP system and the server. Reapplying the configuration brings the mediation server back into synchronization with the CMP database.

To reapply the configuration associated with a mediation server:

1. From the **Mediation** 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 mediation server.
   The Mediation Server Administration page opens.
3. If it is not already selected, select the System tab.
   The Mediation Server Administration page opens, displaying information for the server.
4. Click **Reapply Configuration**.
   The profile information is saved to the mediation server.

The mediation server is synchronized with the CMP system.

Configuring Data Source Information

Use the **Data Sources** tab to configure a Subscriber Profile Repository (SPR) data source interface associated with the mediation server. The SPR data source can be one of the following:

- Oracle Communications Subscriber Database Management (SDM)
- Oracle Communications User Data Repository (UDR)

To configure the an SPR data source interface:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the server.
   The **Mediation Server Administration** page opens.
3. Select the **Data Sources** tab.
   The current data sources are displayed, listing the following information:
   - Administrative state
   - Name
   - Type
   - Primary address
   - Secondary address
4. To add a data sources, click **Modify**.
   a) Click **Add** and then select the data source type from the pulldown list.
   b) The **Add Data Source** window opens.
   c) Configure the data source values.

      You can configure the following values:

      - **Version**— 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.
      - **Unique Name** — The unique identifier of the data source server.
      - **Host** — The IP address of the data source server. The IP addresses of different data source servers must be unique and contain a destination port.
      - **User Name** — The name of the user. This field is used for authentication before connecting to SDM or UDR.
      - **Password** — The password of the user.
      - **Module Name** — The name of the module. This field is used for authentication.
      - **Key Transform Pattern** — This value allows routing between the mediation server and the data source server if the pattern matches.
5. (Optional) Add, modify, delete, or order data sources using the following functions.
   - 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.

6. Click **Save**.

Configuring FTP Settings

The configuration on CMP automatically replicates to the C-Level Mediation servers if the FTP setting are configured.

1. From the **Mediation** section of the navigation pane, select **FTP Setting**.
   The **FTP Setting** page opens displaying the FTP configuration.
2. Select **Enable** to turn on the FTP service.
3. Configure the batch operation setting.
   a) **Data File Path** —The location of the data file. Only characters, digits, hyphens (-) and underscores (_) are allowed in the path configuration.
   b) **Log File Path**—The location of the log file. Only characters, digits, hyphens (-) and underscores (_) are allowed in the path configuration.
   c) **User Name**—The user name cannot be modified.
   d) **Password**
4. Configure mediation synchronization.
   a) **User Name**—The user name cannot be modified.
   b) **Password**
5. Click **Save**.

Mediation Server Groups

For organizational purposes, you can aggregate mediation servers into groups. After a mediation server group is created, it can be populated with individual mediation servers. The following subsections describe how to manage mediation server groups.

Creating a Mediation Server Group

To create a mediation server group:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation servers; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Mediation Server Administration** page opens in the work area.
3. Click **Create Group**.
   The **Create Group** editor page opens.
4. Enter the name of the new mediation server group.

   The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
5. Click **Save**.

The mediation server group is created and appears in the content tree.

Modifying a Mediation Server Group

To modify a mediation server group:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the mediation server group you want to modify.
   The **Mediation Server Administration** page opens in the work area.
3. Click **Modify**.
   The **Modify Group** page opens.
4. Edit the information in the fields.
   The name cannot contain quotation marks (") or commas (,).
5. Click **Save**.

The mediation server group is modified.

Adding a Mediation Server to a Mediation Server Group

To add a mediation server to a mediation server group:

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

The **Mediation Server Administration** page opens in the work area, displaying the contents of the selected mediation server group.

3. Click **Add Mediation Server**.
   The **Add Mediation Server** page opens, displaying the mediation servers not part of the group.
4. Select the mediation server you want to add. Use the Ctrl or Shift keys to select multiple mediation servers.
5. Click **Save**.

The mediation server is added to the mediation server group.

Removing a Mediation Server from a Mediation Server Group

Removing a mediation server from a mediation server group does not delete the mediation server profile. To delete a mediation server profile, see *Deleting a Mediation Server Profile*.

To remove a mediation server from a mediation server group:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays the list of mediation server groups.
2. From the content tree, select the desired mediation server group.
   The Mediation Server Administration page opens in the work area, displaying the contents of the selected mediation server group.
3. Click the Delete icon, located to the right of the mediation server you want to remove.

The mediation server is removed from the group immediately; there is no confirmation message.

Deleting a Mediation Server Group

Deleting a mediation server group does not delete any mediation server associated with the deleted group; profiles remain in the ALL group. You cannot delete the ALL group.

To delete a mediation server group:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays the list of mediation server groups.
2. From the content tree, select the mediation server group you want to delete.
   The **Mediation Server Administration** page opens in the work area, displaying the contents of the selected mediation server group.
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the group.

The mediation server group is deleted.

Checking the Status of a Mediation Server

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

Group View Select **ALL** from the mediation server content tree to view all the defined mediation servers, or select a specific mediation 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 server configuration does not match the CMP database.

Mediation Server Profile View Select a mediation server from the content tree, then click the **System** tab to view the device's current operating status (**On-line** or **Off-line**) and profile configuration.

- **Trash can icon** — Click on the trash can icon to delete an MPE server.

Mediation 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 mediation server.

Report pages provide the following information:

Mode Shows whether data collection is currently:

- **Active**
- **Paused**
- **Absolute** (displaying statistics since the last reset)
- **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 depend 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 All Counters	Resets all counters under Protocol Statistics and Subscriber Statistics back to initial values.

Rediscover Cluster	Rediscovers the cluster, deleting any failed servers that have been removed from service.
Pause/Resume	Stops or restarts automatic refreshing of displayed information. The refresh period is 10 seconds.
Cancel	Returns to previous page.

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

Cluster	Information about the cluster.
Blades	Information about the individual physical components in the cluster.
Protocol Statistics	Information about the active network protocols.

Cluster Information Report

The fields that are displayed in the Cluster Information Report section for the mediation servers include the following:

- **Mode** — Whether the mediation server is active.
- **Cluster Status** — The status of the cluster:
  - **On-line**: If one mediation server, it is active; if two servers, one is active and one is standby.
  - **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.

Also within the Cluster Information Report is a listing of all the mediation servers (blades) contained within the cluster. A symbol () indicates which mediation 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, or Forced-Standby), number of server (blade) failures, and total uptime (time providing active or standby policy or GUI service).
- **Utilization** — Displays the percentage utilization of disk (of the /var/camiant filesystem), average value for the CPU utilization, and memory.

The **Actions** buttons let you restart the Policy Management software on the mediation server or restart the server itself.

Protocol Statistics

The Protocol Statistics section summarizes the protocol activity within the mediation server. 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 protocol statistics are:

SOAP Statistics	Requests made using the SOAP protocol.
SPR Statistics	Requests made to the UDR or the SDM functionality.

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.

Mediation Server Logs

The log files trace the activity of a mediation server. You can view and configure the logs for an individual cluster.

To view the log:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups.
2. From the content tree, select the desired mediation server.
   The Mediation Server Administration page opens in the work area.
3. On the Mediation Server Administration page, select the **Logs** tab.

   The Trace Log, which records application-level notifications, is displayed.

Viewing the Trace Log

The trace log records application notifications, such as protocol messages, policy messages, and custom messages generated by policy actions, for individual mediation servers. Trace logs are not replicated between mediation servers in a cluster, but they persist after failovers. You can use the log to debug problems by tracing through application-level messages. You can configure the severity of messages that are recorded in the trace log.

To view the Trace Log:

1. From the **Mediation** 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 mediation server.
   The **Mediation Server Administration** page opens in the work area.
3. Select the **Logs** tab.
   Log information for the selected device is displayed.
4. Click **View Trace Log**.

   The Trace Log Viewer window opens. While data is being retrieved, the in-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 *Policy Management Troubleshooting Guide*.
   - **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.

5. You can filter the events displayed using the following:

- **Trace Log Viewer for Server** — Select the individual mediation server within the cluster.
- **Start Date/Time** — Click the calendar icon, select the desired starting date and time, then click **Enter**.
- **End Date/Time** — Click the calendar icon, select the desired 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.
- **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.

After entering the filtering information, click **Search**. The selected events are displayed.

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** pulldown 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.

Click **Close**.

Configuring Trace Log Settings

From the **Logs** tab you can configure the log settings for the mediation servers in a cluster.

To configure log settings:

1. From the **Logs** tab, click **Modify**.
   The **Modify Trace Log Settings** page opens in the work area.
2. In the **Modify Trace Log Settings** section of the page, configure the Trace Log Level.

   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

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

3. Click **Save**.

The trace log settings are configured.

Configuring Synchronization Settings

Before the mediation server transfers the files, a data synchronization must be performed between the SPR and the mediation server.

To configure synchronization settings:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the server.
   The **Mediation Server Administration** page opens.
3. Select the **Sync** tab.
4. Click **Apply Sync**.
   The **Apply Sync Request** page opens.
5. Configure the synchronization settings.
   a) **Data Type** — Select from Subscriber and Service (default), Subscriber, or Service.
   b) **Data Consistency Type** — Select from Incremental (default) or All.
   c) **Valid Start Time** — Use the calendar to select a time for an incremental data synchronization to begin.
   d) **Valid End Time** — Use the calendar to select a time for an incremental data synchronization to end.

e) **User Range(7 or 8 bit number, split by comma(,))** — Enter one or more MSISDN prefixes, separated by commas. These prefixes are used as filters when the data set is sent to the system for a data consistency check.

6. Click **Apply**.

The synchronization settings are configured.

Resetting the Server State

You can send a request to recover the system state.

To reset the system state:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. From the content tree, select the server.
   The **Mediation Server Administration** page opens.
3. Select the **Sync** tab.
4. Click **Reset State**.
   The reset message is sent to the server.

