Oracle® Communications Policy Management

CMP Wireless User's Guide

Release 12.0

E60241 Revision 01

March 2015

ORACLE®

Oracle® Communications CMP Wireless User's Guide, Release 12.0

Table of Contents

List of Figures

List of Tables

Chapter 1

About this Guide

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:

- *About this Guide* provides general information about the organization of this guide, related documentation, and how to get technical assistance.
- *The Oracle Communications Policy Management Solution* provides an overview of the Oracle Communications Policy Management Multimedia Policy Engine (MPE) device, which manages multiple network-based client sessions; the network in which the MPE device operates; policies; and the Oracle Communications Policy Management Configuration Management Platform (CMP) system, which controls MPE devices and associated applications.
- *Configuring the Policy Management Topology* describes how to set the topology configuration.
- *Managing Multimedia Policy Engine Devices* describes how to use the CMP system to configure and manage the MPE devices in a network.
- *Configuring Protocol Routing* describes how to configure protocol routing.
- *Configuring Advanced Device Settings* describes how to specify advanced settings for MPE or MRA devices.
- *Managing Protocol Timer Profiles* describes how to manage protocol timer profiles.
- *Managing Charging Servers* describes how to manage charging servers.
- *Mapping Serving Gateways to MCCs/MNCs* describes how to map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs).
- *Managing Subscriber Profile Repositories* describes how to manage a Subscriber Profile Repository (SPR).
- *Managing Subscribers* describes how to manage subscriber tiers, entitlements, and quota usage within the CMP system.
- *Managing Network Elements* describes how to manage network elements.
- *Managing Policy Front End Devices* describes the Oracle Communications Policy Management Policy Front End (also known as the MRA), a standalone entity that supports MPE devices and is manageable by the CMP system.
- *Managing S-CMP Devices* describes how to configure and organize S-CMP devices in a tiered CMP system.
- *System-Wide Reports* 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 Technology

Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Other Publications

The following documents are useful for reference:

- RADIUS RFCs:
  - RFC 2865: "RADIUS"
  - RFC 2866: "RADIUS Accounting"
  - RFC 3576: "Dynamic Authorization Extensions to RADIUS"
- 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 23.203: "Policy and charging control architecture (Release 8)"
  - 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows (Release 6)"
  - 3GPP TS 29.209: "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 11)"
  - 3GPP TS 29.213: "Policy and Charging Control signalling flows and QoS parameter mapping (Release 11.4)"
  - 3GPP TS 29.214: "Policy and Charging Control over Rx reference point (Release 8)"
  - 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 32.240: "Charging architecture and principles (Release 8)"
  - 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications (Release 8)"
- 3rd Generation Partnership Project 2 (3GPP2) technical specifications:
  - 3GPP2 X.S0013-012-0: "Service Based Bearer Control — Stage 2"
  - 3GPP2 X.S0013-013-0: "Service Based Bearer Control — Tx Interface Stage 3"
  - 3GPP2 X.S0013-014-0: "Service Based Bearer Control — Ty Interface Stage 3"

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.

2. Select the **Applications** tile.
   The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Chapter

2

The Oracle Communications Policy Management Solution

Topics:

The Oracle Communications Policy Management Solution provides an overview of the major elements of the Policy Management solution; the Oracle Communications Policy Management Multimedia Policy Engine (MPE) device, which manages multiple network-based client sessions; and the Oracle Communications Policy Management Configuration Management Platform (CMP) system, which controls MPE devices and associated applications.

Elements of the Oracle Communications Policy Management Solution

Figure 2: Interfaces to the MPE Device shows how the Policy Management solution fits into a wireless network. The major elements of a Policy Management network are:

- Oracle Communications Policy Management Multimedia Policy Engine 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 the *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).

The Application Function (AF) is a network element offering applications that require dynamic policy or charging control over IP Connectivity Access Network (IP-CAN) user plane behavior. An example of an AF is a Proxy Call Session Control Function (P-CSCF) device. MPE devices communicate with AFs to obtain dynamic session information and send IP-CAN specific information and notifications about bearer-level events.

The Policy and Charging Enforcement Function (PCEF) receives requests to start new sessions for subscribers. Examples of PCEFs include a Gateway GPRS Support Node (GGSN), and a Packet Data Network Gateway (PGW). MPE devices communicate with PCEFs to receive requests for policy decisions and send those policy decisions to the PCEF for implementation.

The Traffic Detection Function (TDF) can permit, gate, shape, or redirect service traffic. An example of a TDF is a deep packet inspection (DPI) device.

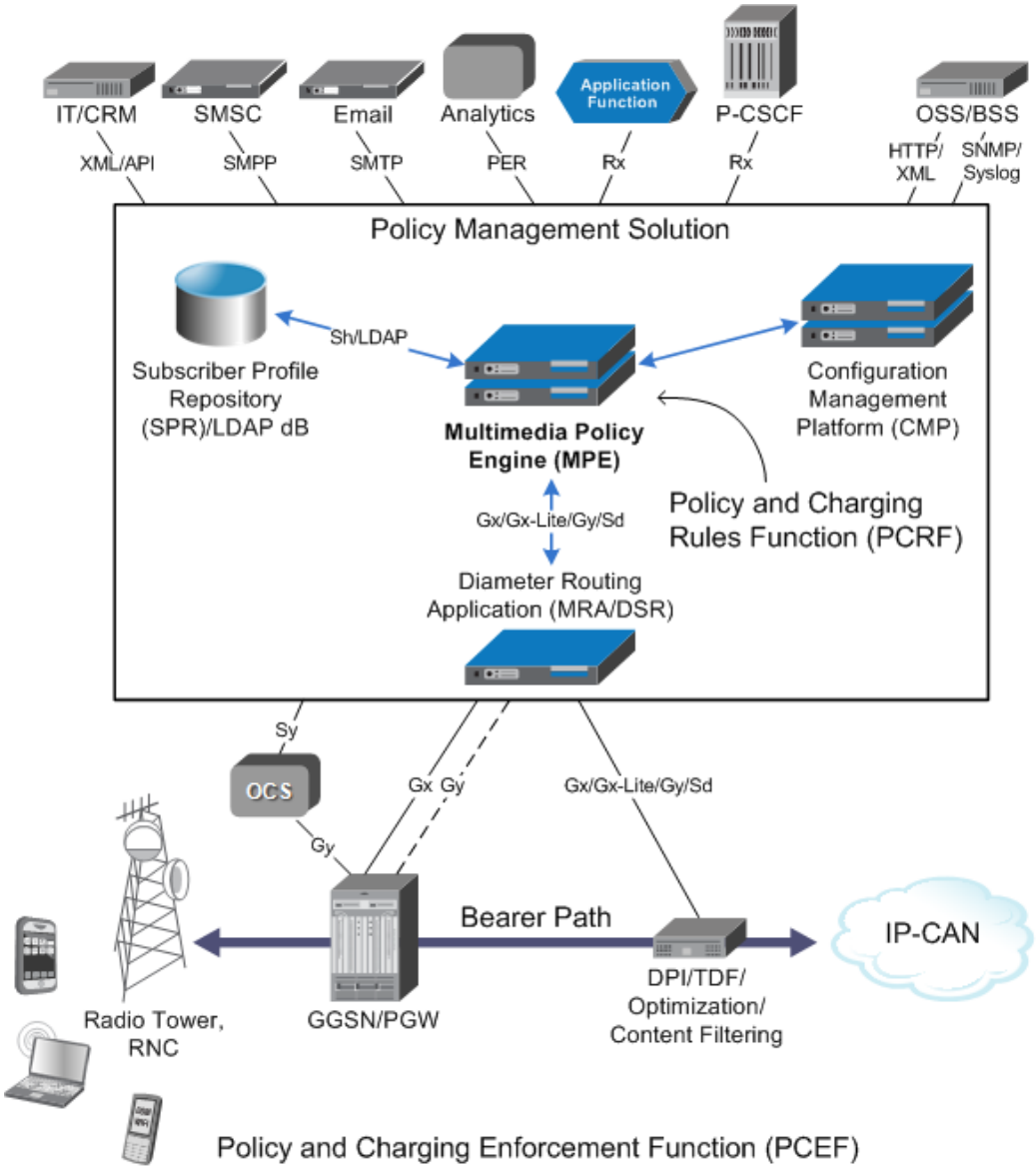


Figure 1: The Policy Management Solution and MPE Devices

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 accessible remotely.

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 PM&C documentation for more information.

The Oracle Communications Policy Management Multimedia Policy Engine

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 and how applications and subscribers are treated. See the *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; to send those policy decisions, as PCC rules, to PCEFs for implementation; to remove PCC rules from PCEFs; and to 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 and HSGWs. MPE devices act as servers for BBERFs, using the Diameter Gxa 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 Gxa 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 the *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.

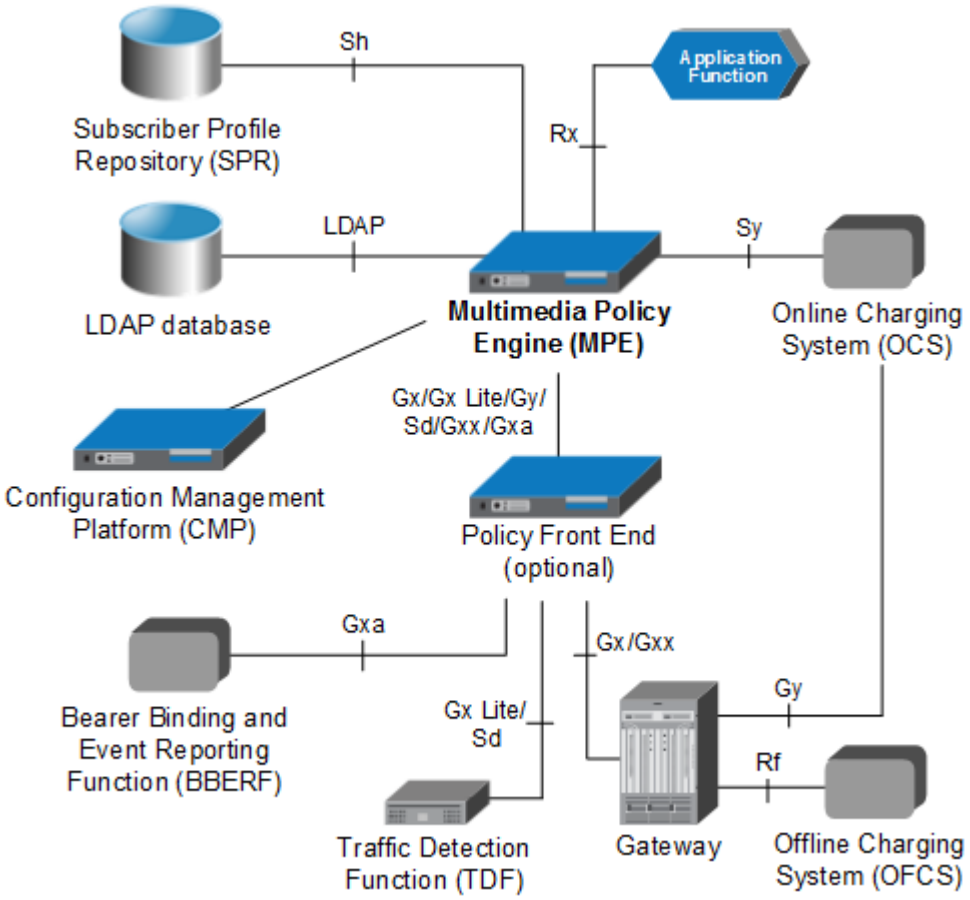


Figure 2: Interfaces to the MPE Device

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.

Policy Front End Overview

The Policy Front End product (referred to in this document as the Multi-Protocol Routing Agent [MRA]) is a product deployed in a Policy Management network that maintains bindings that link subscribers to Multimedia Policy Engine (MPE) devices. An MPE is a Policy Charging and Rules Function (PCRF) device. An MRA ensures that all of a subscriber's Diameter sessions established over the Gx, Gxx, Gx Lite, 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 devce implements the proxy (PA1 variant) DRA functionality defined in the 3GP TS 29.203 [1] and 3GPP TS 29.213 [2] specifications, whereby all Diameter Policy and Charging Control (PCC) application messages are proxied through the 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, using the proprietary Distributed Routing and Management Application (DRMA) protocol, for a binding. If another MRA device has the binding, the MRA device routes the request to it. If no other MRA device has a binding, the MRA device that received the request creates one.

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

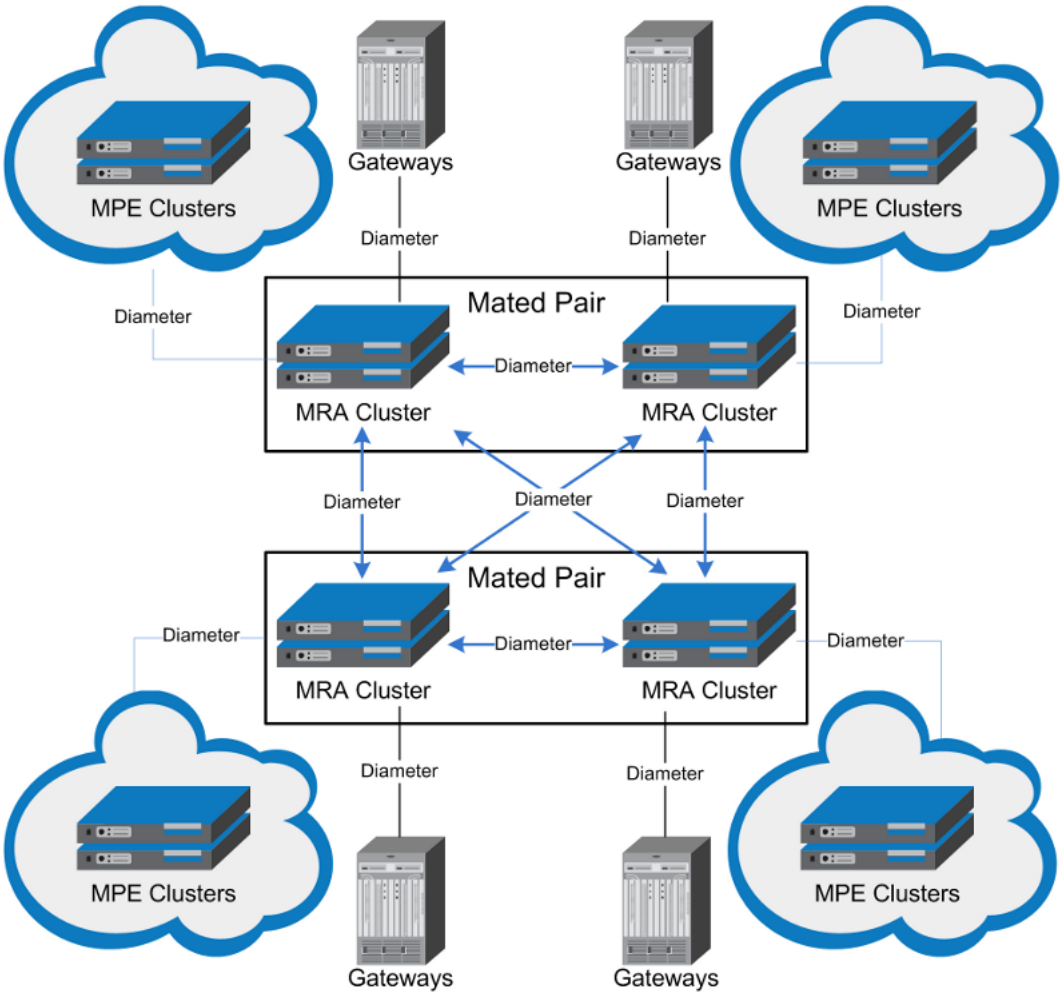


Figure 3: Typical Front End (MRA) Network

The Oracle Communications User Data Repository

The Oracle Communications User Data Repository (UDR) platform provides a highly scalable, consolidated database back-end for subscriber and profile data that can be leveraged across the product portfolio. UDR can utilize multiple application front-ends with the database.

Currently, 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 ESPR for creating, retrieving, modifying, and deleting subscriber and pool data.

The Oracle Communications Policy Management Configuration Management Platform

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

- Configuration and management of MPE devices
- Configuration and management of MRA devices
- Configuration of connections to Subscriber Profile Repository (SPR) devices
- Definition of network elements
- Creation, modification, deletion, and deployment of policy rules
- Creation, modification, and deletion of objects that can be included in policy rules
- Monitoring of individual product subsystem status
- Administration and management of CMP users
- Upgrading the software on Policy Management devices

Specifications for Using the GUI

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

- **Web Browsers**
  - Mozilla Firefox® release 10.0 or higher
  - Microsoft Internet Explorer® 10.0 or higher
  - Google Chrome version 20.0 or higher
- **Monitor** — Use a resolution of 1024 x 768 or higher

  Note: When using the CMP system for the first time, it is recommended that you change the default username and password to a self-assigned value. See *Changing a Password* for information on this procedure.

Logging In

The CMP system supports either HTTP or HTTPS access. Access is controlled by a standard username/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: As delivered, the profile **`admin`** provides full access privileges, and is the assumed profile used in all procedures described in this document. The default username of this profile is **`admin`** and the default password is **`policies`**. You cannot delete this user profile, but you should immediately change the password. See *Changing a Password*.

To log in:

1. Open a web browser and enter the IP address of the CMP system.
   The login page opens (*Figure 4: CMP Login Page* shows an example).
2. Enter the following information in the appropriate fields:
   a) **Username**
   b) **Password**
3. Click **Login**.
   The main page opens.

You are logged in.

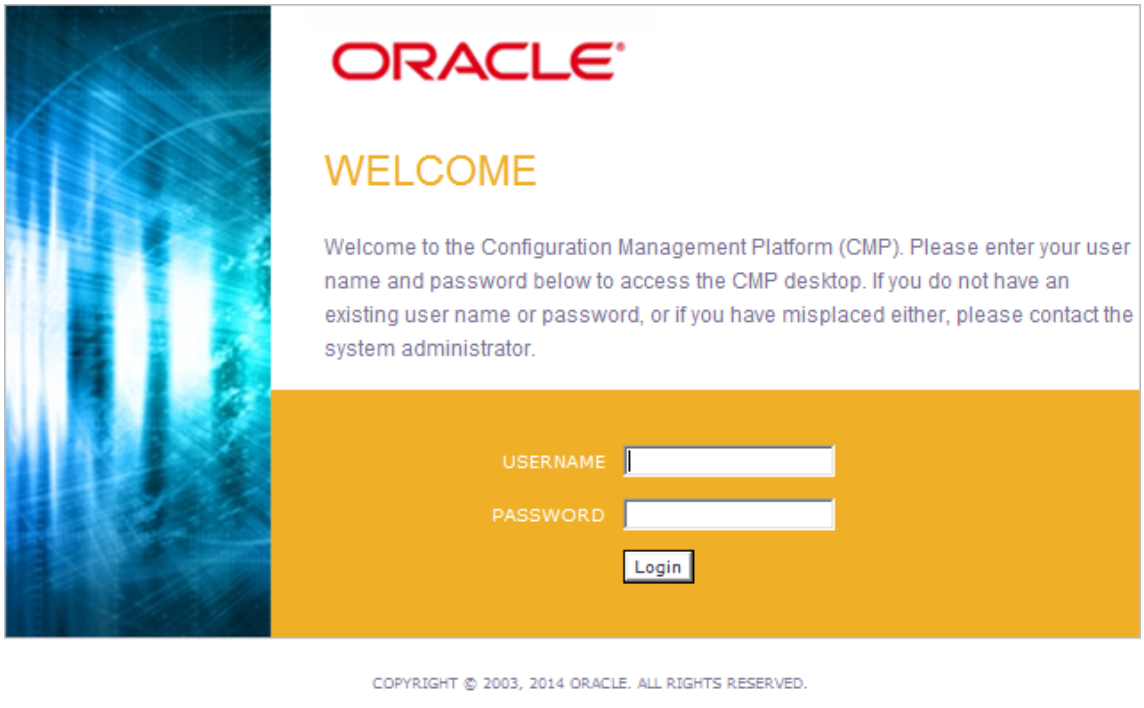


Figure 4: CMP Login Page

Logging In to a Standby or Secondary-Site CMP System

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

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

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

GUI Overview

You interact with the CMP system through an intuitive and highly portable graphical user interface (GUI) supporting industry-standard web technologies (SSL, HTTP, HTTPS, IPv4, IPv6, and XML). *Figure 5: Structure of the CMP GUI* shows the structure of the CMP GUI.