Batch Task Status

You can view the status of batch tasks that the mediation server is processing. The task types that are displayed in the Batch Status view are:

- addBatSubscriber
- updateBatSubscriber
- delBatSubscriber
- addBatService
- updateBatService
- delBatService
- addBatUsrSessionPolicy
- updateBatUsrSessionPolicy
- delBatUsrSessionPolicy

Filtering Batch Task Status

The Batch Task Status can contain a large number of status messages. To reduce the number of messages in the view, you can filter by date, ID, type or status.

To filter the information:

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

The **Mediation Server Administration** page opens.

3. Select the **Batch Task Status** tab.
4. Specify the filtering parameters using any of the following fields.
   - **Start Date/Time** — Click (calendar icon), specify a date and time, and then click **Enter**.
   - **End Date/Time** — Click (calendar icon), specify a date and time, and then click **Enter**.
   - **Task ID** — Enter the ID for the task.
   - **Task Type** — Select one or more of the types listed in the pulldown. Options are:
     - addBatSubscriber
     - updateBatSubscriber
     - delBatSubscriber
     - addBatService
     - updateBatService
     - delBatService
     - addBatUsrSessionPolicy
     - updateBatUsrSessionPolicy
     - delBatUsrSessionPolicy
   - **Status** — The status of the task. Options are:
     - ALL (default)
     - PENDING
     - COMPLETED
     - ABORTING
     - RUNNING
5. Click **Filter**.
   The filtered log displays.

Viewing the Batch Task Status View

You view Batch Task Status message to see the current state of any batch task.

To view the batch status messages:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of mediation server groups; the initial group is **ALL**.
2. Select the mediation server managing the session you are interested in.
   The **Mediation Server Administration** page opens in the work area.
3. Select the **Batch Task Status** tab.
   The Batch Task Status view opens.

Exporting the Batch Task Status View

You can export the Batch Task Status view to a text file.

To export the view:

1. From the **Mediation** section of the navigation pane, select **Configuration**.

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

2. Select the mediation server managing the session you are interested in.
   The **Mediation Server Administration** page opens in the work area.
3. Select the **Batch Task Status** tab.
   The Batch Task Status view opens.
4. (Optional) Specify filtering parameters and click **Filter**.
   See *Filtering Batch Task Status* for more information on the filtering fields.
5. Click **Export**
   A file named `batch_tasks_export.txt` is generated, and a standard **File Download** window opens, so you can save or open the file.

Field Mapping Profiles

Field mapping defines the adaptor fields between the SPR and the Business & Operation Support System (BOSS). There are four types of mapping profiles:

- Subscriber
- Service
- User Session Policy
- User Location

These types are fixed, and cannot be edited or deleted.

A configure mismatch is shown when the mapping records are inconsistent, and require a re-apply to resolve the mismatch.

Creating Field Mapping Profiles

To create a Field Mapping Profile:

1. From the **Mediation** section of the navigation pane, select **Field Mapping Profiles**.
   The content tree displays a list of profile groups.
2. From the content tree, select the profile group. The groups are:
   - **Subscriber**
   - **Service**
   - **User Session Policy**
   - **User Location**
3. Click **Create**.
   The **New Mapping Record** page opens.
4. Configure the field mapping using the following options:
   a) **Name** — The name of the field mapping profile.
   b) **Sequence** — A numeric value specifying the order that the mapping records are displayed on the group page. The default is 0.
   c) **SOAP Field Name** — The name of the SOAP field.
   d) **SPR Field Name** — The name of the SPR field.

e) **Mandatory** — Defines if the field is required. The default is **No**.
f) **Default Value**—The default value for the field.
g) **Validation Rules**—The rules used to validate the data in the field.

5. Click **Save**.

The mapping is created and added to the selected Field Mapping Profiles group.

Viewing a Field Mapping Profile

Field mapping defines the adaptor fields between the SPR and the Business & Operation Support System (BOSS).

To view a Field Mapping Profile:

1. From the **Mediation** section of the navigation pane, select **Field Mapping Profiles**.
   The content tree displays a list of profile groups.
2. From the content tree, select the profile group. The groups are:
   - **Subscriber**
   - **Service**
   - **User Session Policy**
   - **User Location**

   The profiles defined for the type are displayed in the work area.
3. Select a profile.
   The mapping configuration displays in the work area.

Modifying a Field Mapping Profile

Field mapping defines the adaptor fields between the SPR and the Business & Operation Support System (BOSS).

To modify a Field Mapping Profile:

1. From the **Mediation** section of the navigation pane, select **Field Mapping Profiles**.
   The content tree displays a list of profile groups.
2. From the content tree, select the profile group. The groups are:
   - **Subscriber**
   - **Service**
   - **User Session Policy**
   - **User Location**

   The profiles defined for the type are displayed in the work area.
3. Select a profile.
   The mapping configuration displays in the work area.
4. Click **Modify**.
   The **Modify Mapping Record** page opens.
5. Modify the configuration.
6. Click **Save**.

Deleting a Field Mapping Profile

Field mapping defines the adaptor fields between the SPR and the Business & Operation Support System (BOSS).

To delete a Field Mapping Profile:

1. From the **Mediation** section of the navigation pane, select **Field Mapping Profiles**.
   The content tree displays a list of profile groups.
2. From the content tree, select the profile group. The groups are:
   - **Subscriber**
   - **Service**
   - **User Session Policy**
   - **User Location**

   The profiles defined for the type are displayed in the work area.
3. Use one of the following methods to select the Field Mapping Profile to delete:
   - From the work area, click (trash can) located next to the profile you want to delete.
   - From the profile group tree, select the profile. The profile displays in the work area. Click **Delete**.

   A confirmation message displays.
4. Click **OK** to delete.

The profile is removed from the profile group and the system.

Chapter 11

About Subscriber Profile Repositories

Topics:

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 can identify the account for the subscriber. You can enter up to 255 characters.
      - **Billing Day** — The day of the month on which the subscriber's associated quota is reset. For the UDR or the SDM system, the valid range is 0 - 31. For the mediation server, the valid values are 1 - 28 or 97 (the reciprocal third day in each month), 98 (the reciprocal second day in each month), or 99 (the last day in each month). To resolve the value gap between the UDR or the SDM and the mediation server, values of 97, 98, and 99 on the mediation server are translated to 29, 30, and 31, respectively, before being sent to the UDR or the SDM system.
      - **Tier** — The subscriber's tier. 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 tiers.

- **Entitlements** — The subscriber's entitlements. 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.

  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.
- **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** (not visibile with V4 profile) — 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.

- **Package Type** (optional with V4 profile)— Indicates if the user is subscribing to the package.
- **Operate Time** (required with V4 profile)—The length of time the package is available. Specified in the 24-hour format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. (

4. Click **Save**.

The subscriber profile is defined.

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. 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. 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 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 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-dd*T*hh*:*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 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-dd*T*hh*:*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:

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.
5. Click **Search**.
   If sessions are available for the subscriber, **Subscriber Session Data** page appears. *Figure 24: 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.

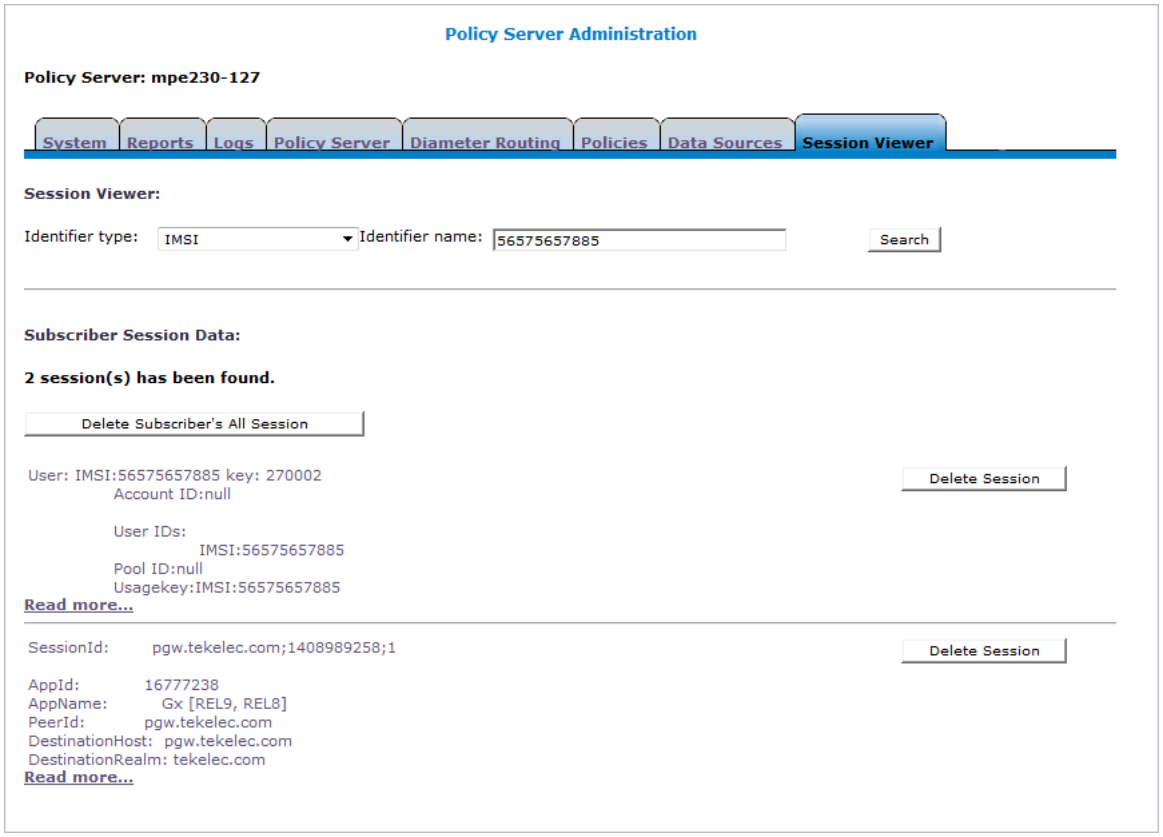


Figure 24: Session Viewer Page

Chapter 13

System-Wide Report

Topics:

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
- Physical 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.

Figure 25: 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)

Filters | Change Thresholds

	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 25: 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.

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.

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 the mapping is described for all three servers. *Table 6: KPI Definitions for MRA Devices* shows the mappings for MRA devices; *Table 7: 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 8: 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 6: 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
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	None
Active Subscribers	CurrentMRABindingCount and CurrentMRABindingPercentageOf Capacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby and spare server (spare only shows Status, CPU % and Memory%)**
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 7: 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 CurrentPDNConnectionPercentageOf Capacity	None

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
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 8: 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

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
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 9: Policy Statistics*
- *Table 10: Quota Profile Statistics Details*
- *Table 11: Diameter Application Function (AF) Statistics*
- *Table 12: Diameter AF Peer Stats (in Diameter AF Stats window)*
- *Table 13: Diameter Policy Charging Enforcement Function (PCEF) Statistics*
- *Table 14: Diameter Charging Function (CTF) Statistics*
- *Table 15: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics*
- *Table 16: Diameter TDF Statistics*
- *Table 17: Diameter Sh / Sh Peer Statistics*
- *Table 18: Diameter Distributed Routing and Management Application (DRMA) Statistics*

- *Table 19: Diameter DRA Statistics*
- *Table 20: Diameter Sy Statistics*
- *Table 21: RADIUS Statistics*
- *Table 22: Diameter Latency Statistics*
- *Table 23: Diameter Event Trigger Statistics*
- *Table 24: Diameter Protocol Error Statistics*
- *Table 25: Diameter Connection Error Statistics*
- *Table 26: LDAP Data Source Statistics*
- *Table 27: Sh Data Source Statistics*
- *Table 28: Sy Data Source Statistics*
- *Table 29: KPI Interval Statistics*

For more information on the OSSI XML interface, see *OSSI XML Interface Definitions Reference*.

Table 9: 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
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 10: 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

Display	MPE	MRA	Name
Event Threshold Reached	Y	N	Quota Event Threshold Reached Count

Table 11: 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
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

Display	MPE	MRA	Name
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 12: Diameter AF Peer Stats (in Diameter AF Stats window)

Display	MPE	MRA	Name
ID	Y	Y	
IP Address: Port			
Currently active connections			
Currently active sessions			
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time

Table 13: 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

Display	MPE	MRA	Name
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
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 14: 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
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

Display	MPE	MRA	Name
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 15: 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
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

Display	MPE	MRA	Name
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 16: 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
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

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
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 17: 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
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count
UDR messages timeout	Y	N	UDR Timeout Count
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

Display	MPE	MRA	Name
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
PUR messages received/sent	Y	N	PUR Messages Received Count\PUR Messages Sent Count
PUR messages timeout	Y	N	PURTimeout Count
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
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 18: 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

Display	MPE	MRA	Name
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	
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	

Display	MPE	MRA	Name
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
LNR messages timeout	Y	Y	LNRTimeout 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 19: 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
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 20: 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

Display	MPE	MRA	Name
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
Currently active sessions	Y	N	Active Sessions Count
Max active sessions	Y	N	Maximum Active Sessions Count
Diameter Sy connections			

Table 21: 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

Display	MPE	MRA	Name
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	
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	

Display	MPE	MRA	Name
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	
Invalid subscriber identifier specified. Message dropped	Y	Y	Unknown Subscriber Request Count

Table 22: 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 22: 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

Display	MPE	MRA	Name
			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 23: Diameter Event Trigger Statistics

Display	MPE	MRA	Name
Diameter Event Trigger Stats by Code	Y	N	
Diameter Event Trigger Stats by Application:			
Diameter PCEF Application Event Trigger	Y	N	
Diameter BBERF Application Event Trigger	Y	N	

Table 24: 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 25: 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

Display	MPE	MRA	Name
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 26: 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
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 27: Sh Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count

Display	MPE	MRA	Name
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
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	

Display	MPE	MRA	Name
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
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 28: 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

Display	MPE	MRA	Name
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 29: KPI Interval Statistics

Display	MPE	MRA	Name
Interval Start Time	Y	Y	Interval Start Time
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 60 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.

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**
- 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.
- 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. Select **Enable** to start the trace for the subscriber ID.
6. Click **Save**.
7. (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.

8. Click **Save**.

The Subscriber Identifier List is populated with the defined subscribers. You have defined and saved the subscribers in the **Subscriber Identifier List**.

Table 30: Status and Related Icons

Status	Icon	Condition
Running		Indicates the log is currently active (running). This status occurs when: • 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.

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 26: Trending Report Definition Configuration Page* shows a sample.

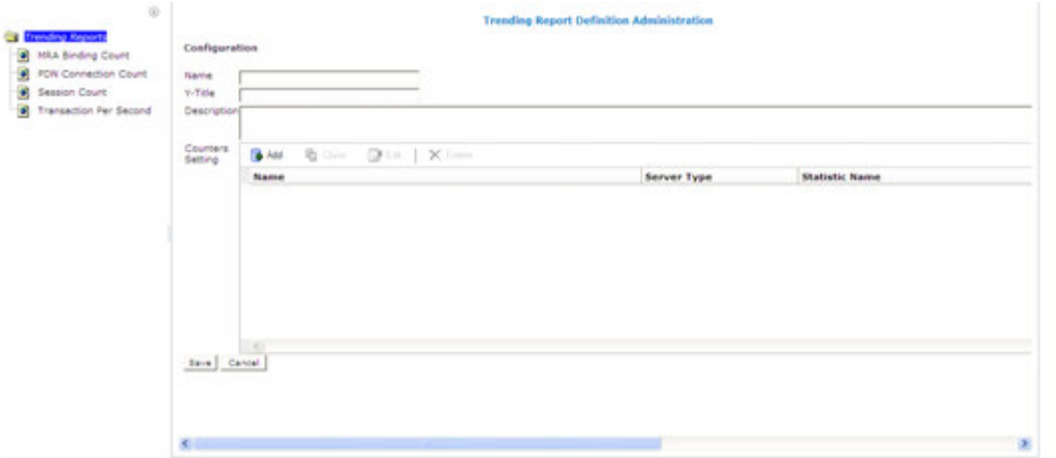


Figure 26: Trending Report Definition Configuration Page

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.

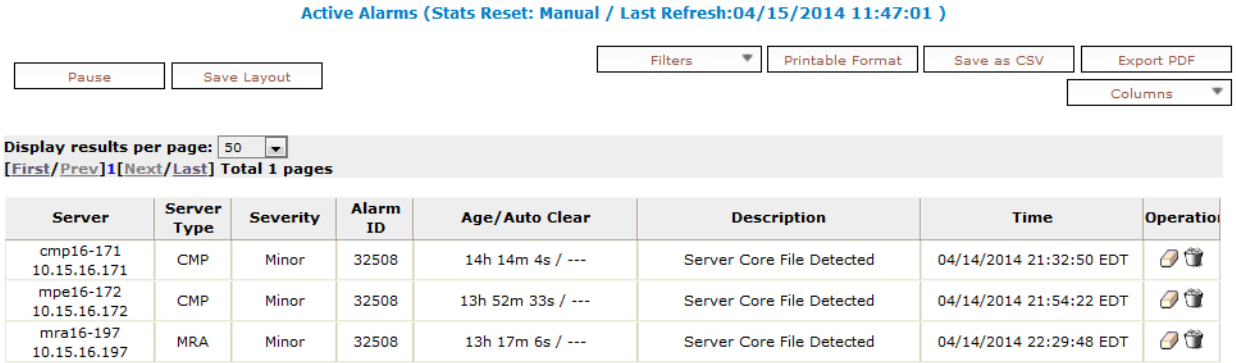
Viewing Active Alarms

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 27: Sample Active Alarms Report shows a sample active alarm report.



Server	Server Type	Severity	Alarm ID	Age/Auto Clear	Description	Time	Operatio
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 27: 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:

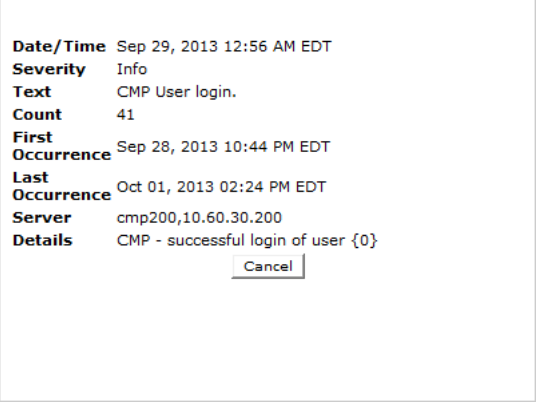


Figure 28: Alert Details

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 29: Sample Connection Status Report shows a sample connection status report.

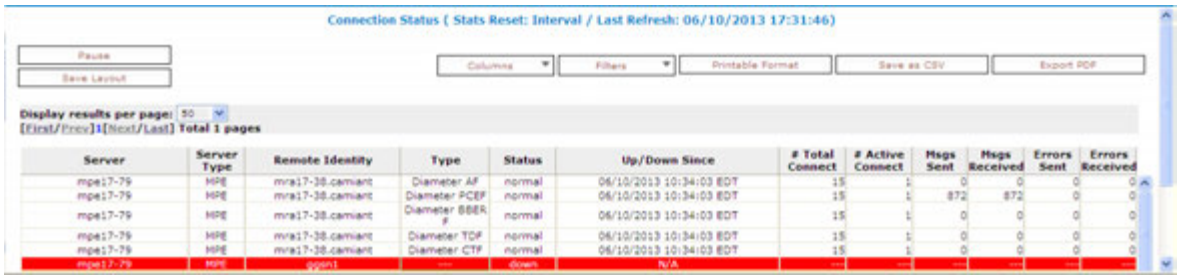


Figure 29: Sample Connection Status Report

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 30: Sample MPE/MRA Replication Statistics Report shows a sample replication report.