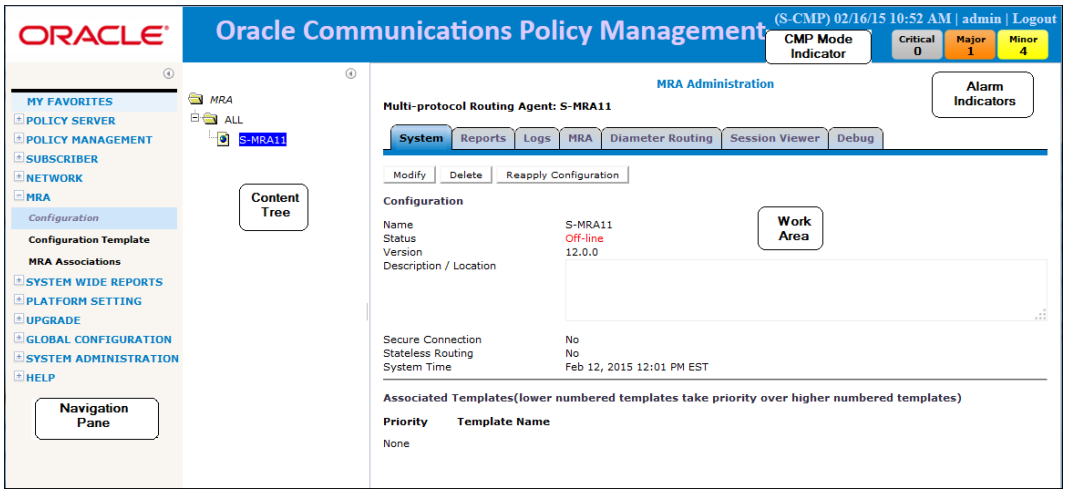


Figure 5: Structure of the CMP GUI

- **Navigation Pane** — Provides access to the various available options configured within the CMP system.

  You can bookmark options in the Navigation pane by right-clicking the option and selecting **Add to Favorite**. Bookmarked options can be accessed from 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.

  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**.

GUI Icons

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

Add icon	Use this icon to add an item to a list.
Calendar icon	Use this icon to select a date and, in some cases, time.
Clone icon	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.
Delete icon	When visible in the work area, selecting the Delete icon deletes an item, removing it from the MPE device. **Note:** Deleting an item from the **ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.
Delete icon	When visible in the work area, selecting the Delete icon deletes an item, removing it from the MPE device. **Note:** Deleting an item from the **ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.
Details icon	The binoculars icon displays when it is possible to view more details for an item.
Edit icon	Use this icon to modify a selection in a list.
External Connection icon	When visible in the work area, indicates which server currently has the external connection (the active server).
Gear icon	The gear icon displays when a policy references another policy or policy group.

Hide icon	When visible in the work area, selecting the hide icon removes the item from the current view but does not delete the item. **Note:** The item is only hidden during the current session. The item will be visible the next time a user logs into the CMP system.
Manual	Displays when a field is configured by the user. Hover over this icon to see the name of the device.
Major error	Displays in reports to indicate a major error during the blade replication process.
Minor error	Displays in reports to indicate a minor error during the blade replication process.
Move icons	The up and down arrow icons are displayed when it is possible to change the sequential order of items in a list.
OK status	Displays in reports to indicate a that the blade replication process completed without error.
Remove icon	When visible in the work area, selecting the Remove icon removes an item from the group it is associated with. The item is still listed in the ALL group and any other group that it is currently associated with. For example, if you remove MPE device PS_1 from policy server group PS_Group2, PS_1 still displays in the ALL group.
Selection icon	The Selection icon is in the Policy Wizard. The icon is used to select conditions and actions to add to the policy rule.
Synch broken icon	When visible in the Upgrade Manager, indicates that the CMP system does not have current information on a server.
Template	Displays when a field is configured by template. Hover over this icon to see the name of the template. Click the icon to view the template.

Shortcut Selection Keys

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

- **Shift + click** — Selects two or more consecutive items. To select consecutive items, select the first item, then press Shift and click the last item to select both items and all items in between.
- **Control + click** — Selects two or more non-consecutive items. To select multiple non-consecutive items, hold down the Ctrl key as you click each item.

The Oracle Communications Policy Management Network Configuration Management Platform

The Oracle Communications Policy Management Network Configuration Management Platform provides centralized management for systems containing multiple CMP servers. This configuration is a tiered configuration that uses two types of CMP servers: Network Configuration Management

Platform (NW-CMP) and System Configuration Management Platform (S-CMP). The NW-CMP server manages the entire system by managing one or more S-CMP servers. The NW-CMP sends configuration updates to the S-CMP servers, and the S-CMP configures MPE and MRA devices.

The NW-CMP server configures Network tier objects. Examples of Network tier objects are policies, network elements, and configuration templates. After the Network tier objects are configured on the NW-CMP, the objects are distributed to S-CMP servers. On the S-CMP the Network tier objects can be associated with MRA or MPE servers. Network tier objects cannot be created, modified, or deleted on S-CMP servers.

The S-CMP servers configure System tier objects. System tier objects are MPE and MRA devices. These objects are used to apply configurations to individual servers. The MPE and MRA configurations can change individual server configuration parameters or associate Network tier objects with an MPE or MRA device. Figure *Figure 6: Policy Management Network Configuration Management Platform* shows the structure of a Network Configuration Management Platform system.

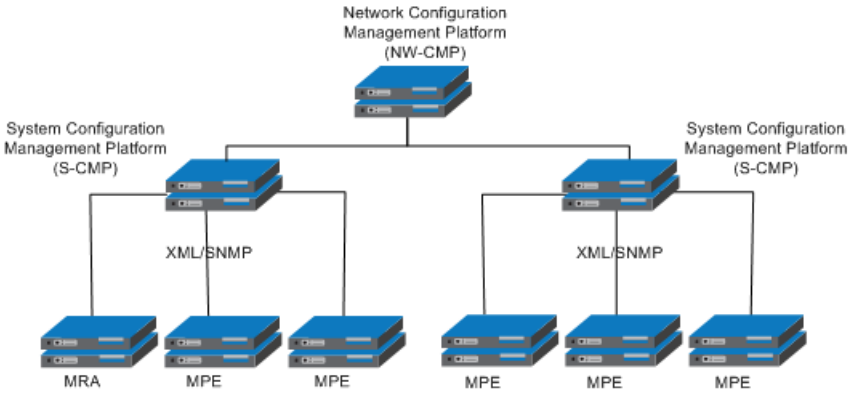


Figure 6: Policy Management Network Configuration Management Platform

Device Configuration in an Network CMP

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

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

It is recommended that a global configuration template is created for each server type. The global configuration template is then distributed from the NW-CMP server to all S-CMP servers. Then the

global template is associated with the appropriate server. This results in a single global configuration template object used network-wide on all servers of the same type. Since all the servers are associated with the same global objects, applying a configuration change from NW-CMP server becomes as simple as making a change either in a configuration template or in another global object (such as a policy) referenced by this configuration template. Any change to the configuration template is immediately propagated from the NW-CMP server through the S-CMP to all associated servers.

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

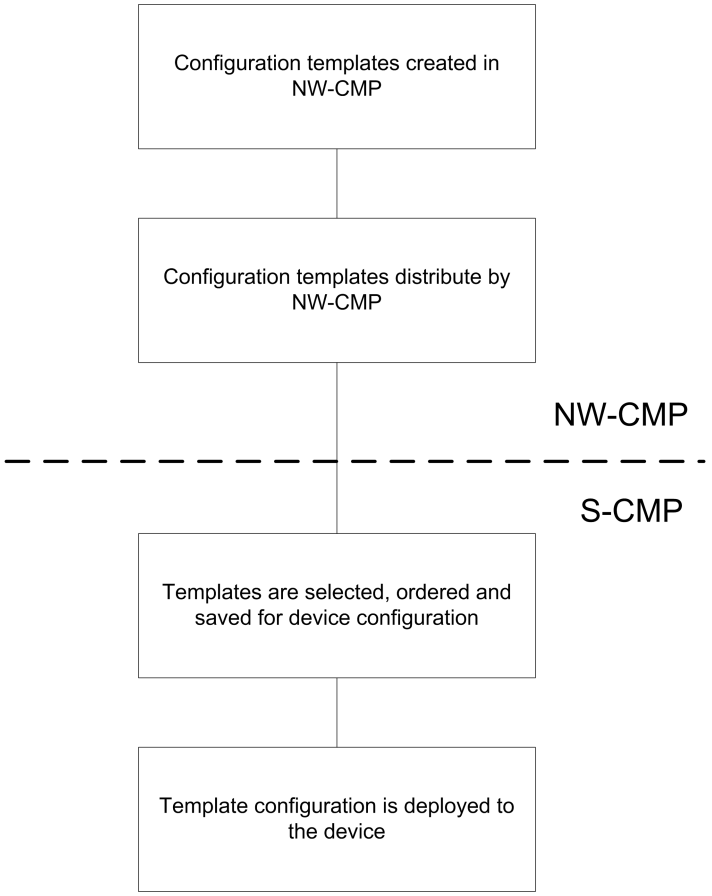


Figure 7: Device Configuration Flow Using Configuration Templates

Network CMP Tier Capabilities

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

Table 2: Top Level Objects by Management Tier lists the tiers (NW-CMP or S-CMP) where top level objects are configured.

Table 2: Top Level Objects by Management Tier

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

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

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

Overview of Main Tasks

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

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

1. Configure the topology, which defines the addresses 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 complete set of tasks is as follows:

- Create network element profiles, including protocol options, for each network element with which the MPE or MRA devices interact. This task is described in *Managing Network Elements*.
- Specify which MPE or MRA device will interact with which network element(s). 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 Multi-Protocol Routing Agent (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 *Managing Subscriber Profile Repositories* and *Managing Subscribers*.

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

- Manage subscriber profiles and sessions. These tasks are described in *Managing Subscriber Profile Repositories* and *Managing Subscribers*.
- View reports on the function of the Policy Management systems in your network. This task is described in *System-Wide Reports*.
- 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:

Configuring the Policy Management Topology describes how to configure the Policy Management devices into a network, and how to configure the CMP system to manage them.

About the Policy Management Topology

You need to configure a network topology for the Policy Management products (CMP, 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 8: Policy Management Topology illustrates a Policy Management topology consisting of a primary (Site 1) and secondary (Site 2) CMP cluster, an MRA cluster, and two MPE clusters.

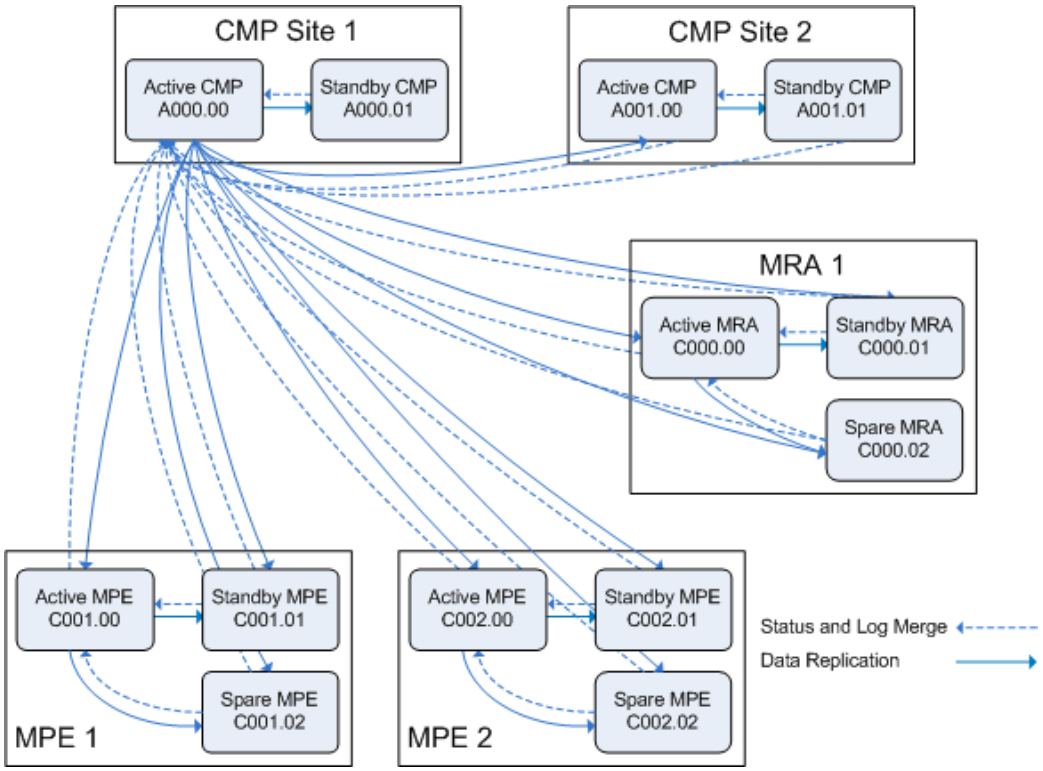


Figure 8: Policy Management Topology

High Availability

High Availability (HA) is provided for all Policy Management cluster configurations. HA is accomplished by using two servers per cluster, an active server and a standby server. Servers are continually monitored by the Communications Core Object Library (COMCOL) in-memory database. As shown in *Figure 9: High Availability*, the active server processes network traffic and is accessible and connected to external devices, clients, gateways, and so forth. Only one server in a cluster can be the active server.

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

1. The active and standby servers communicate using a TCP connection over the Operation, Administration, and Management (OAM) network to replicate current state data, monitor server heartbeats, and merge trace logs and alarms.
2. The servers share a virtual IP (VIP) cluster address to support automatic failover. The active server controls the VIP address.
3. The standby server does not receive any live traffic load, but holds an up-to-date copy of the active session state data at all times, replicated by High Availability. (This is sometimes called a warm standby.)
4. COMCOL database runtime processes on each server constantly monitor server status using heartbeat signals.
5. If the active server fails, indicated by skipping a succession of heartbeats, COMCOL instructs the standby server to become the active server and take over the VIP address and connections. Because it has been receiving session state data updates through replication, it can assume processing of ongoing sessions, so the failover is automatic and transparent to other components.

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

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; if an active server fails and then recovers, it becomes the standby server, rather than resuming its role as the active server.

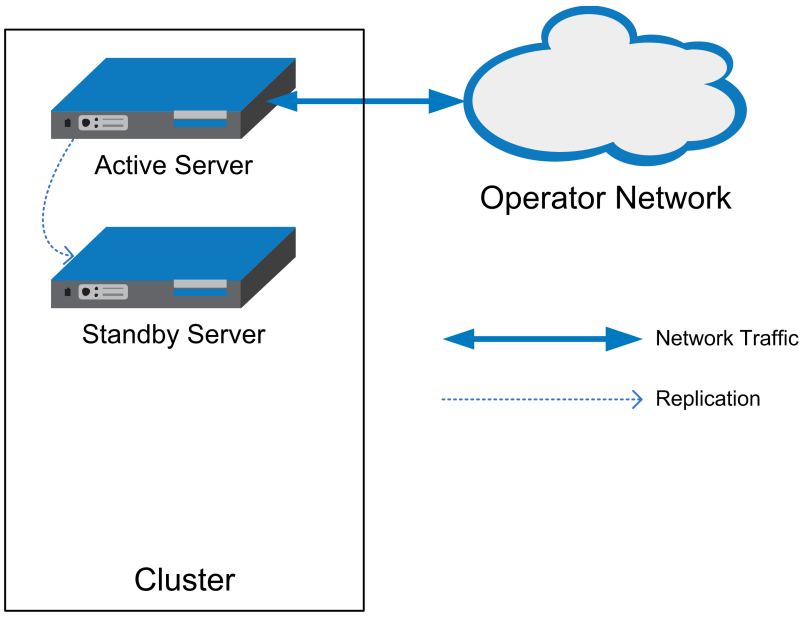


Figure 9: High Availability

Spare Servers

As shown in *Figure 10: Cluster with Active, Standby, and Spare Servers*, an MPE or MRA cluster can contain an additional server, called a spare server. The active server will replicate its database to the spare server as well as the standby 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.

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 in the cluster.
5. If the active server fails, it instructs the standby server to take over and become the active server.

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

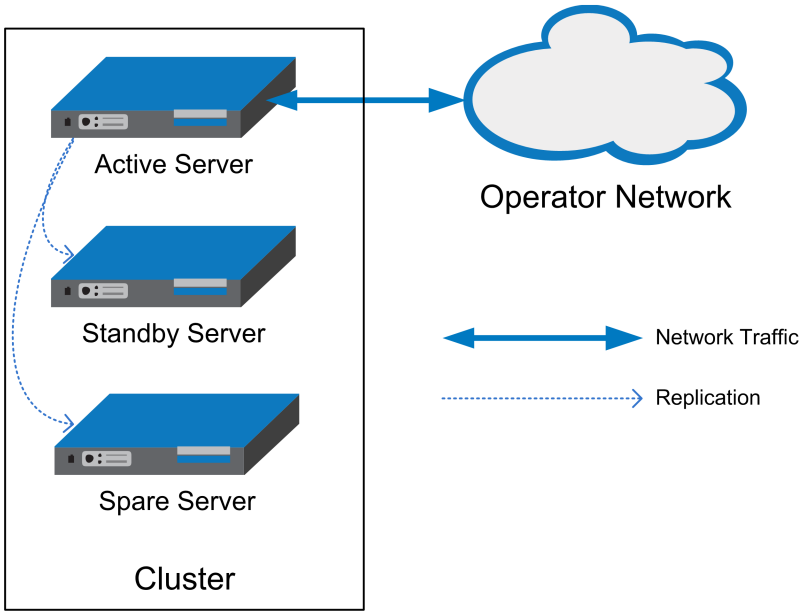


Figure 10: Cluster with Active, Standby, and Spare Servers

CMP Georedundancy

As shown in *Figure 11: 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 High Availability, to active server of the Site 2 cluster.

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 or states 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. 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").

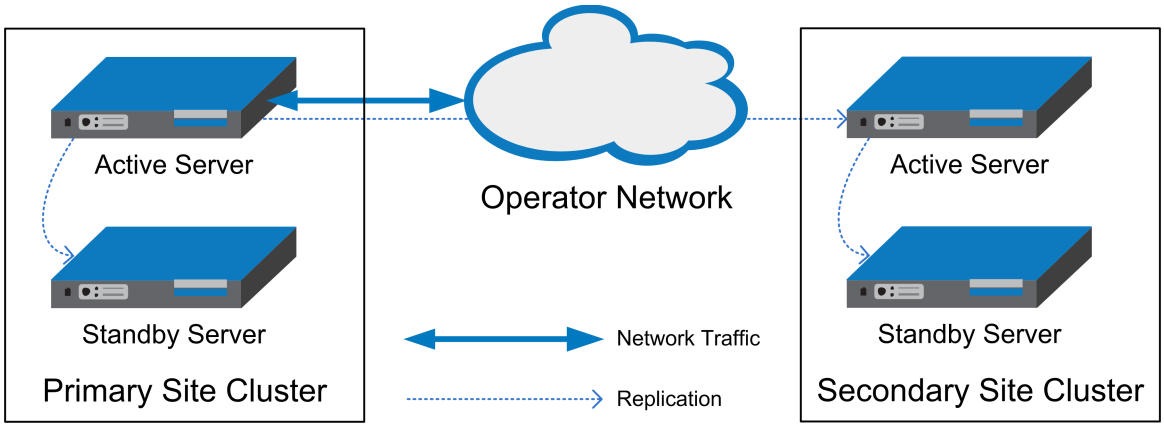


Figure 11: CMP Georedundancy

In a georedundant topology, HP Proliant BL460G6 servers (with a 1x4 mezzanine card) and NETRA servers can communicate over a dedicated backup (BKUP) network.

Note: CMP servers do not use the REP network or DSCP marking.

Georedundancy for non-CMP servers

The spare server does not need to be physically close to the active and standby 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 12: 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 continues to provide service. You can designate sites as primary and secondary.

Georedundancy supports both session-stateful (MPE) and binding-stateful (MRA) 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.

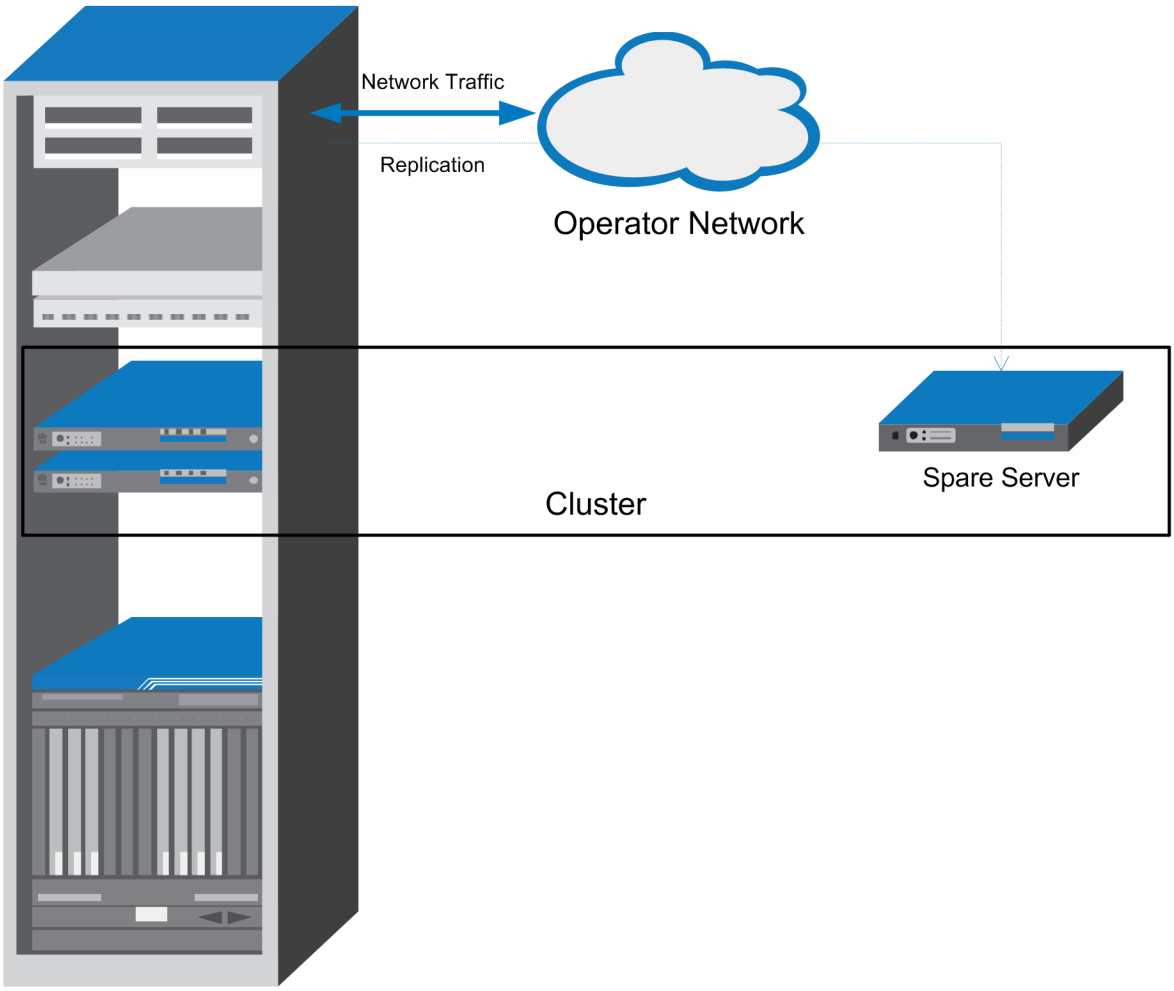


Figure 12: Non-CMP Georedundant Configuration

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, 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 Diameter Routing Agents, 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; once the recovered servers are synchronized with the active servers' state data, they are automatically returned to active roles. This behavior is "revertive;" 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), which 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 traffic between sites (that is, between the active and spare servers) using different VLANs. Replication traffic 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 products, 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 once again 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. Once 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 13: 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 A is also the secondary site of Cluster B, and vice versa.

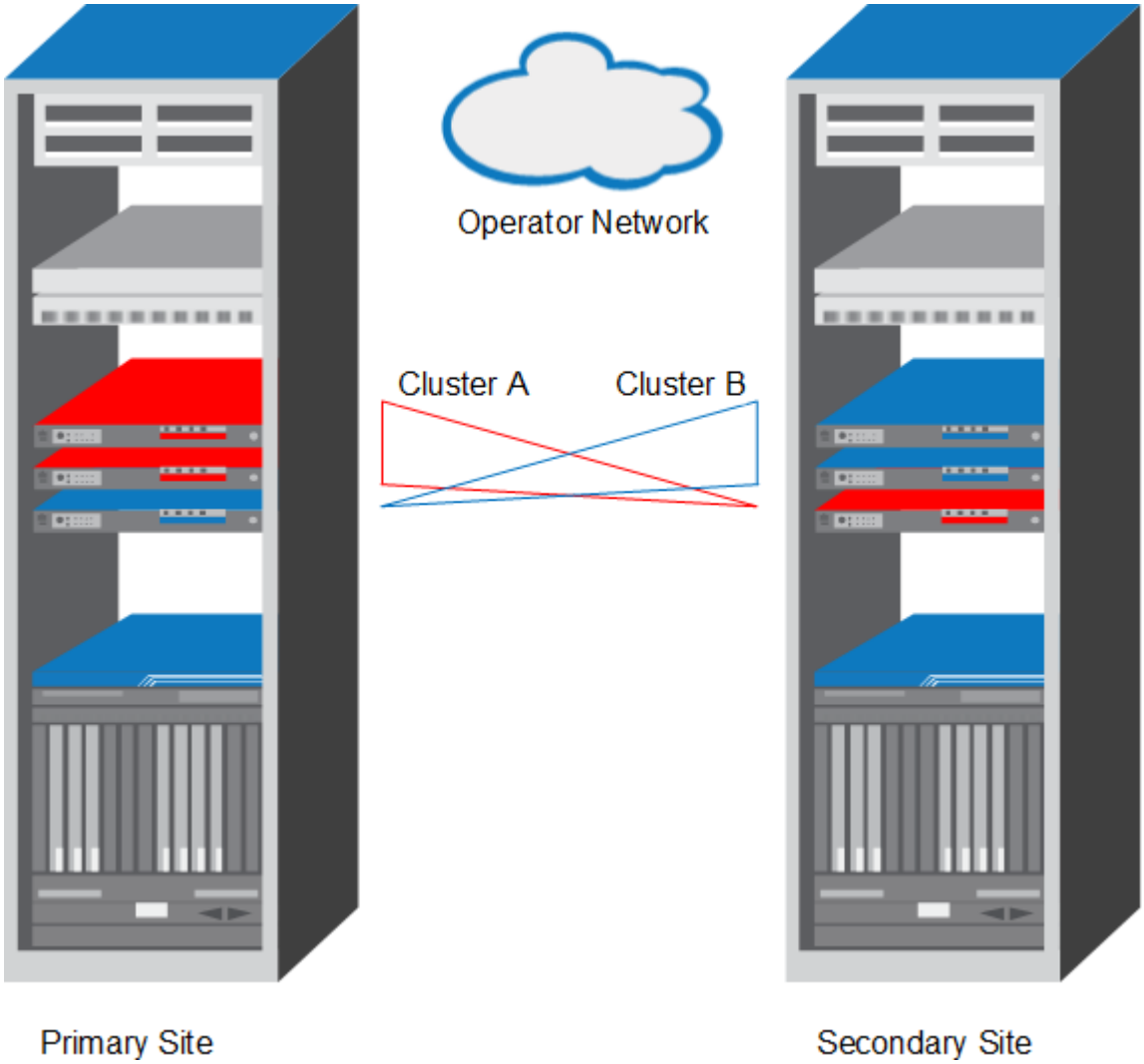


Figure 13: Example of Primary and Secondary Sites

Cluster 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. Once 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 on MPE or MRA cluster preferences under the heading “Site Preference.” A cluster preference is either “Normal” or “Reverse” (or “N/A” for CMP clusters, which 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 no two servers in the same cluster should ever have the same status. (Two servers in the same cluster with the same status is an error condition.)

The status values are as follows:

- **Active:** The active server in a cluster is the server that is the externally connected. The active server is the only server that is handling connections and servicing messages and requests. Only the active server writes to the database. 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 14: 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, do the following:

1. Define the DSR systems in the CMP database as network elements. For more information, see *DSR*.
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.

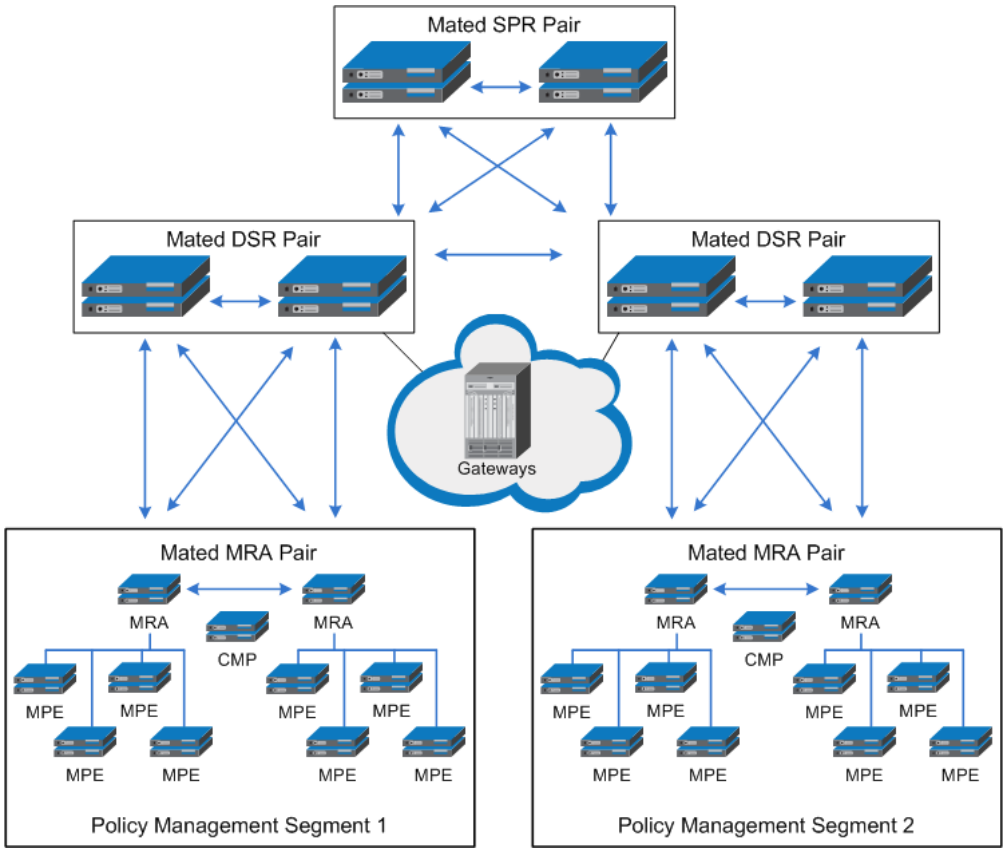


Figure 14: Segmented Policy Management Network

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 — You start to build a topology by logging in to the active CMP server at the primary site. Configure the CMP cluster settings. The settings are replicated (pushed) to the standby CMP server. Together, the two servers form a primary, or Site 1, CMP cluster. This is the primary CMP site for the whole topology network. The primary site cannot be deleted from the topology.
2. Configure the secondary CMP cluster (optional) — Use the primary CMP cluster to configure a secondary, or Site 2, CMP cluster. A secondary CMP cluster can provide georedundancy.
3. Configure MPE and MRA clusters — Enter MPE and MRA cluster settings on the active CMP server on the primary site. You can define the topology before defining the servers themselves. Once defined, the configuration information is replicated as follows:
   a. The 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.
   b. Active servers communicate with standby servers using LAN connections over the OAM network. Active servers communicate with spare servers using WAN connections over the OAM, SIG-A, SIG-B, or REP network.
   c. Active and standby servers share a virtual IP (VIP) cluster address to support automatic failover. (If present, the spare server has a unique VIP address.)
   d. The COMCOL database runtime process constantly monitors the status of the servers in each cluster. If an active server in a cluster fails, COMCOL instructs the standby server to take over and become 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.

Once you define the topology, use the **System** tab of each server to determine if there are any topology mismatches. See *Reapplying the Configuration to Policy Management Devices* for more information.

Note: 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 products, only backup of CMP systems is typical.

Setting Up a CMP Cluster

You must define at least one CMP cluster before continuing with the topology. The first site you define will be the primary (Site 1) cluster. You can optionally define a secondary CMP cluster.

Before defining the primary (Site 1) cluster, ensure the following:

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

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

To set up the primary CMP cluster:

1. Log in to the CMP server.
2. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The **Cluster Configuration** page opens. 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.
4. Click **Add CMP Site1 Cluster**.
   The **Cluster Settings** page opens. The cluster name and application type are fixed.
5. Enter the following information (*Figure 15: Cluster Settings Page for CMP Cluster* shows an example):
   a) **HW Type** — Select **C-Class** (default), **C-Class(Segregated Traffic)** (for a configuration in which Signaling and OAM networks are separated onto physically separate equipment), **NETRA**, or **RMS** (for a rack-mounted server).
   b) **Network VLAN IDs** (appears if you selected **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**) — Enter the Operation, Administration, and Management (OAM), SIG-A, and (optionally) SIG-B virtual LAN (VLAN) IDs, in the range 1–4095. The defaults are 3 for the OAM Virtual IP (VIP) and server IP, 5 for the SIG-A VIP, and 6 for the SIG-B VIP.
   c) **OAM VIP** (required) — Enter up to two OAM VIP addresses (one IPv4 and one IPv6) and their masks. The OAM VIP is the IP address the CMP uses to communicate with a Policy Management cluster. Enter the address in the standard dot format and the subnet mask in CIDR notation from 0–32 (IPv4), or standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128 (IPv6).

      Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

   d) **Signaling VIP 1** through **Signaling VIP 4** (optional) — Enter up to four IPv4 or IPv6 addresses and masks of the signaling virtual IP (VIP) addresses; for each, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. You must enter a Signaling VIP value if you specify either SIG-A or SIG-B. If you enter an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. If you enter an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

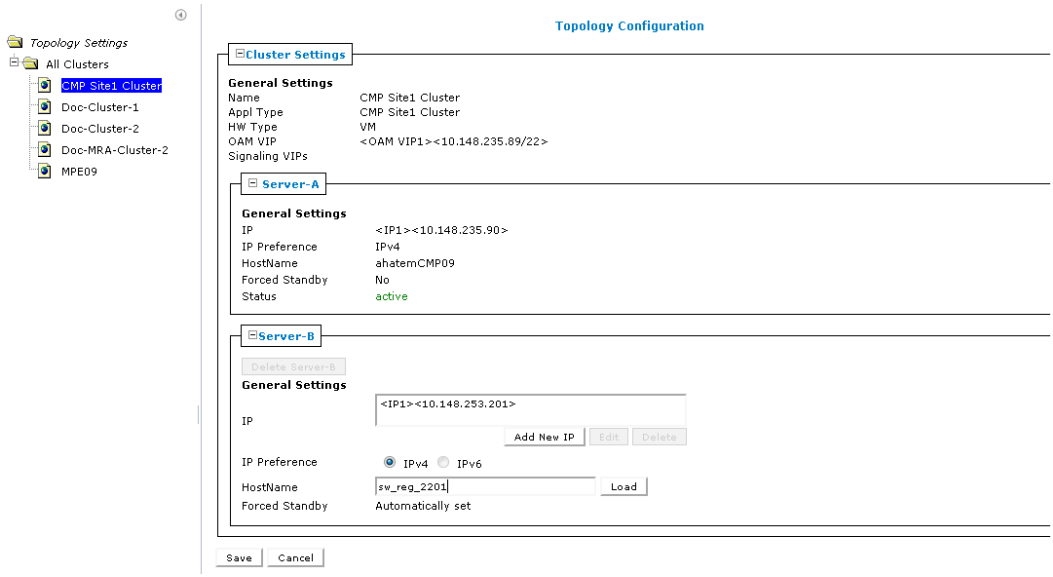


Figure 15: Cluster Settings Page for CMP Cluster

6. Select **Server-A** and enter the following information for the first server of the cluster (which will be the initial active server):
   a) **IP** (required) — The IP address of the server. Up to two IP addresses can be entered (one IPv4 and one IPv6). Use the standard dot-formatted IP address string for an IPv4 address, and the standard 8-part colon-separated hexadecimal string format for an IPv6 address.
   b) **IP Preference** — Specify 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 IPv6 OAM IP nor a static IP address is 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.
   c) **HostName** (required) — The name of the server. This must exactly match the host name provisioned for this server (that is, the output of the Linux command **`uname -n`**).

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

   d) **Forced Standby** — Select to force this server into standby mode. The flag is set automatically when a new server is added to a cluster, or if a server setting is modified and another server already exists in the cluster.
7. When you finish, click **Save** (or **Cancel** to discard your changes).
   You are prompted, "The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving." Click **OK** (or **Cancel** to stop the save operation). You are prompted, "Active server will restart and you will be logged out." When you click **OK**, the active server restarts.
8. Log back into the CMP server.
9. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens.
10. From the content tree, select the **CMP Site1 Cluster**.
    The **Topology Configuration** page opens.
11. Select **Modify Server-B**, and enter the appropriate information for the second server of the cluster.

12. When you finish, click **Save** (or **Cancel** to discard your changes).

The CMP cluster topology is defined.

Once you define the topology, use the **System** tab of each server to determine if there are any topology mismatches. See *Reapplying the Configuration to Policy Management Devices* for more information.

Once you define the primary (Site 1) CMP cluster, you can repeat this procedure to define a secondary (Site 2) CMP cluster.

Using HP Proliant BL460G6 hardware with a 1x4 mezzanine card, backup traffic between CMP sites can be sent between sites on the BKUP network.

Setting Up a non-CMP Cluster

A non-CMP server can be on of the following server types:

- MPE
- MRA

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 application is running on at least one server

If you are creating a cluster in a georedundant system, see *Setting Up a Georedundant Cluster*.

To define a cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens.
2. Click **Add MPE/MRA Cluster**.
   The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.
3. Define the general settings for the cluster in the **General Settings** section of the page.
   a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks (") and commas (,).
   b) **Appl Type** — Select the type of server.
      - **MPE** (default)
      - **MRA**
   c) **HW Type** — Select the type of hardware.
      - **C-Class** (default)
      - **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
      - **NETRA**
      - **RMS** (for a rack-mounted server)
      - **VM**

d) **OAM VIP** (optional) — Enter up to two OAM VIP addresses (one IPv4 and one IPv6) and their masks. The OAM VIP is the address the CMP cluster uses to communicate with the MPE or MRA cluster.