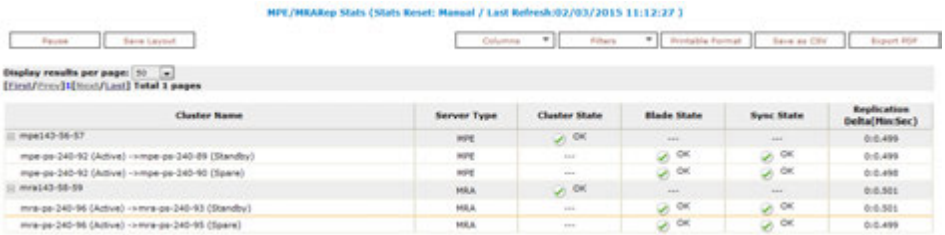


Figure 30: Sample MPE/MRA Replication Statistics Report

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 31: 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
Forcestandby	Minor	Warning Sign
Out of Service	Critical	Red X
Unknown	Critical	Red X

- **Sync State** — displays the values reported from COMCOL.

Table 32: 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
Down Connecting	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
Down Handshake	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
Connected Reinit	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
Connected Incompat	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 33: 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.

Chapter 14

Upgrade Manager

Topics:

The Upgrade Manager lets you 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 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.

Before upgrading, it is recommended that you contact My Oracle Support. See *https://support.oracle.com* for more information.

About ISO Files on Servers

Policy Management software upgrades are distributed and stored for use as ISO files, which are archive files of optical (DVD) discs.

Use the **ISO Maintenance** option to show the current Policy Management software version executing on servers, and determine what ISO files are available to use for upgrades. Operations performed from here include distributing ISO files to servers, deleting ISO files from servers, and pushing the upgrade script to servers. An audit log is generated for each operation that occurs on this page.

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.

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 34: ISO Maintenance Page Elements describes the elements on the **ISO Maintenance** page.

Table 34: ISO Maintenance Page Elements

Element	Description
(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.
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.

Element	Description
	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. **Note:** After an operation is confirmed, it cannot be cancelled.

Viewing the ISO Status of Servers

Use this procedure to view the status of in-service servers before, during, and after a software upgrade.

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
   The **ISO Maintenance** page appears.

2. (Optional) Click **Filters** and specify the criteria to customize the list of servers that display in the table.
3. (Optional) Click **Columns** and select columns to customize the table.

All in-service servers that meet the filter criteria are listed. Server information is updated every ten seconds.

Pushing a Script to the Servers

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

Before adding an ISO file to a server, you should ensure that the directory `/var/TKLC/upgrade` is empty on that 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.

Preparing for an Upgrade

Upgrading a server requires a large amount of preparation. For detailed information about preparing for an upgrade, please see the My Oracle Support website (*https://support.oracle.com*).

Caution: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, go to the My Oracle Support website and review any relevant Technical Service Bulletins (TSBs). Use only the upgrade procedure provided by My Oracle Support.

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.

Note: In Policy Management version 9.3, secure connections used port 443. Before upgrading from version 9.3 to version 11.5, disable **Secure Connection** until all devices are upgraded. For more information, see *Creating a Policy Server Profile*.

About Performing an Upgrade

The information in this section is a general overview of the Upgrade Manager steps you take to upgrade a cluster or servers. Specific details, including the order in which systems are upgraded, are provided by My Oracle Support. See *https://support.oracle.com* for more information.

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.

A server must display **Forced Standby** in the Server State column on the **System Maintenance** page before a software upgrade can be performed on that server.

Before upgrading any server in any cluster of the Policy Management network:

1. Use **Upload ISO** to obtain upgrade files.
2. Use **Push Script** to distribute upgrade files to each server.

You must upgrade the primary-site CMP cluster first. To upgrade a primary-site CMP cluster:

1. On the active server of the primary-site cluster, execute the command **`policyUpgrade.pl --prepareUpgrade`**. (For details of this script and how to execute it, contact My Oracle Support. See *https://support.oracle.com* for more information.)
2. Select the standby server of both the primary-site and secondary-site cluster and apply **Force Standby**.
3. Select the forced standby server of the primary-site cluster and apply **Start Upgrade** to begin the upgrade process on that server.
4. Select the primary site and apply **Switch ForceStandby** to make the standby server active and the active server standby. You are logged out of the CMP system.
5. Log in to the CMP system, select the forced standby server, and apply **Start Upgrade** to begin the upgrade process on that server.
6. Select the forced standby server and apply **Cancel Force Standby** to make it standby.
7. Select each server and apply **Upgrade Completion**.

After you upgrade the primary-site CMP cluster, you can upgrade a secondary-site CMP cluster. To upgrade a secondary-site CMP cluster:

1. Select the forced standby server of the secondary-site cluster and apply **Start Upgrade** to begin the upgrade process on that server.
2. Select the secondary site and apply **Switch Force Standby** to make the standby server active and the active server standby.
3. Select the forced standby server and apply **Start Upgrade** to begin the upgrade process on that server.
4. Select the forced standby server and apply **Cancel Force Standby** to make it standby.
5. Select each server and apply **Upgrade Completion**.

To upgrade a non-georedundant MPE or MRA cluster:

1. Select the active server of the cluster and apply **Turn Off Replication** to stop replication traffic.
2. Select the standby server of the cluster and apply **Force Standby**.
3. Select the forced standby server of the cluster and apply **Start Upgrade** to begin the upgrade process on that server.
4. Select the cluster and apply **Switch Force Standby** to make the standby server active and the active server standby.
5. Select the cluster and apply **Reapply Configuration** (see *About Reapplying a Configuration*) to distribute configuration information to it.
6. Select the forced standby server and apply **Start Upgrade** to begin the upgrade process on that server.
7. Select the active server of the cluster and apply **Turn On Replication** to restart replication traffic.
8. Select the standby server and apply **Cancel Force Standby** to make it standby.
9. Select each server and apply **Upgrade Completion**.

To upgrade a georedundant MPE or MRA cluster:

1. Select the active and spare servers of the cluster and apply **Turn Off Replication** to stop replication traffic.
2. Select the standby server of the cluster and apply **Force Standby**.
3. Select the forced standby server of the cluster and apply **Start Upgrade** to begin the upgrade process on that server.
4. Select the spare server of the cluster and apply **Force Standby**.
5. Select the cluster and apply **Switch Force Standby** to make the standby server active and the active server standby.
6. Select the cluster and apply **Reapply Configuration** (see *About Reapplying a Configuration*) to distribute configuration information to it.
7. Select the forced standby server and apply **Start Upgrade** to begin the upgrade process on that server.
8. Select the spare server of the cluster (at the georedundant site) and apply **Force Standby**.
9. Select the forced standby server and apply **Start Upgrade** to begin the upgrade process on that server.
10. Select the active server of the cluster and apply **Turn On Replication** to restart replication traffic.
11. Select the standby server and apply **Cancel Force Standby** to make it standby.
12. Select each server and apply **Upgrade Completion**.

After the upgrade is accepted, the last step is to select each server and apply **Accept Upgrade**.

Note: An upgrade must be accepted (or rejected) before any subsequent upgrade can occur.

System Maintenance Elements

On the **Upgrade Manager** menu, **System Maintenance** is an option. All servers in the topology appear in the server table on this page. Servers display in groups by cluster; clusters can be collapsed or expanded by clicking the [-] or [+] icons in the first column of the table. Server information is updated every ten seconds.

There are three types of elements that appear on the **Upgrade Manager** page:

- Checkboxes to select servers/ISOs on which to perform operations.

- Table of filtered servers.
- Pulldown menus (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for performing operations.

Table 35: System Maintenance Elements describes all of the elements. *Table 36: System Maintenance Operations* describes all the operations.

Table 35: System Maintenance Elements

Element	Description
(checkbox)	Use the checkbox column to select the servers on which an operation is to be performed. If you select a main cluster server, all servers in that cluster are selected. **Note:** At least one server must be selected before you can select an operation from the **Operations** pulldown menu.
Name	Displays the server name of each server. When a server is in the process of being upgraded, a special upgrade icon appears next to the name. Likewise, if a server upgrade has failed, a special failed icon appears next to the name. If current information on a server is unavailable, a "synch broken" icon ( ) appears next to the name.
Appl Type	Displays the type of Policy Management application running on each server. The **Filters** pulldown menu allows you to display **CMP Site1 Cluster only**, **CMP Site1 Cluster only**, **MPE**, **MRA**, or **All**.
Site	Displays the georedundant site name, if any, that is associated with each server. The **Filters** pulldown menu allows you to display Unspecified only or All servers.
IP	Displays the IP address of each server. The **Filters** pulldown menu allows you to display only the server with a specific IP address or All servers.
Server State	Displays the state of each server. The server state can appear in different colors, depending on the state displayed. The **Filters** pulldown menu allows you to display **Active** only, **Standby** only, **Out-Of-Service** only, **Force Standby** only, or **All** servers (the default).
ISO	Displays the ISOs or CD-ROM on each server. Use the checkbox to select an ISO to use during an upgrade on that server.
Prev Release	Displays the previous Policy Management software release of each server, if known. The **Filters** pulldown menu allows you to display a specific release only or **All** releases.
Running Release	Displays the current Policy Management software release of each server. The **Filters** pulldown menu allows you to display a specific release only or **All** releases.
Replication	Displays whether replication is On or Off.
Upgrade Status	Displays details of last upgrade performed on each server.