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

Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

e) **Signaling VIPs** (required) — The signaling VIP is the IP address a PCEF device uses to communicate with a cluster. A cluster supports redundant communication channels, named SIG-A, SIG-B and SIG-C, for carriers that use redundant signaling channels. Click **Add New VIP** to add a VIP to the system.

Note: SIG-C is only available for MRA clusters.

At least one signaling VIP is required.

You can enter up to four IPv4 or IPv6 addresses and masks of the signaling VIP addresses.

For each new VIP, enter the address and mask in the New Signaling VIP dialog. Select **SIG-A**, **SIG-B** or **SIG-C** to indicate whether the cluster will use an external signaling network.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

4. Define the general network configuration for the C-Class, C-Class segregated, or NETRA servers in the **Network Configuration** section of the page. This section is not available for RMS.
   a) Enter the **OAM**, **SIG-A**, **SIG-B** and **SIG-C** VLAN IDs, in the range 1–4095. The defaults are 3 for the OAM network and server IP, 5 for the SIG-A network, and 6 for the SIG-B network.

   Note: SIG-C is only available for MRA clusters.

5. Define the settings for **Server-A** in the Server-A section of the page.
   a) **IP** (required) — The IP address of the server. Up to two IP addresses can be entered (one IPv4 and one IPv6). Use the standard dot-formatted IP address string for an IPv4 address, and the standard 8-part colon-separated hexadecimal string format for an IPv6 address.
   b) **IP Preference** — Specify 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 IPv6 OAM IP nor a static IP address is 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.
   c) **HostName** — The name of the server. This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

   d) **Forced Standby** — Select to put the server into forced standby. (By default, Server A will be the initial active server of the cluster.)
6. (Optional) Click **Add Server-B** and enter the appropriate information for the standby server of the cluster. See step *Step 5* for information about the fields.
   Server-B is defined for the cluster.

7. When you finish, click **Save** (or **Cancel** to discard your changes).
   You are prompted, "The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving." Click **OK** (or **Cancel** to stop the save operation).
8. If you are setting up multiple clusters, repeat the steps.

The cluster is defined.

Figure 16: 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.

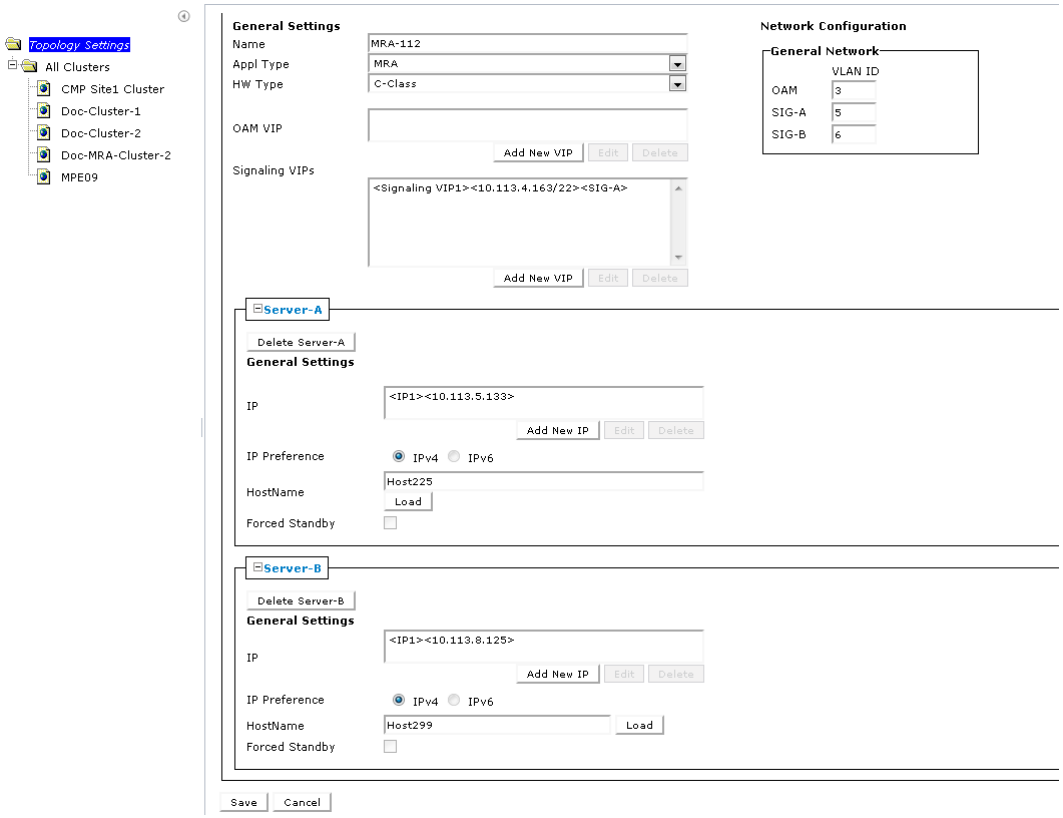


Figure 16: Sample MRA Cluster Topology Configuration

Setting Up a Site

Georedundant sites can contain one or more MPE or MRA clusters. Before setting up sites, you should plan your Policy Management topology to determine site naming conventions.

To set up a site:

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 Sites** group.
   The **Site Configuration** page opens.
3. Click **Create Site**.
   The **New Site** page opens.

4. Enter values for the configuration attributes:
   a) **Name** (required) — The site name. Enter up to 35 alphanumeric characters, underscores (_), or hyphens (-).
   b) **Max Primary Site Failure Threshold** — If the number of cluster pair failures reaches this threshold, a trace log entry and a major alarm are generated.

      A pair failure is recorded when both servers at a primary site are either out of service or in forced standby. You can optionally enter a number up to the total number of servers provisioned at this site. The default is no threshold.
   c) **HW Type** — Select the hardware type.

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

5. If the hardware type is C-Class, C-Class(Segregated Traffic), or NETRA, configure the general network information.

   Virtual LAN (VLAN) IDs are in the range of 1–4095.
   a) Enter the VLAN ID for Operation, Administration, and Management (OAM).
   b) Enter the VLAN ID for SIG-A
   c) (Optional) Enter the VLAN ID for SIG-B
6. If the hardware type is C-Class or C-Class(Segregated Traffic), enter the VLAN ID for the user define network.

   Virtual LAN (VLAN) IDs are in the range of 1–4095.
7. When you finish, click **Save** (or **Cancel** to abandon your request).
   The site configuration is saved in the CMP database.

The site is defined.

To define multiple sites, repeat the procedure starting at step *Step 3*.

Setting Up a Georedundant Cluster

This procedure contains the steps for setting up a non-CMP. The following servers are considered non-CMP:

- MPE
- MRA

Before defining a 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 application is running on at least one server

If your system is not set up for georedundancy, see *Setting Up a non-CMP Cluster*.

To define a cluster in a georedundant system:

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 Clusters** folder.
   The defined clusters are listed.
3. Click **Add MPE/MRA Cluster**.
   The **Topology Configuration** page opens. Each section of the **Topology Configuration** page can be collapsed or expanded.
4. Define the general settings for the cluster in the **Cluster Settings** section of the page:
   a) **Name** (required) — Name of the cluster. Enter up to 250 characters, excluding quotation marks (") and commas (,).
   b) **Appl Type** — Select the application type:
      - **MPE** (default)
      - **MRA**
   c) **Site Preference** — Select **Normal** (default) or **Reverse**.
   d) **DSCP Marking** — Select the type of Differentiated Services Code Point (DSCP) marking 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)** (the default, for no marking). For information on DSCP marking, see *Setting Up a non-CMP Cluster*.
   e) **Replication Stream Count** — Select 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) **Replication & Heartbeat** — Select a network to carry inter-site replication and heartbeat traffic. This field only appears if the system supports georedundancy.
      - **None** (the default)
      - **OAM**
      - **SIG-A**
      - **SIG-B**
      - **REP**

      A warning icon () indicates that you cannot select a network until you define a static IP address on all servers of both sites.
   g) **Backup Heartbeat** — Select a network to carry inter-site backup heartbeat traffic. This field only appears if the system supports georedundancy.
      - **None** (the 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.
5. Define the primary site settings in the **Primary Site Settings** section of the page:

a) **Site Name** — Select **Unspecified** (default) or the name of a previously defined site. If you select **Unspecified**, you create a non-georedundant site, and cannot add a secondary site. You can assign multiple clusters to the same site.

Note: To import the hardware type and VLAN settings from the from the selected site, select **Use Site Configuration**. When this is selected the **HW Type** and VALN IDs become read only. To edit the field, clear the **Use Site Configuration** checkbox. If **Unspecified** is selected for the site name, the **Use Site Configuration** option becomes unavailable.

b) **HW Type** — Select the hardware type.

- **C-Class** (default)
- **C-Class (Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
- **NETRA**
- **RMS**

c) **OAM VIP** (optional) — Enter the address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the address the CMP cluster uses to communicate with the cluster.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

d) **Signaling VIPs** — 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.

At least one signaling VIP is required.

Click **Add New VIP** to add a VIP to the system. You can enter up to four IPv4 or IPv6 addresses and masks of the signaling VIP addresses.

For each new VIP, enter the address and mask in the New Signaling VIP dialog. Select **SIG-A** or **SIG-B** to indicate whether the cluster will use an external signaling network.

For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

e) **General Network VLAN ID** — This field appears if you selected **NETRA**, **C-Class**, or **C-Class(Segregated Traffic)**. Enter the **OAM**, **SIG-A**, and **SIG-B** VLAN IDs, in the range 1–4095. The defaults are 3 for the OAM network and server IP, 5 for the SIG-A network, and 6 for the SIG-B network.

f) **User Defined Network** — This field appears if you selected **C-Class** or **C-Class(Segregated Traffic)**. Enter the REP network VLAN ID, in the range 1–4095.

6. Define Server-A in the **Server-A** section of the page:

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

b) **IP Preference** — Specify 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 IPv6 OAM IP nor a

static IP address is 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.

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

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

d) **Forced Standby** — Select to put Server A into forced standby. (By default, Server A will be the initial active server of the cluster.)

e) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network.

- **SIG-A**
- **SIG-B**
- **REP**
- **BKUP** (if the hardware type is **C-Class(Segregated Traffic)** or **NETRA**)

7. (Optional) Define Server-B in the **Server-B** section of the page. Click **Add Server-B** and enter the standby server information for the cluster:

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

b) **IP Preference** — Specify 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 IPv6 OAM IP nor a static IP address is 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.

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

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

d) **Forced Standby** — Select to put Server A into forced standby. (By default, Server A will be the initial active server of the cluster.)

e) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network.

- **SIG-A**
- **SIG-B**
- **REP**
- **BKUP** (if the hardware type is NETRA)

8. Define the secondary site information in the **Secondary Site Settings** section of the page:

a) **Site Name** — Select **Unspecified** (default) or the name of a previously defined site. This site name must be different from the primary site name. If you select **Unspecified**, you create a non-georedundant site, and cannot add a secondary site. You can assign multiple clusters to the same site.

Note: To import the hardware type and VLAN settings from the from the selected site, select **Use Site Configuration**. When this is selected the **HW Type** and VALN IDs become read only. To edit the field, clear the **Use Site Configuration** checkbox. If **Unspecified** is selected for the site name, the **Use Site Configuration** option becomes unavailable.

b) **HW Type** — Select the hardware type.

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

c) **OAM VIP** (optional) — Enter the address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the address the CMP cluster uses to communicate with the cluster.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

Note: This address corresponds to the cluster address in Policy Management systems before V7.5.

d) **Signaling VIPs** — The signaling VIP is the IP address a PCEF device uses to communicate with a cluster. Clusters support redundant communication channels, named SIG-A and SIG-B, for carriers that use redundant signaling channels.

At least one signaling VIP is required.

Click **Add New VIP** to add a VIP to the system. You can enter up to four IPv4 or IPv6 addresses and masks of the signaling VIP addresses.

For each new VIP, enter the address and mask in the New Signaling VIP dialog. Select **SIG-A** or **SIG-B** to indicate whether the cluster will use an external signaling network.

For an IPv4 address, use the standard dot format, and enter the subnet mask in CIDR notation from 0–32. For an IPv6 address, use the standard 8-part colon-separated hexadecimal string format, and enter the subnet mask in CIDR notation from 0–128.

e) **General Network VLAN ID** — This field appears if you selected **C-Class**, **C-Class(Segregated Traffic)**, or **NETRA**. Enter the **OAM**, **SIG-A**, and **SIG-B** VLAN IDs, in the range 1–4095. The defaults are 3 for the OAM network and server IP, 5 for the SIG-A network, and 6 for the SIG-B network.

f) **User Defined Network** — This field appears if you selected **C-Class** or **C-Class(Segregated Traffic)**. Enter the REP network VLAN ID, in the range 1–4095.

9. Define Server-C in the **Server-C** section of the page. If you define a secondary site, you must define a spare server. Click **Add Server-C** and define the information for the spare server:

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

b) **IP Preference** — Specify 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 IPv6 OAM 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.

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

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

d) **Forced Standby** — Select **Forced Standby** to ensure that the server is in standby mode.

e) **Static IP** — If an alternate replication path and secondary HA heartbeat path is used, then a server address must be entered in this field. Click **Add New**. In the New Path dialog, enter an IP address and mask, and select the network:

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

10. When you finish, click **Save** (or **Cancel** to discard your changes).
You are prompted, "The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving." Click **OK** (or **Cancel** to stop the save operation).

11. If you are setting up multiple clusters, repeat the above steps as often as necessary.

The cluster is defined.

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

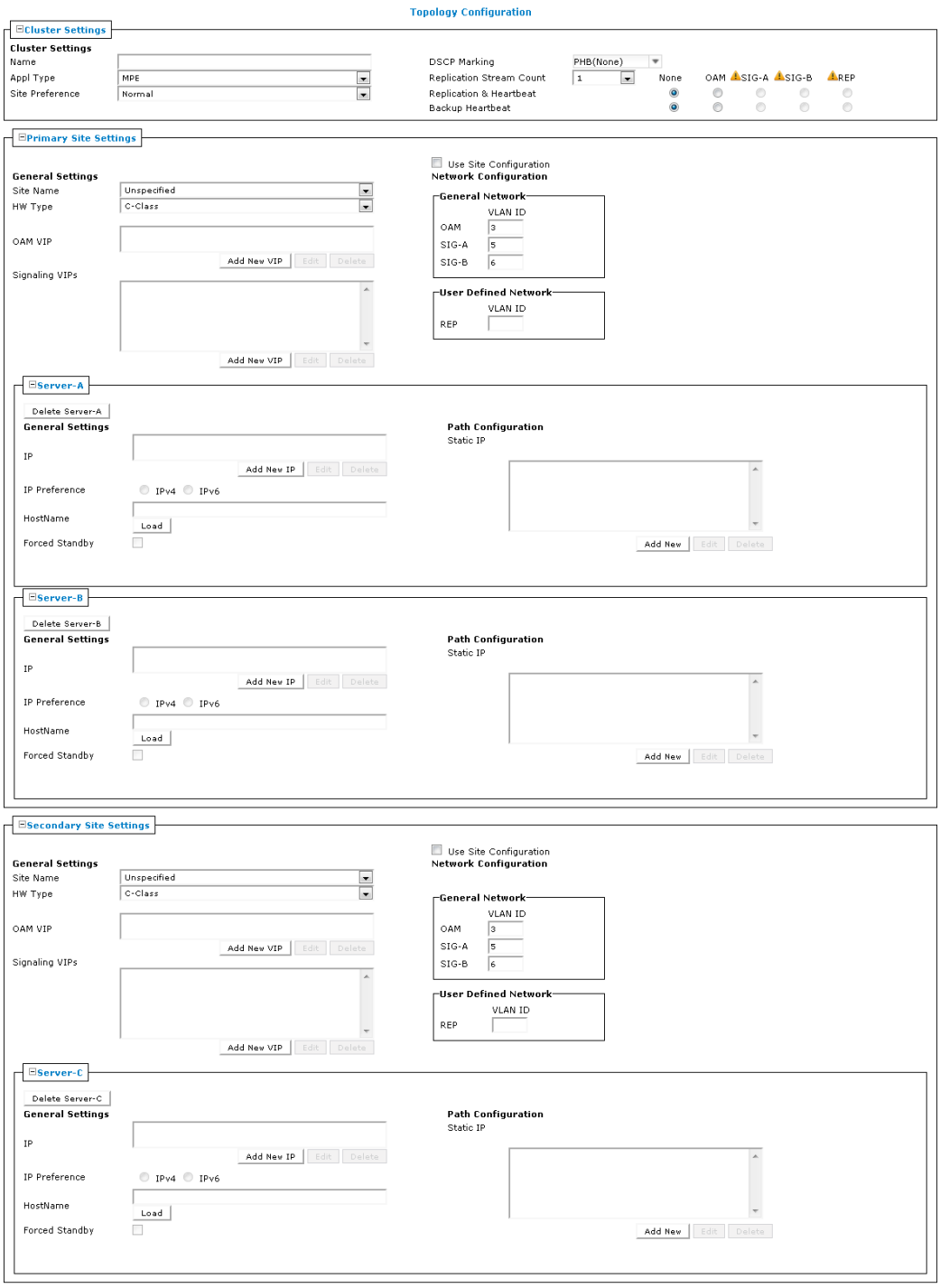


Figure 17: Sample MPE Cluster Topology Configuration

Example: Setting Up Georedundancy

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

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

Before creating a georedundant cluster, ensure the following:

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

Before beginning the procedure, you will need to collect or provide the following information (to collect information, see *Setting Up a Georedundant Cluster*).

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

- The names of existing clusters
- Names for the sites (this procedure uses **`Site-1`** and **`Site-2`**)
- The maximum primary site failure threshold, to record site failures (0 is recommended)
- The OAM VIP address of the existing Site-1 CMP system and, if applicable, the georedundant CMP system
- (Optional) a designated network path, either OAM, REP, SIG-A or SIG-B, for backup (secondary) HA heartbeats between Site-1 and Site-2
- (Optional) a designated network path, either OAM, REP, SIG-A or SIG-B, for WAN replication traffic between Site-1 and Site-2
- Initial provisioning information for Server-C:
  - A hostname (this procedure uses **`Server-C`**)
  - For CMP access, an OAM IPv4 or IPv6 address and subnet mask
  - An OAM IPv4/IPv6 default route
  - A list of network time protocol (NTP) server IP addresses
  - A list of domain name system (DNS) server IP addresses
  - VLAN IDs for OAM, REP, SIG-A, and SIG-B network paths
  - For IPv4-based network elements, an IPv4 VIP address and subnet mask on the SIG-A network
  - For inter-topology communication or any IPv6-based network elements, an IPv6 VIP address and subnet mask on the SIG-A network
  - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, an IPv4/IPv6 static address and subnet mask on the REP network
- For each existing HA cluster:
  - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, a VLAN ID for the REP network path
  - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, an IPv4/IPv6 static address and subnet mask on the REP network for Server-A

  - If the REP network is used for either WAN replication traffic or backup (secondary) HA heartbeats, an IPv4/IPv6 static address and subnet mask on the REP network for Server-B
  - Verify that firewall rules are correctly provisioned (for more information, see the *Platform Configuration User's Guide*)
- If DSCP marking for WAN replication traffic is used, the type of DSCP marking
- If multi-stream WAN replication traffic is used, the replication stream count

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

Caution: This procedure interrupts service.

1. Using the Platform Management & Configuration utility, install the MPE application on Server-C.

   This step is beyond the scope of this document. Refer to the PM&C documentation, and 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.

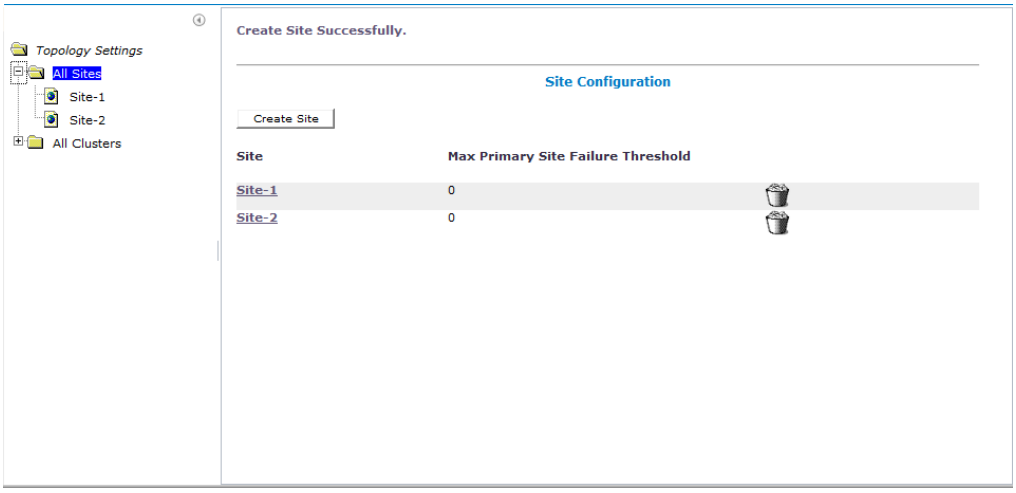
   See *The Mode Settings Page*.

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

6. Define the two sites.

   See *Setting Up a Site*.

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



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:

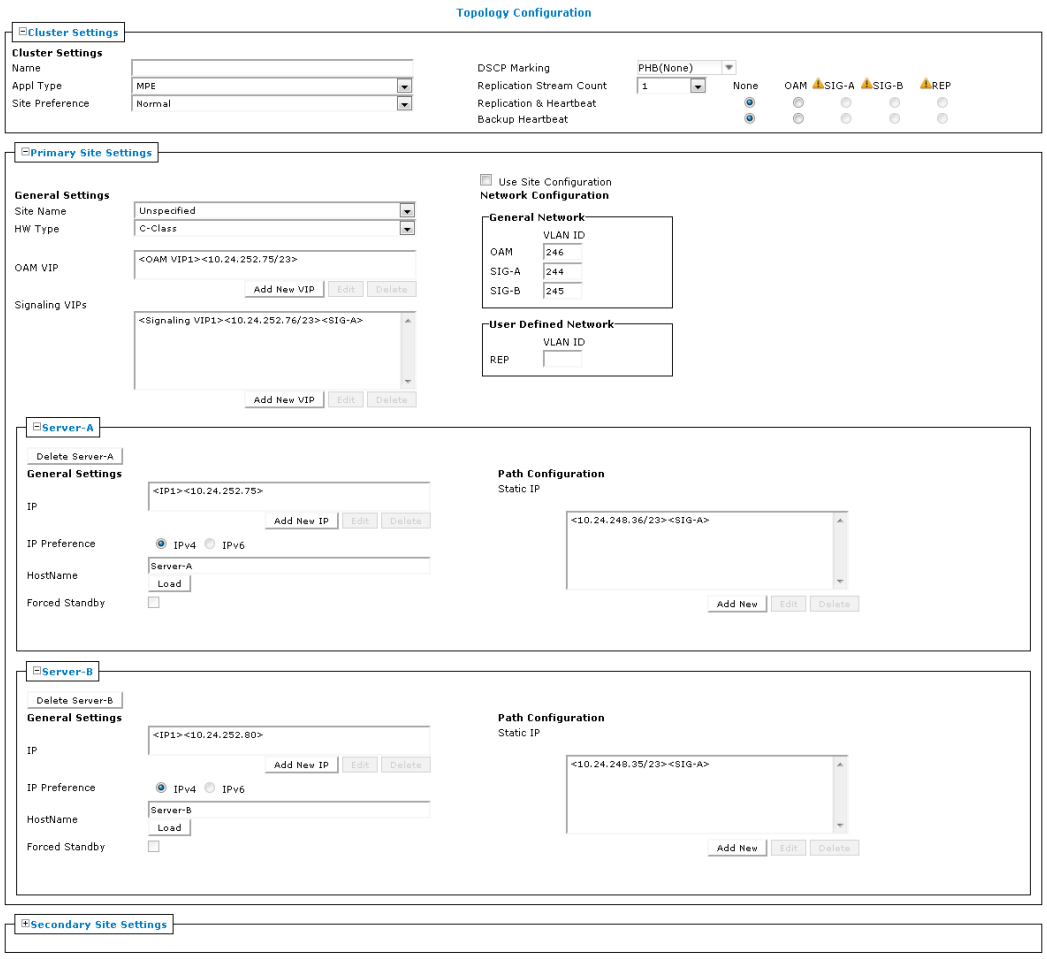


Figure 18: Example of Primary Site Settings

13. Click **Save** (at the bottom of the page). You are prompted, "Active server will restart." Click **OK**. Server-A restarts. You must now define the Site-2 and Server-C configuration.
14. From the **Platform Setting** section of the navigation pane, select **Topology Settings**. The **Cluster Configuration** page opens.
15. From the content tree, select the **All Clusters** group. The **Cluster Configuration** page opens, displaying the defined clusters.
16. 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.
17. Click **Modify Secondary Site**. The fields in the **Secondary Site Settings** section of the page become editable.
18. 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.

19. In the **Server-C** section of the page:

a) Click **Add Server-C**.

b) In the **IP** field, enter the OAM IP address.

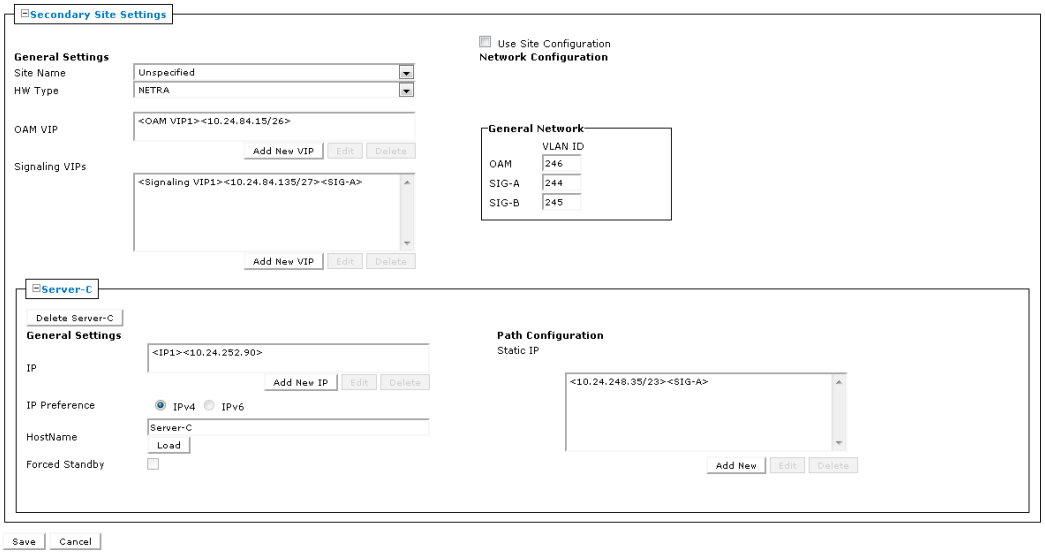
c) In the **IP Preference** field, enter the preferred IP version, either **IPv4** or **IPV6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an OAM IPv6 IP nor a static IP address defined, the IPv6 radio button cannot be selected here. Similarly, If 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 pop-up 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:



20. Click **Save** (at the bottom of the page). You are prompted, "Active server will restart." Click **OK**. Server-A restarts.

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

21. Click the status of Server-C.
The status changes to **Spare**.

22. Click **Save**.
The configuration is saved.

23. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens.

24. From the content tree, select the **All Clusters** group.
The **Cluster Configuration** page opens, displaying the defined clusters.

25. 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.

26. Click **Modify Cluster Settings**.
    The fields in the **Cluster Settings** section of the page become editable.
27. 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).
28. Click **Save**.
    The configuration is saved.
29. Verify the status of Server-C by viewing the cluster.
    Server-C appears as part of the cluster in the Force Standby state with replication on.
30. 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") will appear in the report, but with severity Clear.
31. 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*.
32. 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*.
33. Modify the cluster configuration to cancel the "Force Standby" state of Server-C.
    The state of Server-C changes to Spare.
34. 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 appears as part of the cluster, in the state "Spare."
35. (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*.
36. Use the **Data Sources** function to configure routes on Server-C to existing data sources.

    For more information, see *Configuring Data Source Interfaces*.
37. 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." Click **OK**.
e) Use the **System Maintenance** function to verify that Server-C has become the active server.
f) Use the **Policy Server Reports** function to verify that Sh connections are active on Server-C.
For more information, see *Data Source Statistics*.

38. 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 role. Oracle recommends not attempting to force Server-A back into the Active role, 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

Once 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

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

Modifying a Site

To modify a site:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
The **Cluster Configuration** page opens, displaying information about the clusters in the Policy Management network topology.
2. From the content tree, select the site you want to modify.
The **Site Configuration** page displays information about the site.
3. Click **Modify**.
The **Modify Site** page opens.
4. Modify site information.
For a description of the fields contained on this page, see *Setting Up a Site*.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The site is modified.

Removing a Site from the Topology

You can remove a site from a georedundant topology. You can only remove a site if it is not referenced by a C-level cluster. Once the site is in use by a cluster, if you try to delete it, you are prompted, "*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 **Topology 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 the Delete icon, located to the right of the site you wish to delete.
   - From the content tree, select the site and click **Delete**.

   You are prompted, "Are you sure you want to delete this Site?"
4. Click **Delete** (or **Cancel** to abandon your request).
   The page closes.

The site is removed from the topology.

Modifying an MPE or MRA Cluster

To modify an MPE or MRA 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 cluster you want to modify.
   The **Topology Configuration** page opens, displaying information about the cluster.
3. Click the appropriate button for the changes you want to make:
   - To modify cluster settings, click **Modify Cluster Settings**.
   - To modify the Server-A configuration, click **Modify Server-A**.
   - To modify the Server-B configuration, click **Modify Server-B**.
   - To delete either server configuration, click the appropriate button to modify the server and then click the delete button.

   The appropriate fields on the **Topology Configuration** page become editable.
4. Make changes as required.

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

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

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

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

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

Modifying a CMP Cluster

To modify a CMP cluster:

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

   The fields on the **Topology Configuration** page become editable. For information on configurable fields, see *Setting Up a CMP Cluster*.
4. Make changes.

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

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

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

Removing a Cluster from the Topology

You can remove an MPE, MRA, or Site 2 CMP cluster from the topology. (You cannot remove the Site 1 (primary) 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** folder.
   The **Cluster Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology.
3. In the topology configuration table, in the row listing the cluster you want to remove, click **Delete**.
   You are prompted, "Are you sure you want to delete this Cluster?"
4. Click **Delete** (or **Cancel** to abandon your request).
   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.

Once the cluster is removed, use the Platform Configuration utility to remove cluster information. For more information, see the *Platform Configuration User's Guide*.

Reversing Cluster Preference

You can change the preference, or predilection, of the servers in a cluster to be active or spare. This setting is only available when the system has been configured for georedundancy.

To reverse cluster preference:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Topology Configuration** page opens.
2. Select the cluster from the content tree.
   The **Topology Configuration** page opens, displaying information about the selected cluster.
3. Click **Modify Cluster Settings**.
   The fields become editable.
4. In the **Cluster Settings** section of the page, toggle the **Site Preference** between **Normal** and **Reverse**.
5. Click **Save** (or **Cancel** to abandon your change).

The cluster preferences are reversed.

Demoting a 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.

When you demote a CMP cluster, the secondary site (which is typically the Site 2 cluster) can become the primary site. This is a manual process. 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. 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 CMP cluster:

1. Log in to the currently active georedundant CMP cluster.
2. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Topology Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology. 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 options to **View** and **Demote**.
3. 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.

4. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Topology Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology. You should see options 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.

5. Return to the browser window logged in to the primary CMP cluster.
   You should still be on the **Topology Configuration** page.
6. In the Cluster Settings table, in the row listing the primary CMP cluster, click **Demote**.
   You are prompted, "Are you sure you want to demote this Cluster?"
7. Click **OK** (or **Cancel** to abandon your request).
   The page displays the message "Demote cluster successfully."
8. Log out of the CMP system for the cluster you have just demoted.
9. Return to the browser window logged in to the secondary CMP cluster.
   You should still be on the **Topology Configuration** page.
10. Wait two minutes.
11. 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?"
12. Click **OK** (or **Cancel** to abandon your request).
    The page displays the message "Promote cluster successfully."
13. Log out of the CMP system for the cluster you have just promoted.
14. Log in to the CMP system for the cluster you have just promoted.
15. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
    The **Topology Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology. The cluster is marked with (P), and the name of the secondary cluster is marked with (S). The old primary cluster may briefly display as off-line.

    Note: You should see options to **View** and **Demote**. All functions available from the primary CMP cluster should now appear and be accessible.

16. Wait ten minutes and then use the **Topology Configuration** page to verify that both the primary and secondary CMP clusters are available and have the correct status.

The primary CMP cluster is demoted, and the secondary cluster is promoted to primary status.

Forcing a Server into Standby Status

You can change the status of a server in a cluster to Forced Standby. A server placed into Forced Standby status is prevented from assuming the role Active. You would do this, for example, to the active server prior to performing maintenance on it.

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

- If the server is active, 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 force all servers in a cluster into Standby status, you can trigger a site outage.

To force a server into standby status:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Topology Configuration** page opens, displaying a cluster settings table listing information about the clusters defined in the topology.
2. In the cluster settings table, in the row listing the cluster containing the server you want to force into standby status, click **View**.
   The **Topology Configuration** page displays information about the cluster.
3. Select the server. Click **Modify Server-A** or **Modify Server-B**, as appropriate.
4. Select **Forced Standby**.
5. Click **Save** (or **Cancel** to abandon your request).
   The page closes.

The server is placed in standby status.

Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network. 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 server in the primary cluster. A banner warning appears if the login is not on the active primary CMP system.

To configure SNMP settings:

1. Log in to the CMP system from its server address as a user with administrator privileges.

   The navigation pane is displayed.

2. From the **Platform Setting** section of the navigation pane, select **SNMP Setting**.

   The **SNMP Settings** page displays.

3. Click **Modify**.

   The **SNMP Settings** page opens.

4. Edit the settings.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

Table 3: SNMP Attributes describes the SNMP attributes that can be edited.

Table 3: SNMP Attributes

Field Name	Description
Manager 1-5	SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IPv4/IPv6 address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. Port configuration is optional for each manager and it can have a value between 1 and 65535. If it is not configured and left blank, the port defaults to 162. By default, these fields are blank.
Enabled Versions	Supported SNMP versions: • **SNMPv2c** • **SNMPv3** • **SNMPv2c and SNMPv3 (default)**
Traps Enabled	Enable the sending SNMPv2 traps (default is enabled). **Note:** This option must be selected to use the SNMP Trap Forwarding feature. Clear the checkbox to disable sending SNMPv2 traps.
Traps from individual Servers	Enable sending traps from an individual server (default is disabled). **Note:** To use the SNMP Trap Forwarding feature, ensure that this option is not selected. Clear the checkbox to send traps from the active CMP system only.
SNMPv2c Community Name	The SNMP read-write community string. 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`**.
SNMPv3 Engine ID	Configured Engine ID for SNMPv3. The field is required If SNMPv3 is enabled.

Field Name	Description
	The Engine ID includes only hexadecimal digits (0-9 and a-f). The length can be from 10 to 64 digits. The default is no value (empty).
SNMPv3 Security Level	SNMPv3 Authentication and Privacy options are: 1. **No Auth No Priv** — Authenticate using the Username. No Privacy. 2. **Auth No Priv** — Authentication using MD5 or SHA1 protocol. 3. **Auth Priv** — Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol. The default value is **Auth Priv**.
SNMPv3 Authentication Type	Authentication protocol for SNMPv3. Options are: 1. **SHA-1** — Use Secure Hash Algorithm authentication. 2. **MD5** — Use Message Digest authentication. The default value is **SHA-1**.
SNMPv3 Privacy Type	Privacy Protocol for SNMPv3. Options are: 1. **AES** — Use Advanced Encryption Standard privacy. 2. **DES** — Use Data Encryption Standard privacy. The default value is **AES**.
SNMPv3 Username	The SNMPv3 User Name. The field is required if SNMPv3 is enabled. The name must contain alphanumeric characters and cannot not exceed 32 characters in length. The default value is **`TekSNMPUser`**.
SNMPv3 Password	Authentication password for SNMPv3. This value is also used for msgPrivacyParameters. The field is required If SNMPv3 is enabled. The length of the password must be between 8 and 64 characters; it can include any character. The default value is **`snmpv3password`**.

Configuring the Upsync Log Alarm Threshold

You can configure the threshold of outstanding updates to a slave machine 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 is displayed.

2. Click **Modify**.
3. Enter the threshold.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

Configuring Concurrent Bulk Transfers

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

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

The recommended number is based on the available bandwidth within the WAN. For example, if the WAN is 1GB/s, it is best to specify 1 bulk transfer.

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

   The **Platform Configuration** page is displayed.

2. Click **Modify**.
3. Enter the number bulk transfers. Valid values are 1 to 8. 1 is the default.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

Chapter 4

Managing Multimedia Policy Engine Devices

Topics:

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

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

Policy Server Profiles

A policy server profile contains the configuration information for an MPE device (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. Once you define profiles, you deploy them to MPE devices across the network.

The following subsections describe how to manage policy server profiles. For information on deploying defined policies to an MPE device, see the *Policy Wizard Reference*.

Creating a Policy Server Profile

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

To create a policy server profile:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Policy Server Administration** page opens in the work area.
3. Click **Create Policy Server**.
   The **New Policy Server** page opens.
4. Enter values for the configuration attributes:
   a) **Associated Cluster** (required) — Select the cluster with which to associate this MPE device.
   b) **Name** — Name of this MPE device. The default is the associated cluster name. A name is subject to the following rules:
      - Is case insensitive (uppercase and lowercase are treated as the same)
      - Must be no longer than 255 characters
      - Must not contain quotation marks (") or commas (,)
   c) **Description / Location** (optional) — Information that defines the function or location of this MPE device.
   d) **Secure Connection** — Designates whether or not to use the HTTPS protocol for communication between Policy Management devices. If selected, devices communicate over port 8443.

      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.

   e) **Type** — Defines the policy server type:
      - **Oracle** (the default) — The policy server is an MPE device and can be fully managed by the CMP.
      - **Unmanaged** — The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non-Oracle policy server.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

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

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

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

Configuring or Modifying a Policy Server Profile

To configure or modify a policy server profile:

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

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

   The page contains the following tabs:

   - **System** — Defines the system information associated with this policy server, including the name, host name or IP address in IPv4 or IPv6 format, information about the policy server, and whether or not the policy server uses a secure connection to any management system (such as the CMP).
   - **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, Syslog, and SMS log configurations.
   - **Policy Server** — Lets you associate applications and network elements with the MPE device and configure protocol information.
   - **Diameter Routing** — Lets you configure the Diameter peer and route tables.
   - **Policies** — Lets you manage policies that are deployed on the policy server.
   - **Data Sources** — Lets you configure interfaces to LDAP (Lightweight Directory Access Protocol), Diameter Sh, or SPR (Subscriber Profile Repository) systems.
   - **Session Viewer** — Displays the Session Viewer.

3. Select the tab that contains the information you want to modify and click **Modify**.
4. When you finish your modifications, click **Save** (or **Cancel** to discard your changes).