Element	Description
Columns	Use the **Columns** pulldown menu to change the columns that appear on this page. By default, all columns appear. To change which columns appear, uncheck the columns to be removed from the page. The Name column is mandatory.
Filters	Use the **Filters** pulldown menu to select a subset of servers to appear on this page. On this menu are the following pulldown filter submenus: **Appl Type**, **Site**, **IP**, **State**, **Prev Release**, and **Running Release**. These filters are set to **All** by default, so all servers appear initially. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	Use the **Operations** pulldown menu to select an upgrade operation to perform. **Note:** At least one server must be selected before you can select an operation from the **Operations** pulldown menu. The operations that appear in the pulldown menu depend on the state of the servers that are selected. In other words, when more than one server is selected, only the operations that are applicable to all selected servers appear. See *Table 36: System Maintenance Operations* for the possible operations. As a protective feature, when a command is executed, a warning message pops up, asking if you are sure you want to execute this operation (you can click **OK** or **Cancel**). If you click **OK**, a progress bar displays the status of the command completion in a pop-up window. **Note:** Once the operation is confirmed, it cannot be cancelled.

Table 36: System Maintenance Operations

Operation	Description
Push Script	Pushes script to remote server. Upgrade Manager uses the script to communicate with the remote server and to perform the upgrade or backout.
Upload ISO	Adds ISO to the specified Policy Management products.
Force Standby	Forces the selected server(s) into standby status. CAUTION **Caution:** Setting Force Standby for all servers in a cluster effectively removes the cluster from service. **Note:** You cannot force both servers of a CMP cluster into Standby status.
Prepare Upgrade	Turns off COMCOL replication of database tables.
Upgrade Completion	Turns off legacy replication.

Operation	Description
Undo Upgrade Completion	Prepare for a backout of a software upgrade. This process turns on legacy replication for all the clusters.
Switch ForceStandby	Switches the upgraded server to active and the previously active server to forced standby in order to upgrade it.
Cancel Force Standby	Cancels the Force Standby status.
Start Upgrade	Begins the upgrade with selected ISO on each server.
Accept Upgrade	Removes backout information. Once the upgrade is accepted for any server in a cluster, the cluster cannot be rolled back. The server's status must be Force Standby and the upgrade status must be Pending. Clears alarm 32532 ("Upgrade Pending Accept/Reject"). If the upgrade results in a conversion of the file system, the server restarts. **Note:** If a server fails after an upgrade is accepted, you must accept the upgrade again for the replacement server.
Backout	Initiates a backout on the selected server(s).

Viewing Upgrade Status of Servers

Use this procedure to view the status of in-service servers before, during, and after a software upgrade.

1. From the **Upgrade Manager** section of the navigation pane, select **System Maintenance**.
   The **System Maintenance** page appears.
2. (Optional) Click **Filters** and specify the information to customize the list of servers that display in the table.
3. (Optional) Click **Columns** to select columns display in the table.

All in-service servers that meet the filter criteria are listed. Server information is updated every ten seconds.

About Rolling Back an Upgrade

It is possible to roll back, or back out, the Policy Management software to the previous version in a production environment until the upgrade is accepted. Procedures and scripts are available to preserve the current state of subscriber data, such as MPE sessions. Before beginning a rollback, contact My Oracle Support and inform them of your plans.

Note: When an upgrade is accepted with the**Accept Upgrade** operation, it cannot be rolled back.

Rollback is subject to the following limitations:

- You can roll back one version only, regardless of whether the last upgrade was a major, minor, or maintenance release.
- If any new features are enabled, you must disable them before rolling back the upgrade.
- Subscriber sessions affected by new features may be affected.

If you decide to roll back an upgrade, you should do so in reverse order. That is, first roll back the last cluster you upgraded, then the previous one, and so on, and then roll back CMP clusters. After the systems are rolled back to a previous release, they can be upgraded to another supported version.

Chapter 15

Global Configuration

Topics:

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 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 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 60 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 60. The default is 60.
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.

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 16

System Administration

Topics:

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**.

The system settings are configured.

Figure 31: 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.

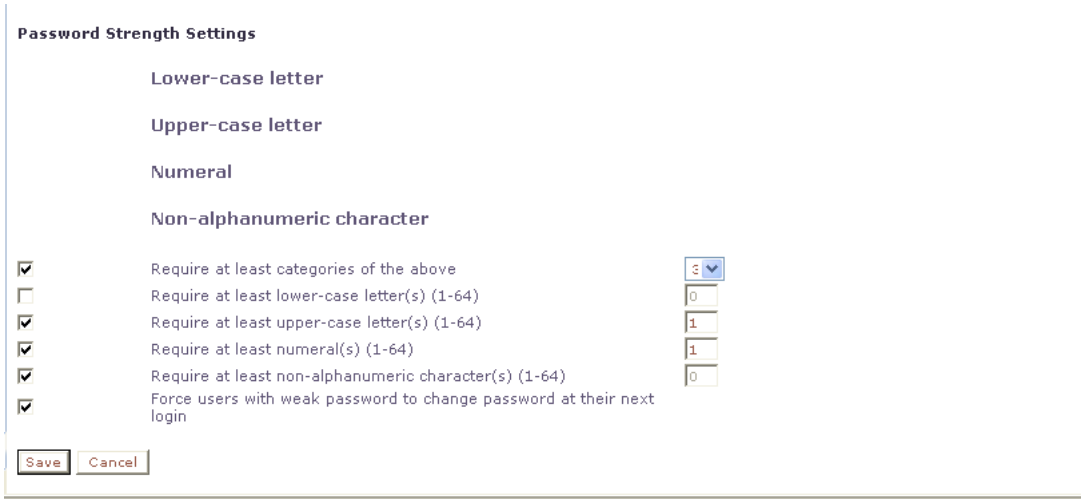


Figure 31: Sample Password Strength Policy

Importing and Exporting Configurable Objects

In addition to defining manageable objects manually, you can add them to the CMP database using the OSSI XML Interface or by importing them from an XML file. You can also export a list of objects of various types to an XML output file. This section describes the OSSI XML interface and the XML bulk import and export processes.

This section describes how to perform a simple or a bulk export of configurable objects and how to import object configurations into the CMP system.

Using the OSSI XML Interface

The OSSI XML interface provides access to raw data in the system directly via HTTP. The system data is entered and returned as XML documents in accordance with a defined schema. The schema for the input XML is provided to specify exactly which attributes of a manageable object are permitted on import, as well as the formatting for those attributes.

You can also define object groups as part of the XML file and import them within the same file. Groups let you define a logical organization of objects within the CMP database at the time of import. Group structures include not only group attributes, but also relationships between groups, subgroups, and objects.

The OSSI XML interface includes the following:

- **Topology Interface** — Allows you to query and manage network elements within the system
- **Operational Measurements (OM) Interface** — Allows you to retrieve statistical data from the system
- **Identity Management** — Allows you to configure user names, passwords, and roles
- **Policy Tables** — Allows you to export policy tables, and import them to add, edit, replace or delete a table

For detailed information, see *OSSI XML Interface Definitions Reference*.

Importing an XML File to Input Objects

During the import process, object definitions are read one at a time from the user-specified XML file. Each object is then validated and checked against the existing database for collisions (duplications). Collisions are detected based on the object name, which is a unique database key. If the object already exists within the system, the existing object's attributes are updated (overwritten) by the attributes specified in the XML file being imported. If the object does not exist within the system, the object is created and imported as a new object. A blank element value is replaced with a default or null value, as appropriate.

An XML import is limited to 20,000,000 bytes. If you try to import a file larger than that the import will fail with a result code of 102 (input stream error).

Note: Export the existing database of objects before starting an import operation to ensure that you can recreate the previous state if necessary (see *Exporting an XML File*).

To use an XML file to input defined objects:

1. From the **System Administration** section of the navigation pane, select **Import/Export**. The **Import/Export** page opens in the work area.

   Note: Do not select **Policy Import/Export**, in the **Policy Management** section; that is a different function.

2. On the **Import/Export** page:
   - Enter the file name of the XML import file
   - Click **Browse** and select the file.

3. Select what to import:
   - * (specifies import all types) (default value)

     Note: When importing NRM/PM template files, the corresponding type must be selected. If the default value of asterisk (*) is used, the import will fail.

   - **Network Elements**
   - **Tiers**
   - **Serving Gateway/MCC-MNC Mapping**
   - **Traffic Profiles**
   - **Retry Profiles**
   - **Quotas**
   - **Services**
   - **Charging Servers**
   - **Time Periods**
   - **Quota Conventions**
   - **Match Lists**
   - **Monitoring key**
   - **Custom AVP Definition**
   - **Customer Vendor**
   - **Policy Table**
   - **Policy Counter ID**
   - **PRA Lists**

- **Applications**
- **Roles**
- **Scopes**
- **Users**
- **NRM**
- **PM**
- **Mediation Subscriber Profile Mapping**
- **Mediation Quota Profile Mapping**
- **Mediation Field Mapping Profile**

If you select **Network Elements**, additional filtering fields display to help you manage the volume of data being imported. You can filter by network element name or Diameter identifier. Each additional field accepts a string that can include the wildcard characters * (to represent any string) and ? (to represent any character). By default, all elements matching the filter are included. For each field you can select the operators **AND**, **OR**, **AND NOT**, or **OR NOT**; if you select an operator, an additional statement field displays. You can specify up to six logical combinations of filtering statements.

Note: The concatenation of all filters is left associative. For example, C1 AND C2 OR C3 equals (C1 AND C2) OR C3. The NOT operator affects the succeeding statement(s); for example, C1 AND NOT C2 AND C3 equals C1 AND (NOT C2) AND C3.

4. Click **Import**.
   Data from the XML file is imported. If the operation takes more than five seconds, a progress bar displays.

Following the import, status messages provide the total counts of all successful imports, updates, and failures. Click **Details** (the button is below the status messages) to open a window containing detailed warnings and errors for each object. The error messages contain identifying information for the XML structure that caused the error, allowing you to pinpoint and fix problems in the XML file.