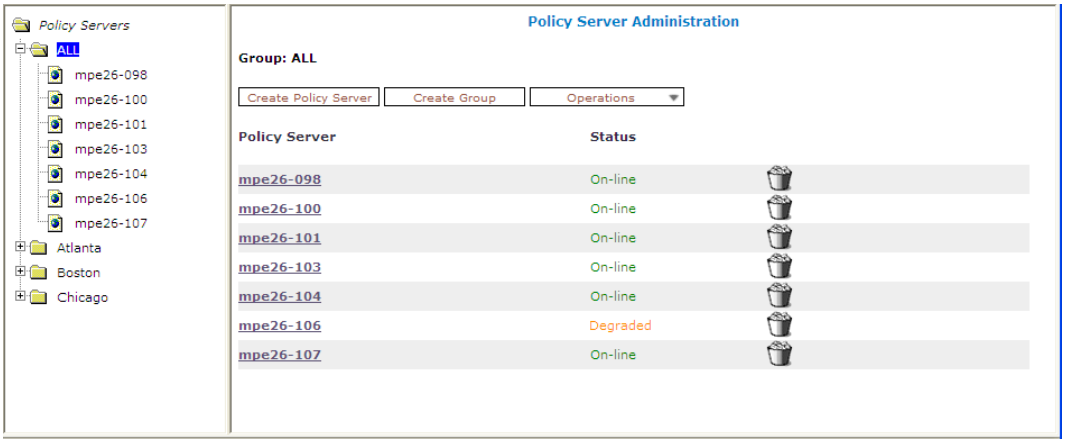
Deleting a Policy Server Profile

Deleting a policy server (MPE device) profile from the ALL group also deletes it from any associated group. You cannot delete a policy server profile if it is configured in an MPE pool.

To delete an MPE device profile:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of 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, displaying all defined MPE devices; for example:



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

   You are prompted, "Are you sure you want to delete this Policy Server?"
4. Click **OK** to delete the MPE device profile (or **Cancel** to cancel the request).
   The profile is removed from the list.

The policy server profile is deleted.

Managing Configuration and Virtual Templates

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

Virtual Templates

Virtual templates are similar to symbolic links in Linux. Virtual templates are particularly efficient when users want to replace a template that has been associated to multiple MPEs or MRAs with another template.

Overlaps

Overlaps occur when both a template and an MRA or MPE are assigned an identical value for the same attribute or field. For example, the index of a user name is true in template A, and the index of a user name is also true in an MRA or MPE. The result is that when the template and MRA or MPE are associated, the index of the user name becomes an overlapped field. When an overlap occurs, a prompt opens stating, "The server configuration has overlaps with the associated template(s)." The user can take one of two actions:

- Remove the overlaps and use the settings from the template. For this action, the value of the template is used.
- Keep the overlaps and use the settings from the server. For this action, the value of the server will be used.

Creating a Template

Since an MPE or an MRA can exist independently of one another, there are two locations in the Policy Management interface where, both virtual and configuration, templates can be created. Either in the **MRA** or the **Policy Server** section of the Navigation Pane. Once created, the templates will have the functionality specific to their instance (MPE or MRA).

Note: Both MPE or MRA devices are described in this procedure.

Complete these steps to create a configuration template.

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**. The content tree displays a list of **All Templates** including Virtual and Configuration.

   Note: You must create a Configuration Template before a Virtual Template because a Virtual Template references and is dependent on a Configuration Template.

2. From the content tree, select **Configuration Template**.
   The **Configuration Template Administration** page opens.
3. Click **Create Template**.
   The **New Configuration Template** page opens.
4. Enter the **Name** of the template.

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

5. (Optional) Select a template from the Copy From pull-down menu.
6. (Optional) Type in a **Description / Location** (limited to 255 characters).
7. Click **Save** (or **Cancel** to discard changes).
   The settings are saved for the template and applied to all associated MPE or MRA devices.

Modifying a Template

Since an MPE or an MRA can exist independently of one another, there are two locations in the Policy Management interface where , both virtual and configuration, templates can be managed. Either in the **Policy Server** or the **MRA** section of the **Navigaton Pane**. Once created, the templates will have the functionality specific to their instance (MPE or MRA). After templates are created and associated, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

Note: Both MPE or MRA devices are described in this procedure.

Complete these steps to modify a configuration template.

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**. The content tree displays a list of all templates including Virtual and Configuration.

   Note: You must create a Configuration Template before a Virtual Template because a Virtual Template references and is dependent on a Configuration Template.

2. From the content tree, select the Configuration Template for modification.
   The **Configuration Template Administration** page opens with the template.
3. Click **Modify**. From the **MRA** and **Diameter Routing** tabs, you can configure the following:
   - From the **MRA** section you have the following tabs and options:
     - **Template** tab
       - **Name**
       - **Description**
     - **MRA** tab - **Modify** button
       - **Associations** or
       - **MPE Pools**
       - **Subscriber Indexing**
       - **Diameter** settings
     - **MRA** tab - **Advanced** button
       - **Expert Settings**
       - **Service Overrides**
       - **Load Shedding Configuration**
     - **Diameter Routing** tab
       - **Diameter Peers**
       - **Diameter Routes**
   - From the **Policy Server** section you have the following tabs and options:
     - **Template** tab
       - **Name**
       - **Description**
     - **Logs** tab
       - **Modify Policy Log Settings**
       - **SMS Log Configuration**
       - **SMTP Log Configuration**
     - **Policy Server** tab - **Modify** button
       - **Associations**
       - **Subscriber Indexing**
       - **Configuration**
       - **Diameter** settings
       - **User Profile Lookup Retry on Session Updates**
       - **Diameter AF Default Profiles**
       - **Default Charging Servers**
     - **Policy Server** tab - **Advanced** button
       - **Expert Settings**
       - **Service Overrides**

    - **Load Shedding Configuration**
- **Diameter Routing** tab
    - **Diameter Peers**
    - **Diameter Routes**
- **Policies** tab
    - **Deployed Policies**
- **Data Sources** tab
    - **Data Sources**
    - **General Settings**
    - **Sh Settings**

4. Click **Save** (or **Cancel** to discard changes).

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

Reordering Templates

Since an MPE or an MRA can exist independently of one another, there are two locations in the Policy Management interface where templates can be created. Either in the **Policy Server** or the **MRA** section of the Navigation Pane. Templates have the functionality specific to their instance (MPE or MRA). After a template is created and associated, the template can be viewed in the **System** tab of the **Configuration** for the MPE or MRA device.

Note: Both MPE or MRA devices are described in this procedure.

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

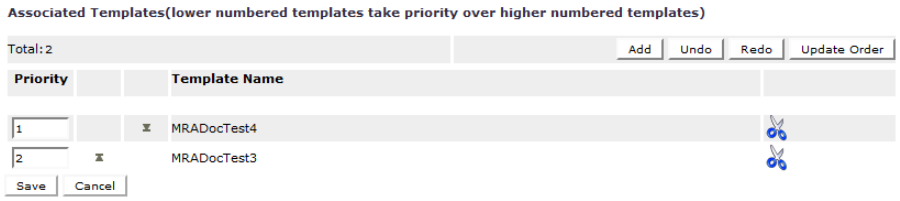


Figure 19: Template Reorder Feature

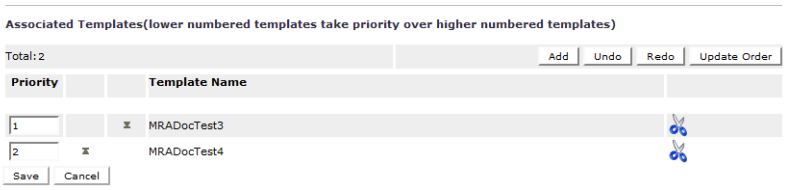


Figure 20: Template Reorder Feature Amended

Creating Virtual Templates

Since an MPE or an MRA can exist independently of one another, there are two locations in the Policy Management interface where, both virtual and configuration, templates can be created. Templates can be created and managed either in the **Policy Server** or **MRA** section of the Navigation pane. Because Virtual templates are based on Configuration Templates, modifying a Configuration Template associated with a Virtual Template automatically modifies the Virtual Template. After the templates are created, the templates have the functionality specific to their instance (MPE or MRA).

Note: Both MPE or MRA devices are described in this procedure.

Complete these steps to create a configuration template.

1. From the **MRA** or **Policy Server** section of the Navigation pane, select **Configuration Templates**. The content tree displays a list of all templates including Virtual and Configuration.

   Note: You must create a Configuration Template before a Virtual Template because a Virtual Template references and is dependent on a Configuration Template.

2. From the content tree, select **Virtual Templates**.
   The **Virtual Template Administration** page opens.
3. Click **Create Virtual Template**.
   The **New Virtual Template** page opens.
4. Enter the **Name** of the template.

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

5. Select a template from the **Associated Configuration Template** pull-down menu.
6. (Optional) Type in a **Description**.
7. Click **Save** (or **Cancel** to discard changes).
   The settings are saved for the template, and applied to all associated MRA or MPE devices.

Configuring Protocol Options on the Policy Server

To configure protocol options on an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the desired MPE device.
   The **Policy Server Administration** page opens.
3. Select the **Policy Server** tab.
   The current configuration options are displayed.
4. Click **Modify** and define options as necessary.

   Table 4: Policy Server Protocol Configuration Options defines available options. (The options you see may vary depending on the mode in which your system is configured.)

5. When you finish, click **Save** (or **Cancel** to discard your changes).

You have defined the protocol options for this MPE device.

Table 4: Policy Server Protocol Configuration Options

Attribute	Description
Associations	
Applications	The application profiles associated with this MPE device. To modify this list, click **Manage**. For more information on application profiles, see the *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*.
Subscriber Indexing	**Note:** The indexing parameters to use depend on how Sh is used. If you are unsure which indexing method(s) to configure, contact My Oracle Support.
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).
Index by IP Address	Select if the associated Subscriber Profile Repository is indexed by IP address. You can select **Index by IPv4**, **Index by IPv6**, or both formats.
Overrides by APN	Select to configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN). In the **Overrides by APN** section, click **Add**. Enter the APN and click **Save** to enable **Index by IPv4**, **Index by IPv6**, or both. You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.
Configuration	
Time of Day Triggering	Select **Enable** or **Disable** (default) from the pulldown menu. 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 the *Policy Wizard Reference*.
Billing Day	If enabled, you can configure a global monthly billing day for subscribers who do not have a specific day configured in their profiles in a backend 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

Attribute	Description
	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 Savings Changes	If selected, the MPE device observes Daylight Savings Time for the configured Billing Time Zone.
Default Local Time Mode	Select the time used within a user's session from the pulldown menu: **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 disabled, the full monthly quota for the subscribers is granted for the billing cycle following a quota reset. If enabled, 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 subscriber's 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 enabled, 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 *off* (at the MPE device), then the unknown users are allowed to create sessions. In this case, if Subscribe for Unknown Users is enabled, 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 enabled, the MPE device reads multiple Sh user data blocks (subscriber, quota usage, and entity state) with a single read request. If you enable this

Attribute	Description
	feature, you must also configure the Sh data source with the option **Notif-Eff**. If disabled, separate lookups are used.
Use Combined Writes	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 enabled, the MPE device caches the quota usage objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.
Cache Entity State	If enabled, 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	Subscribe to receive notifications from the SPR for any changes to the quota.
Subscribe Entity State	Subscribe to receive notifications from the SPR for any changes to the entity state.

RADIUS-S	
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	
Diameter Port	The port for the MPE device. (for example, 3868)
Diameter Realm	The domain of responsibility (for example, **`galactel.com`**) for the MPE device.
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, **`mpe3.galactel.com`**).
Default Resource Id	The bearer used if a GGSN does not send any bearer information in a Credit-Control Request (CCR). Enter an alphanumeric string of up to 100 characters. The default is no resource ID (that is, no bearer).
Correlate PCEF sessions	If selected, 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 enabled, 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.
Use Synchronous Sd	If selected, 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 enabled, 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	Available only if "Identify Duplicate sessions based on APN" is selected. Select the subscriber index type to use from the pulldown list: **Username**, **NAI**, **E.164 (MSISDN)**, or **IMSI**.
Protocol Timer Profile	The timer profile to use.
Prevent Overlapping Rule Names	If selected, rule names that are dynamically generated on the primary and spare MPE devices in the same Gx session are unique.

User Profile Lookup Retry and Session Updates	
Enforcement	If enabled, allows user profile lookup retry on session updates for Gx and Gxx updates.
Application	If enabled, allows user profile lookup retry on session updates for Rx.

Diameter AF Default Profiles	
	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: • **Default** • **Audio** • **Video**

	• **Data** • **Application** • **Control** • **Text** • **Message** • **Other**. The **Default** profile is used when a profile for a media type is not defined. To specify values, create Diameter profiles in the general profile configuration.
Default Charging Servers	
Primary Online Server	FQDN of the primary online charging server (used, for example, for prepaid accounts).
Primary Offline Server	FQDN of the primary offline charging server (used, for example, for billed accounts).
Secondary Online Server	FQDN of the secondary (backup) online charging server.
Secondary Offline Server	FQDN of the secondary (backup) offline charging server.

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

SMPP Configuration	
SMPP Enabled	Select 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 to validate message length.
SMPP Long Message Support	If selected, 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 pulldown list: • **Segmentation and Reassembly (SAR)** (default) • **Message Payload**
(Primary) SMSC Host	Enter the FQDN or IP address of the primary Short Messaging Service Center store-and-forward server, which 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. 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	Enter the FQDN or IP address of the secondary Short Messaging Service Center store-and-forward server, which accepts SMS messages from the relay server. The secondary SMSC server is used if the primary server fails.
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. 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 pulldown menu: • **UNKNOWN** (default) • **INTERNATIONAL**

	• **NATIONAL** • **NETWORK SPECIFIC** • **SUBSCRIBER NUMBER** • **ALPHANUMERIC** • **ABBREVIATED**
ESME Source Address NPI	Select the source address Number Plan Indicator (NPI) from the pulldown menu: • **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 pulldown menu: • **SMSC Default Alphabet** • **IA5 (CCITT T.50)/ASCII (ANSI X3.4)** • **Latin 1 (ISO-8859-1)** • **Cyrillic (ISO-8859-5)** • **Latin/Hebrew (ISO-8859-8)** • **UCS2 (ISO/IEC-10646)** • **ISO-2022-JP (Music Codes)** • **JIS (X 0208-1990)** • **Extended Kanji JIS(X 212-1990)**
SMSC Default Encoding Scheme	Select the SMSC default encoding from the pulldown menu: **UTF-8** or **GSM7**.
Request Delivery Receipt	Select the global default behavior when evaluating the policy action **send SMS** from the pulldown menu: • **No Delivery Receipt** • **Delivery Receipt on success and failure** • **Delivery Receipt on failure**

SMS Relay Configuration	
SMS Enabled	Select to enable SMS messaging to subscribers.
Relay Host	FQDN or IP address of the relay server.
Relay Port	Port number on which the relay server is listening for SMS messages. The default port is 8080.

Throttle Value	Sets the time interval, in milliseconds, at which SMS messages are sent from the MPE device. If set to 1000 ms (default), the MPE device sends one SMS message per second; if set to 500 ms, the MPE device sends two messages per second.

SMTP Configuration	
SMTP Enabled	Select 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. They range from 1–10. **Note:** SMTP connections can be increased to support a higher throughput.
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 appears as a signature in an SMTP message. The default is none.

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 to the table** — Click **Add** and then select the data source type from the **Add** pulldown list; the appropriate **Add Data Source** window opens. Configure values as appropriate.
     - 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*.
   - **To clone a data source in the table** — Select an existing data source in the table and click **Clone**; the **Clone Data Source** window opens with the information for the data source. Make changes as required.
   - **To edit a data source in the table** — Select the data source in the table and click **Edit**; the **Edit Data Source** window opens, displaying the information for the data source. Change the configuration values as required.

- **To delete a data source from the table** — Select the data source in the table and click **Delete**; you are prompted, "Are you sure you want to delete the selected data source(s)?" Click **Delete** to remove the data source entry (or **Cancel** to cancel your request).
- **To change the order of the list** — If you define multiple data sources, they are searched in the order displayed in this list. To change the order, select a data source and click the **Up** or **Down** arrows.

When you finish, click **Save** (or **Cancel** to discard your changes).

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

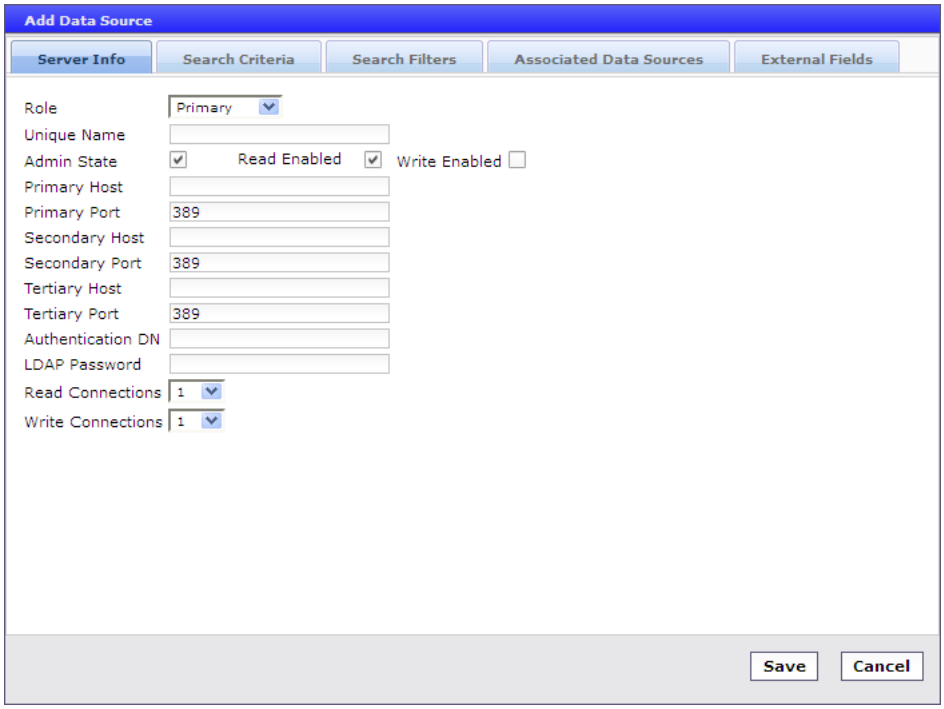
Configuring an LDAP Data Source

For LDAP, you can configure connections to up to three servers. The **Add Data Source** window contains the following tabs:

- **Server Info**
- **Search Criteria**
- **Search Filters**
- **Associated Data Sources**
- **External Fields**

Server Info Tab

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



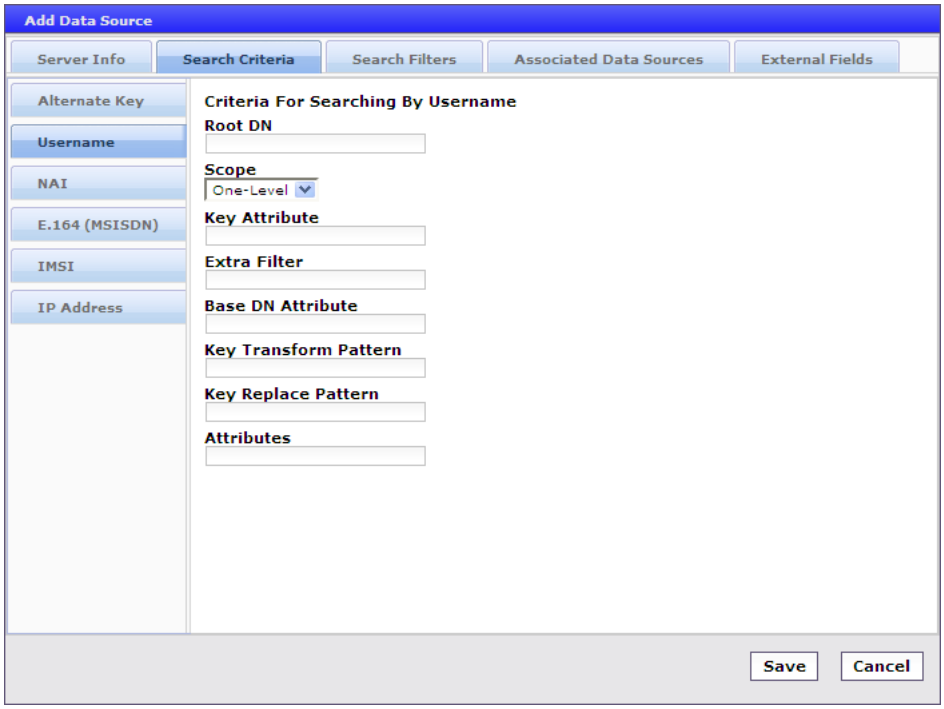
- **Role**— Data source attribute:
  - **Primary** — The data source which performs the initial level of lookups.
  - **Secondary** — Indicates a dependency on the results of the prior lookup. It must initially be associated with the primary data source and configured to be used in a subscriber lookup.
- **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 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** (the 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 form *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:

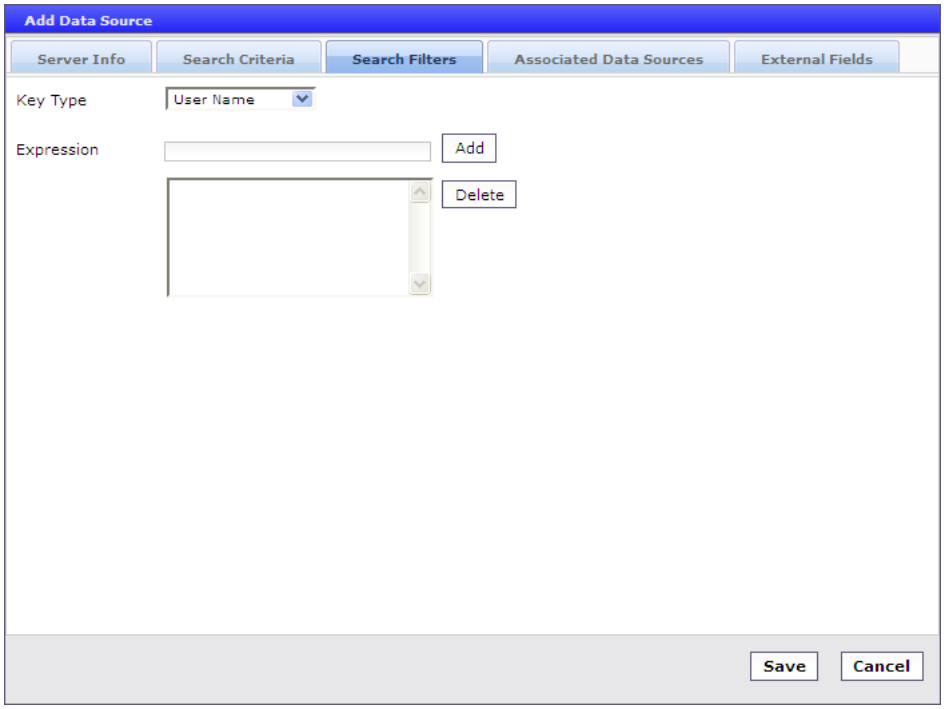
   - *attr* — A field is saved with the same name and value as the specified attribute.
   - *field=attr* — A field with the specified name is saved with the value of the specified attribute.
   - *field=attr*[*from*:*to*] — A field with the specified name is saved with a substring of the value of the specified 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.

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:



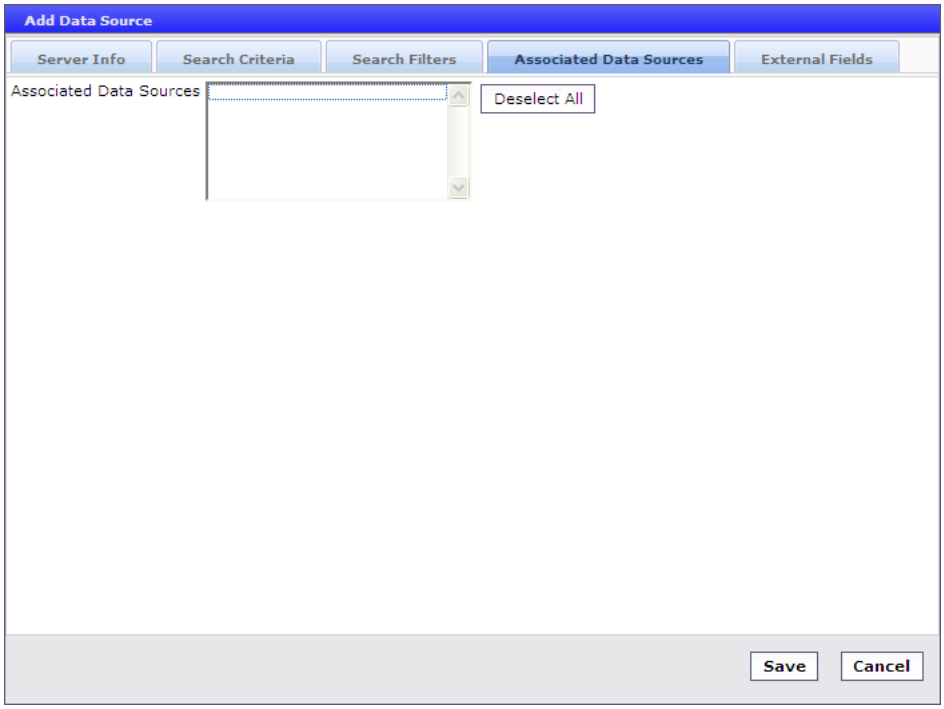
1. **Key Type** — Select from the list:
   - **User Name** (the default) — User name (account ID)
   - **NAI** — Network address ID
   - **E.164(MSISDN)** — E.164 phone number
   - **IMSI** — International Mobile Subscriber Identity
   - **IP Address** — IP address
2. **Expression** — Enter a regular 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. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The expression is added to the filters.

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:

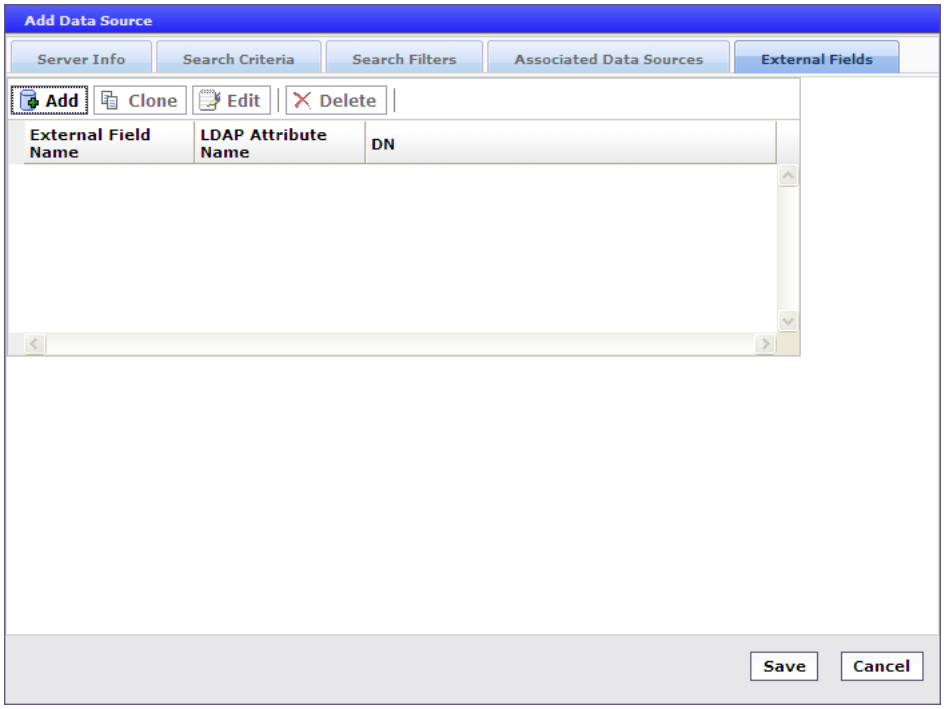
```
LDAP1.AssociatedLDAPs=1234567890111111, 123456789022222
```

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 lets you 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:



- **To add a field to the table** — Click **Add**; the **Add External Field** window opens. Enter the external field name, LDAP attribute name, and distinguished name (DN). Click **Save** when you finish (or **Cancel** to close the window and abandon your change).
- **To clone a field in the table** — Select an existing field in the table and click **Clone**; the **Clone External Field** window opens with that field's information filled in. Make changes as required. Click **Save** when you finish (or **Cancel** to close the window and abandon your change).
- **To edit a field in the table** — To edit a field name or value, select the field in the table and click **Edit**; the **Edit External Field** window opens, displaying the field's information. Make changes as required. Click **Save** when you finish (or **Cancel** to close the window and abandon your change).
- **To delete a field from the table** — Select the field(s) in the table and click **Delete**; you are prompted, "Are you sure you want to delete the selected External Field(s)?" Click **Delete** to remove the data source entry (or **Cancel** to cancel your request).

Configuring an Sh Data Source

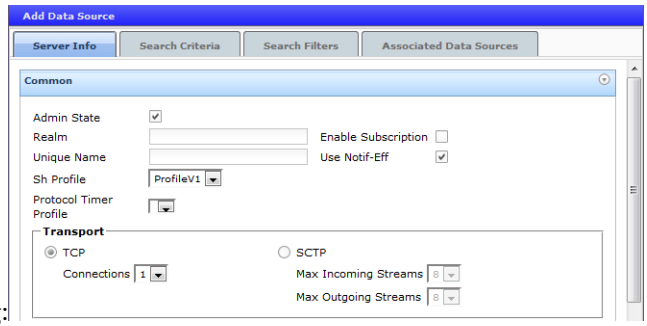
For an Sh data source, you can define two active primary connections and two standby backup connections. An incoming message can be handled from either active connection. You can subscribe through the MPE device (via the Sh interface) to receive notifications on changes to the Quota and Entity State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

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

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

You can specify settings that apply to all Sh data sources. See *Configuring Data Source Interfaces* for more information.

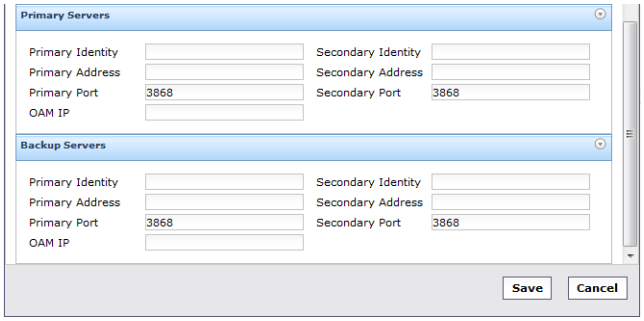
Server Info Tab



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

1. **Admin State** — Enable this data source.
   Selected by default.
2. **Realm** -- Server realm; for example, **`galactel.com`**
   - **Enable Subscription** — Allow the MPE device to receive subscription notifications as changes are implemented to the Quota and Entity state. This function manages dynamic profile changes. The data is returned in one XML response. If this option is disabled, separate lookups are used.
3. **Unique Name** --- Provide the MPE device with a specific name for organizational purposes.
   - **Use Notif-Eff** — Enable reads of multiple user data blocks (subscriber, quota, and entity state).
4. **Sh Profile**:
   - **ProfileV1** (the default) — third-party HSS
   - **ProfileV2** — HSS/Sh (7.5 or earlier version)
   - **ProfileV3** — SPR (8.0 or later version)
   - **ProfileV4** — Oracle Communications User Data Repository-Base
5. **Protocol Timer Profile**—select a protocol timer profile. For information on creating Protocol Timers, see *Managing Protocol Timer Profiles*.
6. **Transport** --- Provides the transport mode for the MPE device.

Option	Description
TCP	Indicates whether the Sh data source can support TCP protocol. If checked, an MPE device can communicate with the Sh data source in TCP. Select range 1-8 (default is "1").
SCTP	Indicates whether the Sh data source can support SCTP protocol. If checked, an MPE device can communicate with the Sh data source in SCTP. Select range 1-8 (default is "8") for both **Max Incoming Streams** and **Max Outgoing Streams**.

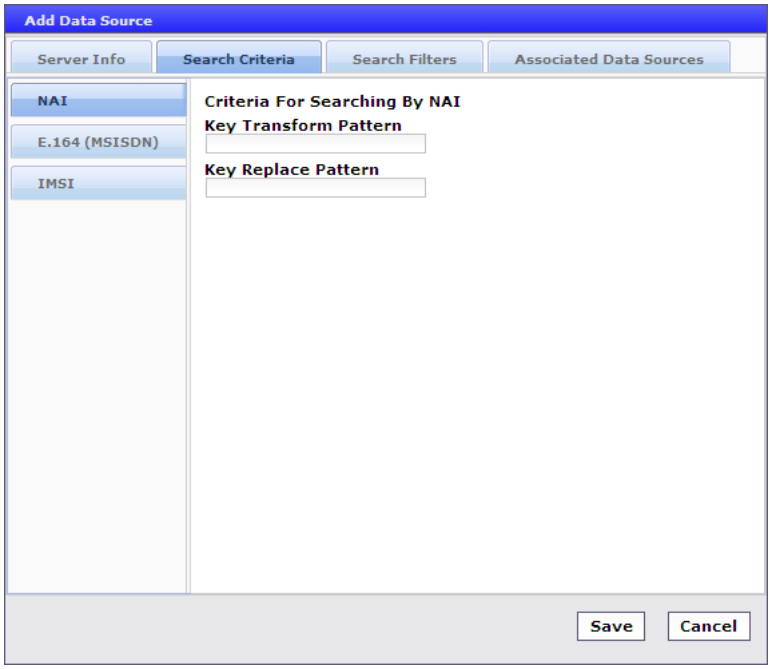


7. **Primary Servers**:
   a) **Primary Identity** — Primary server host name.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary server.
   c) **Primary Port** — Primary server port number.
      The default port number is 3868.
   d) **Secondary Identity** — Secondary server host name.
   e) **Secondary Address** — IP address, in IPv4 or IPv6 format, of the secondary server.
   f) **Secondary Port** — Secondary server port number.
      The default port number is 3868.
8. **Backup Servers**:
   a) **Primary Identity** — Primary backup server name.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary backup server.
   c) **Primary Port** — Primary backup server port number.
      The default port number is 3868.
   d) **Secondary Identity** — Secondary backup server name.
   e) **Secondary Address** — IP address, in IPv4 or IPv6 format, of the secondary backup server.
   f) **Secondary Port** — Secondary backup server port number.
      The default port number is 3868.
   g) **OAM IP** — The SPR feature queries and edits data from the Sh data source via RESTful API.
9. When you finish, click **Save** (or **Cancel** to discard your changes).

The Sh data source is configured.

Search Criteria Tab

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

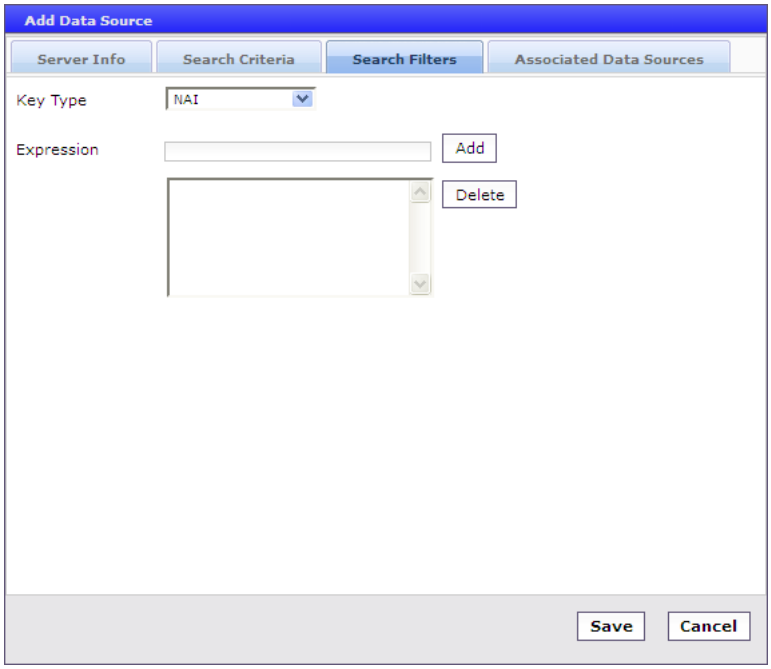


1. Select how the database is indexed:
   - **NAI** — The database is indexed by NAI (network access ID).
   - **E.164 (MSISDN)** — The database is indexed by E.164 (E.164 phone number).
   - **IMSI** —The database is indexed by International Mobile Subscriber Identity.
2. **Key Transform Pattern** — Regular expression (regex) pattern to use to transform a key.
3. **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.
4. When you finish, click **Save** (or **Cancel** to abandon your changes).

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** (the 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

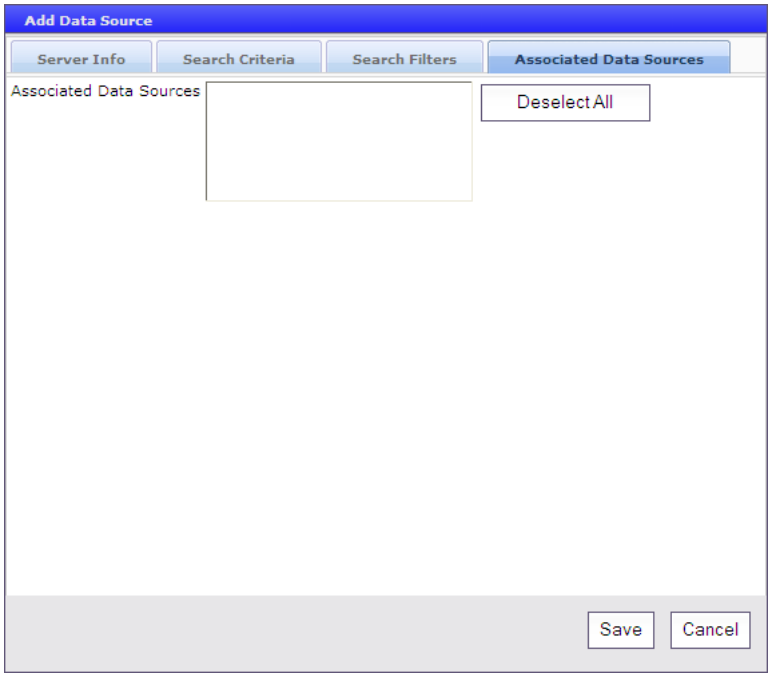
   To add the expression to the list, click **Add**. To remove an expression from the list, select it in the list and click **Delete**.
3. When you finish, click **Save** (or **Cancel** to discard your changes).

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 source(s) to associate with this Sh data source.

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

2. When you finish, click **Save** (or **Cancel** to discard your changes).

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 the *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 then the request is sent to the secondary connection. If the primary and secondary connections are unavailable then the request is sent to the tertiary server. Connections are used in order always defaulting to the highest server available. As soon as a higher connection is available, requests resume on that connection.

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

You can specify settings that apply to all Sy data sources. See *Configuring Data Source Interfaces* for more information.