For each User element, ensure that Role and Scope data is also defined. The recommended sequence of elements in the XML import file is Network Element, Role, Scope, and then User.

If an imported user password does not satisfy the current password rules, the user will have to change passwords on first login. Password expiration timestamps are imported, so the passwords will expire on the schedule of the CMP system from which they were exported.

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. See *Setting the Precedence Range* for more information.

Exporting an XML File

The Export feature creates an XML file containing definitions for objects within the CMP database, in the same schema used on import. You can back up data by exporting it to an XML file, and restore it by importing the same file. The export file can also be transferred to a third-party system. To export an XML file:

1. From the **System Administration** section of the navigation pane, select **Import/Export**.
   The **Import/Export** page opens in the work area.

   Note: Do not select **Policy Import/Export**, in the **Policy Management** section; that is a different function.

2. Select the type of export:
   - **Network Elements** (default)
   - **Tiers**
   - **Serving Gateway/MCC-MNC Mapping**
   - **Traffic Profiles**
   - **Retry Profiles**
   - **Quotas**
   - **Quota Conventions**
   - **Match Lists**
   - **Charging Servers**
   - **Time Periods**
   - **Monitoring key**
   - **Custom AVP Definition**
   - **Policy Table**
   - **PRA Lists**
   - **Applications**
   - **Roles**
   - **Scopes**
   - **Users**
   - **Mediation Subscriber Profile Mapping**
   - **Mediation Quota Profile Mapping**
   - **Mediation Field Mapping Profile**

   The user accounts datacollector, LIadmin, and _policy_server cannot be exported. The role LIadmin cannot be exported.

   If you select **Network Elements**, additional filtering fields display to help you manage the volume of data being exported; you can filter by network element name, or Diameter identifier. Each additional field accepts a string that can include the wildcard characters * (to represent any string) and ? (to represent any character). By default, all elements matching the filter are included. For each field you can select the following operators:

   - **AND**
   - **OR**
   - **AND NOT**
   - **OR NOT**

   If you select an operator, an additional statement field displays. You can specify up to six logical combinations of filtering statements.

   Note: The concatenation of all filters is left associative. For example, C1 AND C2 OR C3 equals (C1 AND C2) OR C3. The NOT operator affects the succeeding statement(s); for example, C1 AND NOT C2 AND C3 equals C1 AND (NOT C2) AND C3.

3. Click **Export**.
   A standard file download window opens, and you are prompted to open or save the file.
4. Click **Save** to save the file.
   Data exported to an XML file. If the operation takes more than five seconds, a progress bar displays.

User passwords are exported in encrypted text. Password expiration timestamps are retained, so the passwords will expire on the schedule of the CMP system from which they were exported.

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 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. 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 (calendar icon), specify a date and time, and then click **Enter**.
   - **End Date/Time** — Click (calendar icon), 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.

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** (the 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

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

4. Click **Save**.

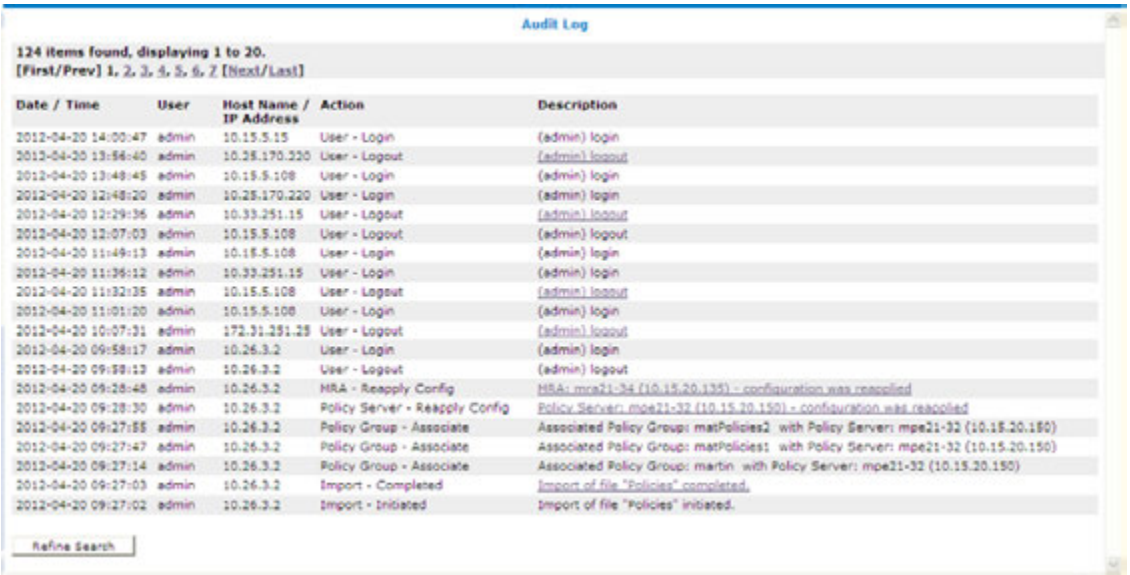
The system trace log settings are configured.

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 32: 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]

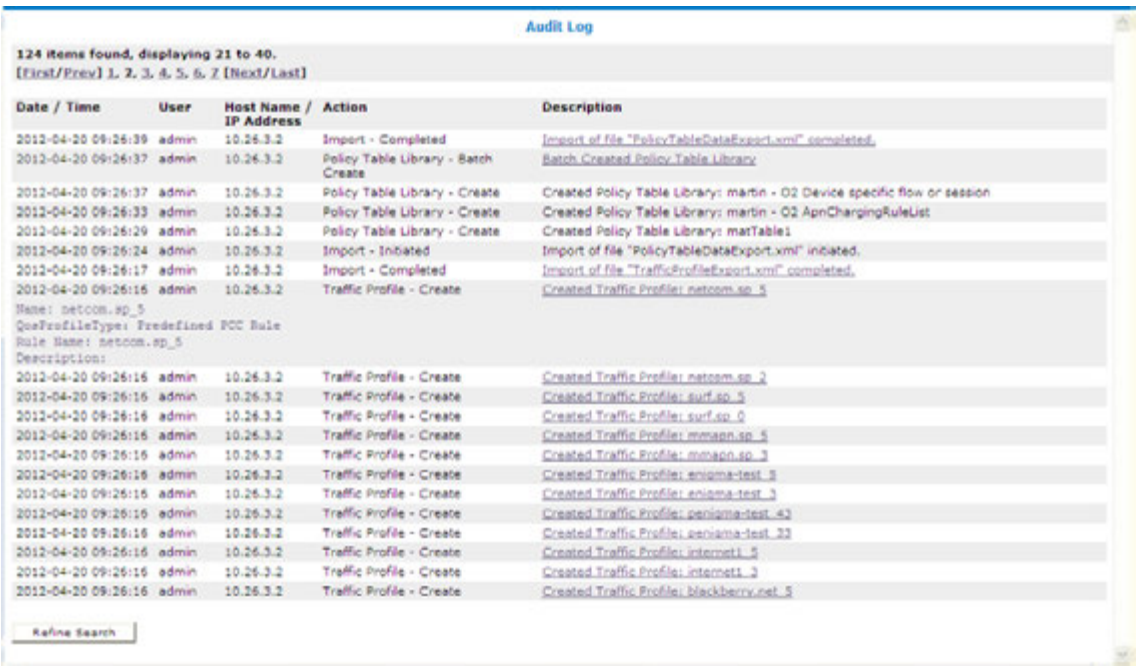
Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 14:00:47	admin	10.15.5.15	User - Login	(admin) login
2012-04-20 13:56:40	admin	10.25.170.220	User - Logout	(admin) logout
2012-04-20 13:48:45	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 12:48:20	admin	10.25.170.220	User - 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: mra21-34 (10.15.20.135) - configuration was reapplied
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 reapplied
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 32: Audit Log

For a detailed description of an item, click the underlined description. The details of the event display. (*Figure 33: Audit Log Details* shows an example.)

To filter search results, click **Refine Search**, located at the bottom of the page. (See *Searching for Audit Log Entries*.)



Audit Log

124 items found, displaying 21 to 40.
[First/Prev] 1, 2, 3, 4, 5, 6, 7 [Next/Last]

Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 09:26:39	admin	10.26.3.2	Import - Completed	Import of file "PolicyTableDataExport.xml" completed.
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Batch Create	Batch Created Policy Table Library
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 Device specific flow or session
2012-04-20 09:26:33	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 ApnChargingRuleList
2012-04-20 09:26:29	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: matTable1
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 PCC 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: mmapn.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmapn.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: genigma-test_43
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: genigma-test_33
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

Refine Search

Figure 33: 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 of these tasks to better manage network load or to propagate a network element change to the Policy Management devices on demand. You can also abort a running task.

CAUTION

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	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. **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. **Note:** If access to configuration is restricted to Read-Only, you will not be able to configure this task.

Health Checker Periodically checks the MPE devices to ensure that they are online.

SMS Notification Statistics Uploading Uploads SMS notification statistics files to the defined remote server. The default interval is one hour. The statistics files contain logs of all generated CMPP SMS messages. The logs include SMS sending times and results, triggering policy IDs and names, subscriber IDs, connection IDs, and message IDs.

This task retries when the remote server is unreachable if the retry limit is set to greater than 0. If the task cannot reach the remote server, a major alarm is triggered. The task clears the alarm if it succeeds at the next scheduled interval. If an upload period is missed, any files from the missed upload period are uploaded at the next scheduled interval.

Note: A remote server must be defined before beginning this task. If no remote server is defined, this task will fail. Remote server information that must be defined is: Host Name/IP Address, FTP user credentials, and the path of the remote repository.

Note: This task depends on the SMS Relay configuration. The CMCC mode must be enabled and the CMPP log level must be set to INFO. See *Configuring a CMPP Client-based SMSR* for information about SMS Relay configuration.

OM Statistics 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.

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. *OSSI XML Interface Definitions Reference* describes the OM Interface and the OM Statistics in detail.

PM Statistics Files Uploading Uploads Performance Management (PM) statistics to the remote FTP server.

PM Statistics Queries statistics data from the OSSI/XML interface or the TPD platform and writes the data to an XML file.

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: 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 Task

To configure an individual task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**. The **Scheduled Task Administration** page opens in the work area.
2. To display details about a task, click the task name. The current settings and status are displayed.

   For example:

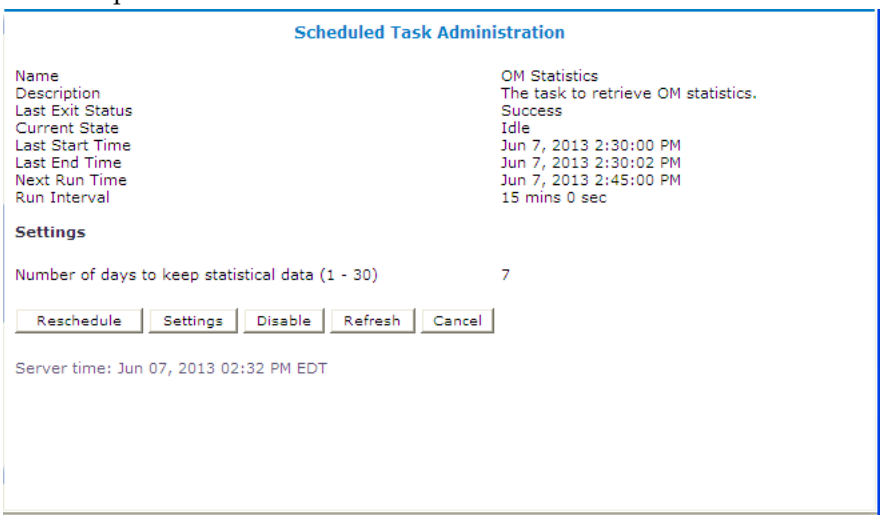


Figure 34: Schedule Task Administration - OM Statistics

3. The options for this task are as follows:
   - **Reschedule** — Click to reschedule the time that this task is performed on the Policy Management device.

     For example:

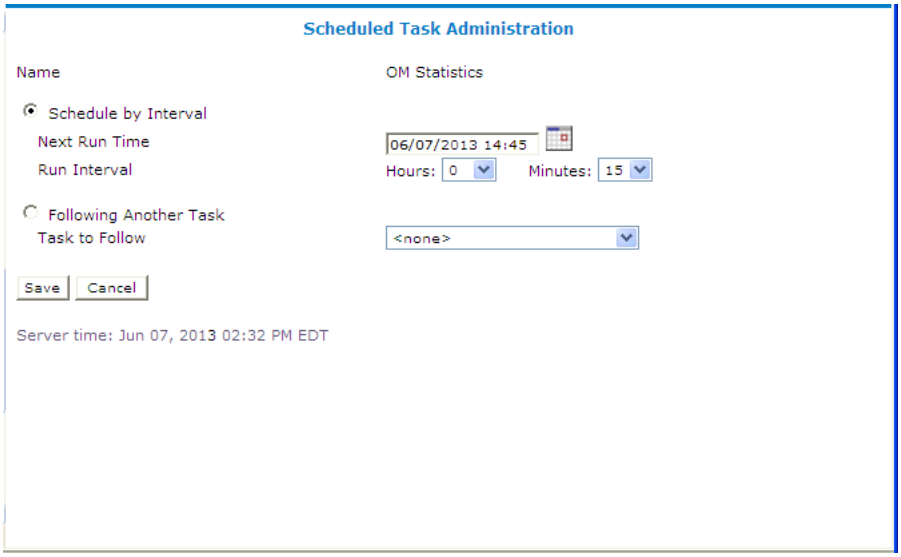


Figure 35: Scheduled Task Administration

- **Schedule by Interval** (**Next Run Time** or **Run Interval**) — Defines the run interval for the task to follow.

  Valid run intervals are from 0 to 24 hours in 5-minute increments.

- **Following Another Task** — Schedules the task run time as following the completion of another scheduled task selected from the list.

- **Settings** — Number of days to keep data; the default is seven days. Available for the OM Statistics and Replication Statistics tasks only.
- **Run Now** — Runs the process immediately.

  You are prompted with a confirmation message. Click **OK** to run the task.

- **Disable** or **Enable** — Disables or enables the next scheduled execution of this process.

  If you click **Disable**, a confirmation message displays. Click **OK**. The task is disabled and will not run at the next scheduled time, and the button changes to **Enable**.

- **Refresh** — Refreshes the page.
- **Cancel** — Returns to the previous page.

About Managing Users

The CMP system lets you configure the following user attributes:

Roles	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**
   - **PRA Lists**
   - **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**)

  If set to **Read-Only**, the following fields are displayed for the **Stats File Generator** (see *Managing Scheduled Tasks*) setting:

  - **Name**
  - **Description**
  - **Last Exit Status**
  - **Current State**
  - **Last Start Time**
  - **Last End Time**
  - **Follows Task**

  Task Settings

  - **Local Repository** — Root directory of the local repository.
  - **Maximum age to keep files (hours)** — Stats file retention period. Default is 72 hours.
  - **File Format** — Either CSV or XML (default).
  - **Stats Type** — Any stats type can be selected to generate stats. If you do not select a stats type, the task will not run normally.

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.

Note: There are a total of four synchronized tasks which are supported but cannot be edited.

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*
- *Modifying a Scope*
- *Deleting a Scope*

Creating a Scope

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.

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 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 36: 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 37: 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 37: 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 38: 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.

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.

Configuring a CMPP Client-based SMSR

You can configure a CMPP client-based Short Message Service Relay (SMSR) on the CMP system. The SMSR establishes a connection to the Short Message Service Center (SMSC), which is used when submitting short messages to the subscriber.

The SMSR is configured using the SMS Relay option in the System Administration section of the navigation pane. You can also use this option to set the log levels for the SMS and CMPP logs.

You can also configure a CMPP profile for an individual MPE device. See *Configuring MPE Protocol Options*.

To configure a CMPP Client-based SMSR:

1. From the **System Administration** section of the navigation pane, select **SMS Relay**.
   The current CMPP profile settings and SMS log settings are displayed.
2. Click **Modify**.
   A page that allows you to modify the CMPP configuration and SMS log settings opens.
3. In the **CMPP Configuration** section, define the following:
   a) **CMPP Enabled** — Enables the CMPP client to establish a connection with the SMSC. If this box is not checked, all CMPP messages to the SMSC are dropped. The default is to not enable the field.
   b) **SMSC Host** — The host name of the CMPP client that the SMSC server will connect to. The default value is to leave the field blank.
   c) **SMSC Port** — The port number of the CMPP client that the SMSC server will connect to. The default value is 7890.
   d) **Source Address** — The source address of the CMPP client. The default value is to leave the field blank.
   e) **Shared Secret** — The name of the shared secret, which is used to generate the authenticator source. The default value is to leave the field blank.
   f) **Registered Delivery** — Requests an SMSC delivery receipt or SME originated acknowledgments.
      Valid values are:
      - No Delivery Receipt (default)
      - Delivery Receipt
   g) **Service ID** — The service ID. Enter a string value with a 10-character length. The default value is to leave the field blank.
   h) **Message Format** — The format of the message encoding.
      The valid values are:
      - ASCII Encoding
      - Message Write Card Operation
      - Binary Message
      - UCS2 Encoding (default)
      - GBK Encoding

      To support Chinese characters in the message content, the format should be UCS2 or GBK.
4. In the **Modify SMS Log Settings** section, define the following:

a) **SMS Log Level** — The level at which an SMS log is generated.
b) **SMS Rotation Cycle** — The interval at which SMS logs are generated. The default value is HOUR, which generates logs hourly.

5. In the **Modify CMPP Log Settings** section, define the level at which a CMPP log is generated.
6. Click **Save**.

The CMPP Client-based SMSR is configured.

Appendix A

CMP Modes

Topics:

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

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

The Mode Settings Page

When you use a web browser to connect to a CMP system after the software is first installed, the **Mode Settings** page opens (*Figure 39: Mode Settings Page*). Select modes, sub-modes, and management options, and then click **OK**. The browser page closes and you are automatically logged out. When you next log in, the CMP system reopens in the selected mode.

Table 37: CMP Modes and Sub-Modes briefly describes each mode and sub-mode.

The management options are as follows:

- **Manage Policy Servers** — Manage MPE devices
- **Manage MA Servers** — Manage Management Agent servers
- **Manage Policies** — Enable the policy wizard
- **Manage MRAs** — Manage Policy Front End servers
- **Manage SPR Subscriber Data** — Manage Subscriber Profile Repository servers
- **Manage Mediation Servers** — Manage mediation servers
- **Manage Geo-Redundant MPE/MRA/BoD** — Manage georedundant MPE, MRA, or BoD clusters
- **Manager is HA (clustered)** — Enable High Availability features
- **Manage Analytic Data** — Enable output of policy event records
- **Manage Direct Link** — If enabled, all replication and HA traffic goes through the backplane interface; if disabled, all replication and HA traffic goes through the OAM interface

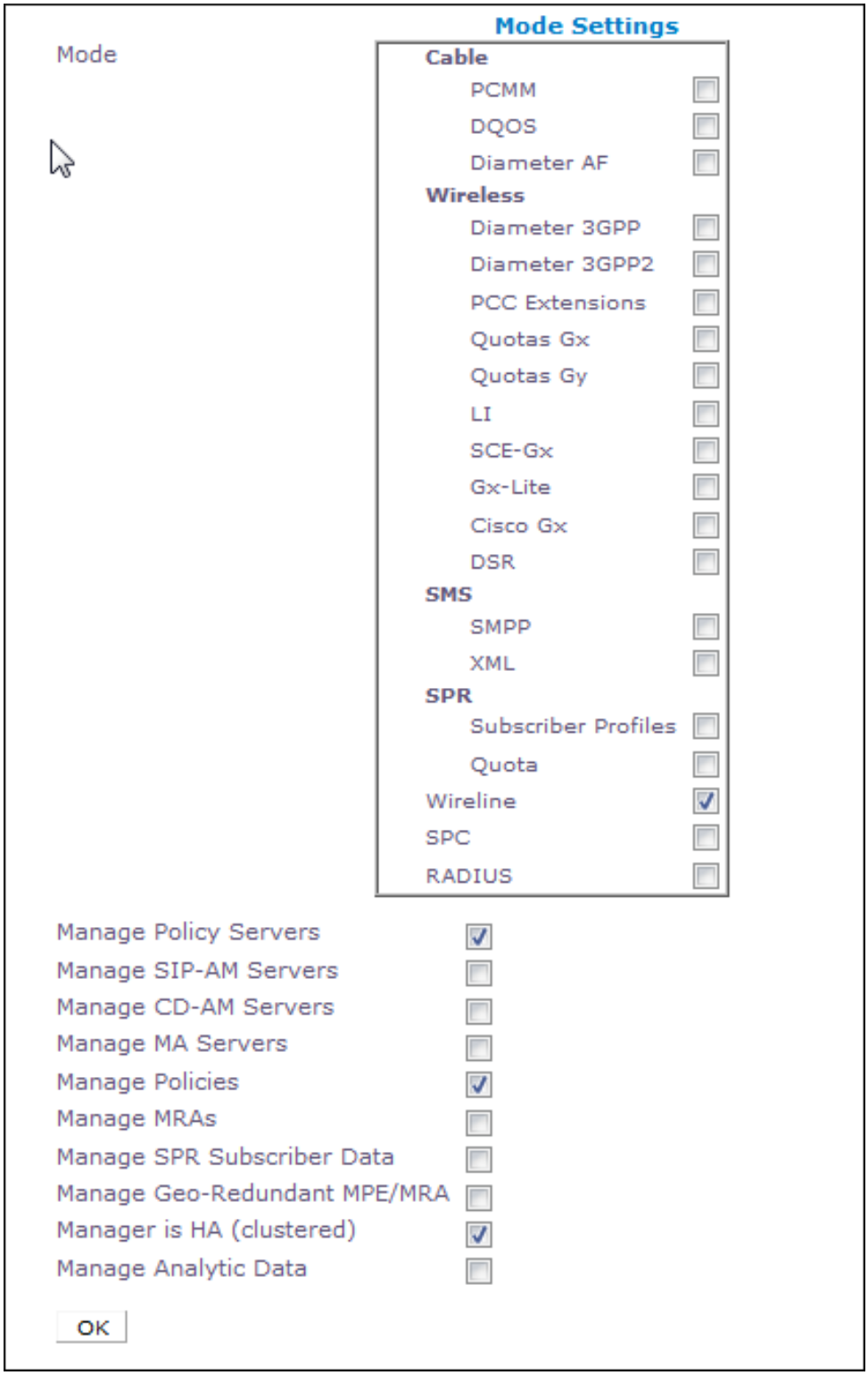


Figure 39: Mode Settings Page

Table 37: CMP Modes and Sub-Modes

Mode	Sub-Mode	Description
Cable Mode	Enables support of a cable carrier environment. Functions are described in the *Configuration Management Platform Cable User's Guide*.	
	PCMM	Supports PacketCable MultiMedia functions.
	DQOS	Supports Dynamic Quality of Service functions. (This mode enables a configuration that is no longer supported.)
	Diameter AF	Supports Diameter AF.
Wireless Mode	Enables support of a wireless carrier environment. Functions are described in the *Configuration Management Platform Wireless User's Guide*.	
	Diameter 3GPP	Supports Diameter 3GPP protocol.
	Diameter 3GPP2	Supports Diameter 3GPP2 protocol.
	PCC Extensions	Supports Policy and Charging Control functions.
	Quotas Gx	Supports a subscriber quota environment using the Diameter Gx protocol. The Gx protocol supports deep packet inspection (DPI) devices.
	Quotas Gy	Supports a subscriber quota environment using the Diameter Gy protocol
	LI	Supports Lawful Intercept functions. Described in the *Configuring Lawful Intercept Application Note*.
	SCE-Gx	Supports the Cisco Service Control Engine Gx protocol. If this mode is selected, Diameter 3GPP and RADIUS must also be selected, and other Gx sub-modes must not be selected.
	Gx-Lite	Supports the Gx-Lite protocol, a simplified version of 3GPP Gx for use by non-GGSN PCEF

Mode	Sub-Mode	Description
		vendors that do not have access to network-level information.
	Cisco Gx	Supports the Cisco Gx protocol.
	DSR	Supports Policy Management network segmentation using an Oracle Communications Diameter Signaling Router system.
	CMCC	Supports integration with the China Mobile Communications Corporation (CMCC) system.
SMS Mode	Enables support of SMS servers. Functions are described in the *Configuration Management Platform Wireless User's Guide*.	
	SMPP	Supports SMS using SMPP protocol.
	XML	Supports SMS using XML.
	CMPP	Supports integration with the China Mobile Peer to Peer (CMPP) system.
SPR Mode	Enables support of a Subscriber Profile Repository. Select only one sub-mode. Functions of the Oracle Communications Enhanced Subscriber Profile Repository are described in the ESPR documentation.	
	Subscriber Profiles	Supports subscriber profile functions.
	Quota	Supports subscriber quotas.
Wireline Mode	Enables support of a wireline carrier environment. Functions are described in the *Configuration Management Platform Wireline User's Guide*.	
SPC Mode	Enables the COPS Application Manager product, which accepts service provisioning requests from a Session Border Controller over the Common Open Policy Service (COPS) protocol. Functions are described in the *Service Provisioning over COPS Application Manager User's Guide*.	
RADIUS Mode	Enables support of RADIUS AAA.	
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*.	

Mode	Sub-Mode	Description
	PCMM	Supports a network creating PacketCable Multimedia (PCMM) sessions.
	Diameter	Supports a network creating Diameter sessions.
	RDR	Supports a network containing Service Control Engine (SCE) devices transmitting Raw Data Records (RDRs).
OMC Mode	Enables the CMP system to push Performance Management (PM) Statistics to the remote FTP server.	
Policy Method	Enables the policy method function.	

Glossary

#

3GPP	3rd Generation Partnership Project The standards body for wireless communications.
3GPP2	3rd Generation Partnership Project 2

A

AAA	Authentication, Authorization, and Accounting (Rx Diameter command)
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.
AF	Application Function (such as P-CSCF)
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

C

CID	Connection ID
CMTS	Cable Modem Termination System An edge device connecting to subscribers' cable modems in a broadband network. A CMTS device can function as a PCEF device; see PCEF. Equipment used by cable companies to provide high speed data services to cable subscribers.
COPS	Common Open Policy Service 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).
CPU	Central Processing Unit

D

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.
Distinguished Name	A unique name for an entry in a directory service.

D

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 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.
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.

F

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 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

HTTP	Hypertext Transfer Protocol

I

IMSI	International Mobile Subscriber Identity A unique internal network ID identifying a mobile subscriber.

I

IP-CAN

Internet Protocol Connectivity Access Network

Collection of network entities and interfaces that provide the underlying IP transport connectivity between the user 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.

L

LDAP

Lightweight Directory Access Protocol

A protocol for providing and receiving directory information in a TCP/IP network.

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.

O

OCS	Online Charging System A system allowing a Communications Service Provider to charge customers in real time based on service usage.
OFCS	Offline Charging Server
OM	Operational Measurement
OSSI	Operation Support System Interface An interface to a “back-end” (office) system. The Configuration Management Platform includes an OSSI XML interface.

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.
PCC	Policy and Charging Control Policy rules that define the conditions and actions used by a carrier network to control how subscribers and applications are treated and how network resources are allocated and used.
PCEF	Policy and charging enforcement function

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.
PCRF	Policy and Charging Rules Function Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF. In the Policy Management system, PCRF is located in the MPE device. Software node designated in real-time to determine policy rules in a multimedia network.
PDN	Packet Data Network A digital network technology that divides a message into packets for transmission.
PER	Policy Event Record A Policy Management-related message in the Analytics Data Stream.
PGW	PDN Gateway
policy and charging rules function	See PCRF.

P

PUR

Profile Update Request on Sh Interface

The Command sent by a Diameter client to a Diameter server to update user data in the server.

Q

QoS

Quality of Service

Control mechanisms that guarantee a certain level of performance to a data flow.

R

RADIUS

Remote Authentication Dial-In User Service

A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

realm

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.

S

SANE

Secure Access to Network Elements

Verizon Wireless's central authentication and auhorization system for network elements. It provides single-sign-on capability to network elements, for user of the

S

	SANE GUI client, and it allows network element vendors to use open-source, open-protocol methodologies to integrate clients int he Verizon Wireless security infrastructure.
SCTP	The transport layer for all standard IETF-SIGTRAN protocols. 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.
Secure Access to Network Elements	See SANE.
server	In Policy Management, a computer running Policy Management software, or a computer providing data to a Policy Management system.
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.

S

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.
SMSR	SMS Relay Application An interface between the MPE and SMSC or other specific SMS web service(s).
SMTP	Simple Mail Transfer Protocol
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

T

TPD	Tekelec Platform Development

T

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

VLAN

Virtual Local Area Network

A logically independent network. A VLAN consists of a network of computers that function as though they were connected to the same wire when in fact they may be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware. Several VLANs can co-exist on a single physical switch.

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.