Server Info Tab

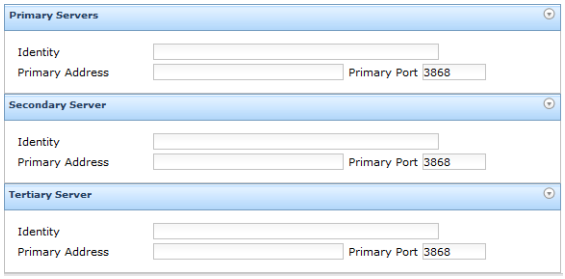
On the **Server Info** tab, enter the following:

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

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

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

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



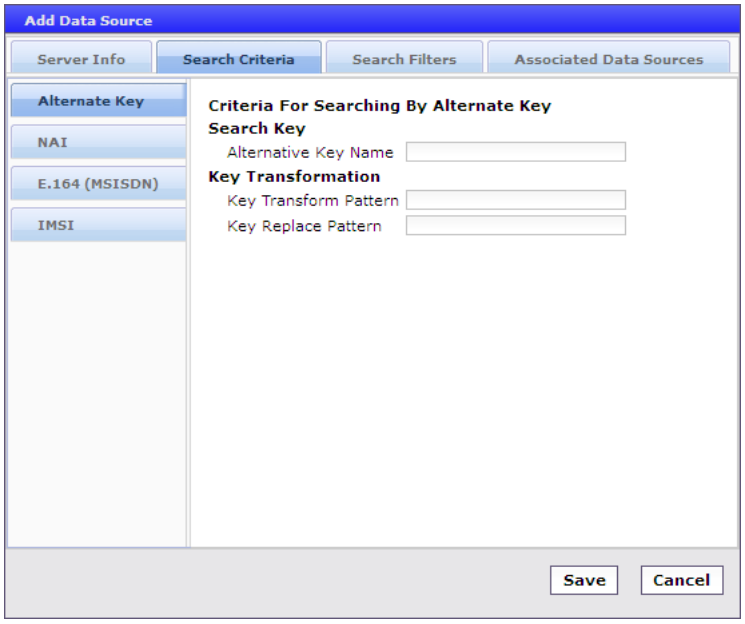
2. **Primary Server**:
   a) **Identity** (required) — Fully qualified domain name (FQDN) of the primary server.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary server. If omitted, the primary identity is used to look up the server address.
   c) **Primary Port** — Primary 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. When you finish, click **Save** (or **Cancel** to discard your changes).

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** (the 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.

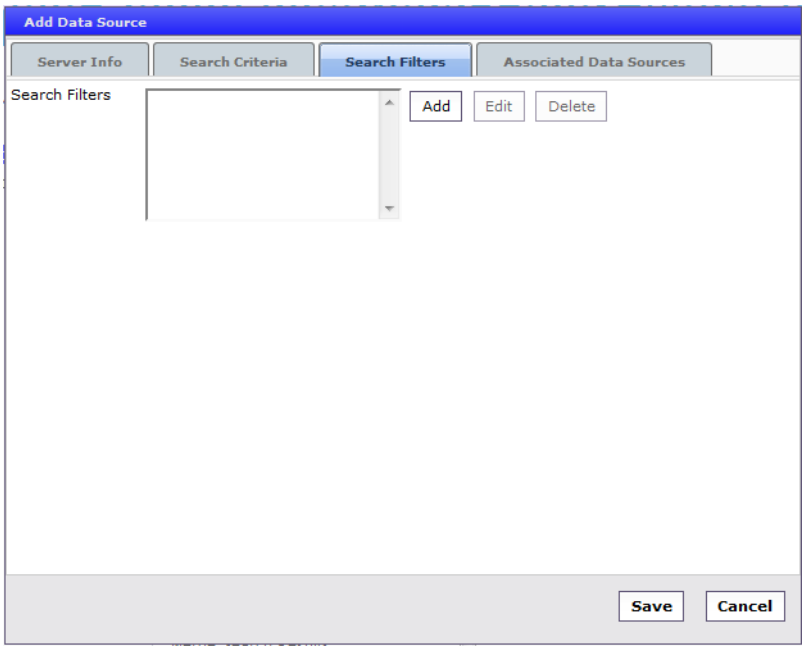
4. When you finish, click **Save** (or **Cancel** to abandon your changes).

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** (the 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. When you finish, click **Save** (or **Cancel** to discard your changes).
   The filter is added to the filters list. To remove an expression from the list, select it and click **Delete**.

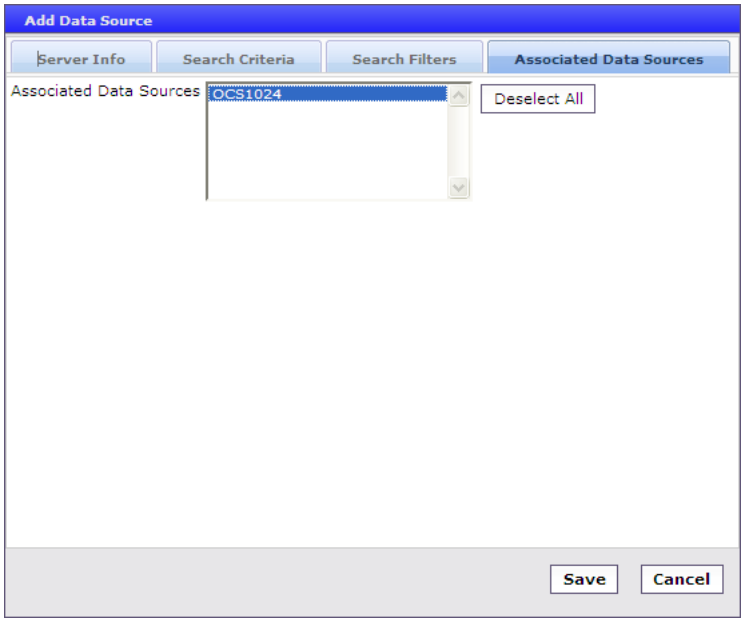
The Sy data source filters are defined.

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



1. **Associated Data Sources** — Displays a list of defined data sources. Select the data source(s) to associate with this Sy data source.
   Select **Deselect All** if you want to deselect your choices.
2. When you finish, click **Save** (or **Cancel** to discard your changes).

The associated data sources are defined.

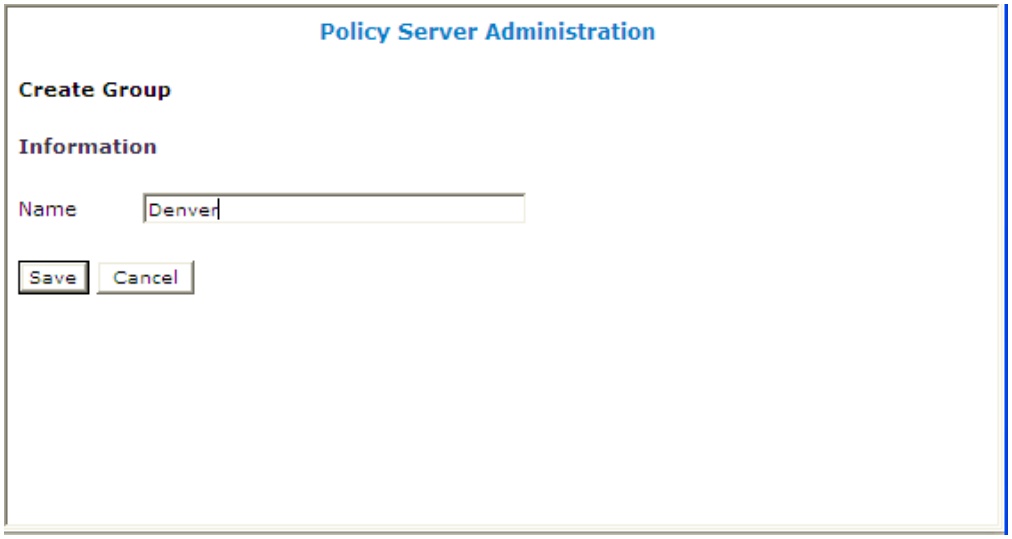
Working with Policy Server Groups

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. On the Policy Server Administration page, 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. When you finish, click **Save** (or **Cancel** to discard your changes).
   The new group appears in the content tree.

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. On the **Policy Server Administration** page, 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; use Ctrl or Shift-Ctrl to select multiple policy servers.
5. When you finish, click **Save** (or **Cancel** to cancel the request).

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. On the **Policy Server Administration** page, 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. When you finish, click **Save** (or **Cancel** to discard your changes).
   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. On the **Policy Server Administration** page, 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. When you finish, click **Save** (or **Cancel** to cancel the request).
   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 (scissors) 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. Click the **System** tab. 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**.
   You are prompted, "Are you sure you want to delete this Group?"
4. Click **OK** to delete the group (or **Cancel** to cancel the request).

The policy group is deleted.

Reapplying the Configuration to Policy Management Devices

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 server(s) with topology information, ensuring that the configuration matches the data in the CMP system. This action is not needed during normal operation but is useful in the following situations:

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

To reapply the configuration associated with an MPE device:

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.
   - To reapply the configuration to a single device continue with the next step.
   - To reapply the configuration to a group, go to step *Step 6*

   The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. To reapply the configuration to a single device continue with the next step.
3. From the content tree, select the **ALL** group.
   The **Policy Server Administration** page opens in the work area.
4. From the group **ALL**, select the MPE device.
   The **Policy Server Administration** page opens to the **System** tab, displaying information for that device.
5. Click **Reapply Configuration**.
   The profile information is saved to the MPE device.
6. From the content tree, select the group.
   The appropriate **Administration** page opens in the work area.
7. From the **Operations** menu, select **Reapply Config**.
   The **Bulk Reapply Config** dialog displays stating the number of servers affected.
8. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.
9. Click **Reapply Config** to reapply the configuration (or click **Cancel** to cancel your changes).

   To reapply the configuration to another device or group, return to the beginning of this procedure.

The individual server or all of the servers in a group are synchronized with the CMP system.

Resetting Counters

The **Reset Counters** option is included in the **Operations** menu when the **Stats Reset Configuration** option is set to **Interval**. The **Reset All Counters** option is included in the **Operations** menu when the **Stats Reset Configuration option** is set to **Manual**. See *Setting Stats Settings* for more information.

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

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the group that contains the servers of interest.
   The **Policy Server Administration** page opens in the work area.
3. From the **Operations** menu, select **Reset Counters** or **Reset All Counters**.
   The **Bulk Reset All Counters** or **Bulk Reset Counters** dialog displays showing the number of servers affected.
4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.

The counters are reset.

Enabling or Disabling All Sh Connections

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

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

To manually disable or enable all Sh connections:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the group that contains the servers of interest.
   The **Policy Server Administration** page opens in the work area.
3. From the **Operations** menu, select **Enable Sh** or **Disable Sh**.
   The **Bulk Enable Sh** or **Bulk Disable Sh** dialog displays stating the number of servers affected.
4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.
5. Click **Enable Sh** or **Disable Sh** to perform the action (or **Cancel** to cancel the action).

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

Checking the Status of an MPE Server

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

- **Group View** — Select **ALL** from the policy server content tree to view all the defined MPE servers, or select a specific policy server group or sub-group to view just the servers associated with that group. The display in the work area includes a status column that indicates the following states:
  - **On-line** — The servers in the cluster have completed startup, and their database services are synchronized.

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

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

- **Out of Service** — Communication to the cluster has been lost.
- **No Data:** Communication to the cluster has been lost. This status value provides backward compatibility with previous Policy Management releases. It can be observed during the upgrade process.
- **Config Mismatch** — The MPE device configuration does not match the CMP database.

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

Figure 21: Group View shows an example of a Group View in which one of the servers is degraded.

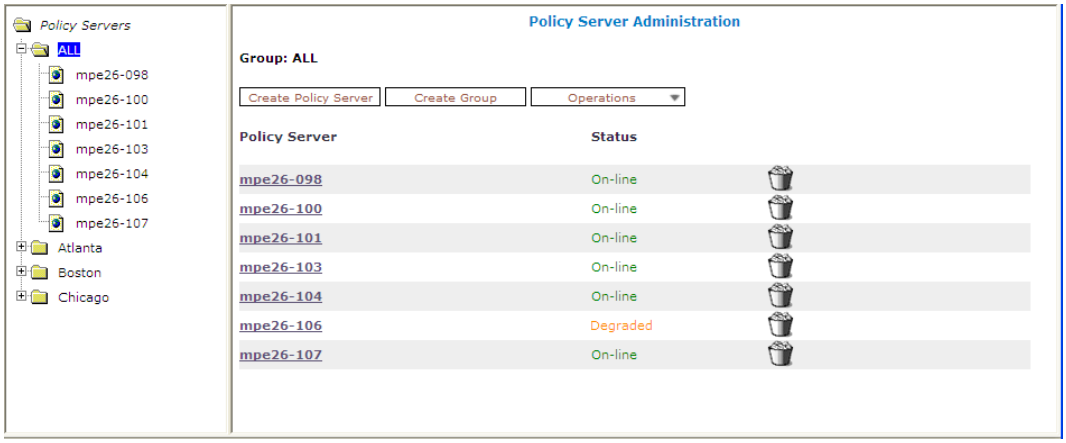


Figure 21: Group View

- **Trash can icon** — Click (trash can) 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 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 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" under Network Elements).
- **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 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.
- **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 filesystem), average value for the CPU utilization, and memory.

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

Time Period

The Time Period section shows the current time period for the cluster ("none" if 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 transitioned to any time periods.
- **Transitioning** — The cluster is updating sessions based on a time period's transition.
- **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.

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 finishing.
- **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** — 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, and >250.

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 Expert Settings*.

The following statistics are included:

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

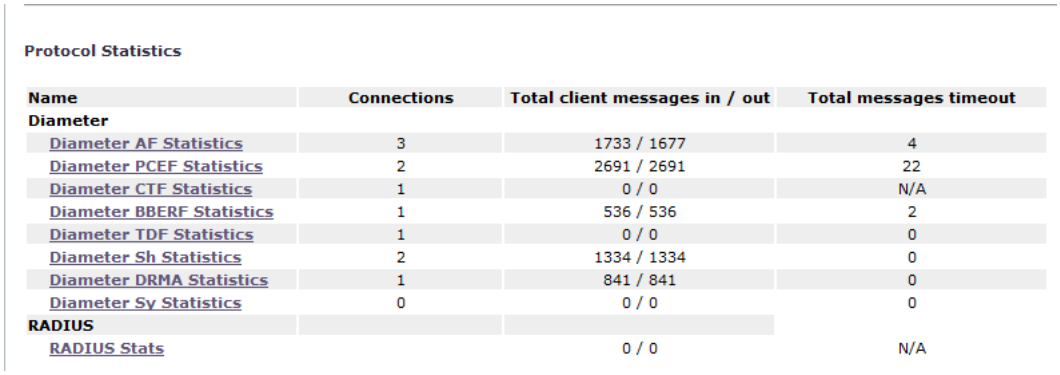
Protocol Statistics

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, 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 22: 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 22: 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 resampling from the newly active primary server. Therefore, when an MPE device is brought on line, or after a failover, one or more sample periods will display no statistical information.
2. Historical network element statistical data is inaccurate if configuration values (such as capacity) were changed in the interim. If the network element was renamed in the interim, no historical data is returned.

For example, the DRMA statistics are 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.

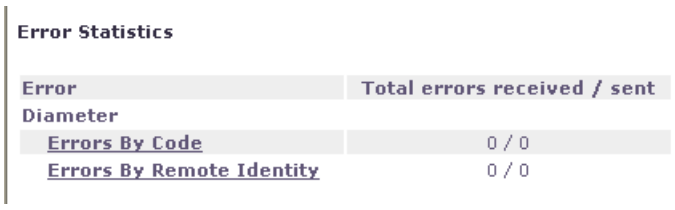
Event Trigger Statistics

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 23: 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 23: 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**
- **Number of unsubscription errors that triggered 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**

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.

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.

   Log information, including the log levels, is displayed. Refer to example for *Figure 24: Policy Server Administration, Logs Tab - Wireless*. You can configure the following logs:

   - **Trace log** — Records application-level notifications.
   - **Policy Log Settings** — Records the policy-level messages.
   - **Policy Syslog** — Records policy-processing activity. Supports the standard UNIX logging system, in conformance with RFC 3164.
   - **SMS log** — Contains all Short Messaging Service messages sent by the MPE device as well as any ACK messages received from an SMS Center (SMSC) server or its equivalent
   - **SMS log** — Contains all Short Message Peer-to-Peer Protocol (SMPP) notification 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.

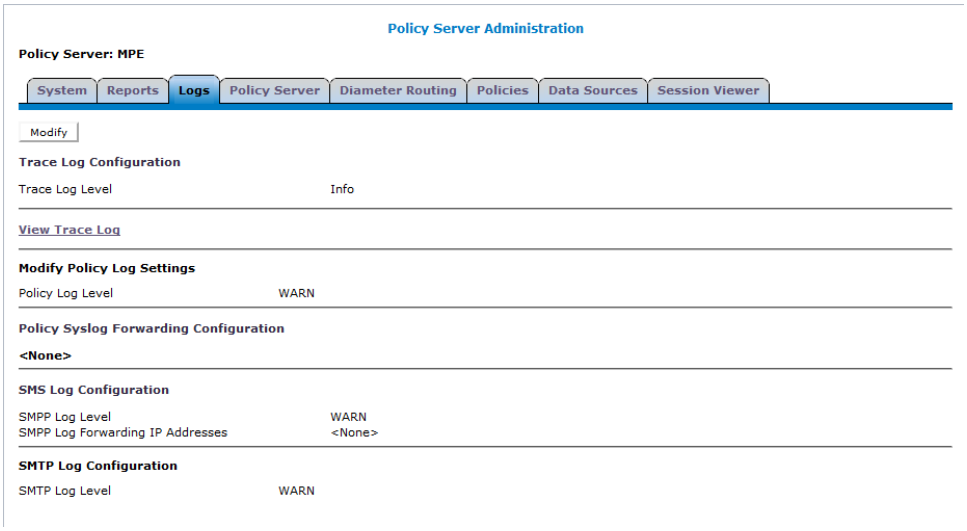


Figure 24: Policy Server Administration, Logs Tab - Wireless

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 log to debug problems by tracing through application-level messages. You can configure the severity of messages that are recorded in the trace log.

Note: Prior to V7.5, the trace log was called the event log, which also contained platform events. Platform and connectivity events are now displayed as alarms. Additionally, prior to V7.5, a policy log file recorded the activity of the Policy Rules Engine, at seven levels: Alert, Critical, Error, Warning, Notice, Info, and Debug. This information is now recorded in the trace log, which is a database table, at eight levels: Emergency (ID 4560), Alert (ID 4561), Critical (4562), Error (ID 4563), Warning (ID 4564), Notice (ID 4565) Info (ID 4566), and Debug (4567).

To view log information using the Trace Log Viewer:

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

   The **Trace Log Viewer** window opens. While data is being retrieved, the in-progress message "Scanning Trace Logs" appears.

   All events contain the following information:

- **Date/Time** — Event timestamp. This time is relative to the server time.
- **Code** — The event code. For information about event codes and messages, see the *Troubleshooting 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 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 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 Code(s)** — 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 appear.

     Note: The **Start Date/Time** setting overrides the **Contains** setting. For example, if you search for events happening this month, and search for a string that appeared in events last month and this month, only results from this month appear.

   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 any of the following:

- **Show Most Recent** — Applies filter settings and refreshes the display. This displays the most recent log entries that fit the filtering criteria.
- **Next/Prev** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.
- **First/Last** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.

When you are finished viewing the trace log, click **Close**.

Syslog Support

Notifications generated by policy actions are sent to the standard UNIX syslog. No other notifications are forwarded to syslog. For information on policy actions, see the *Policy Wizard Reference*.

Note: This feature is separate from TPD syslog support.

You can define multiple destinations for notifications, and filter notifications by severity level. For more information, see *Configuring Log Settings*.

The SMS Log

The SMS log, **`/var/Camiant/log/smsr.log`**, contains all Short Message Service (SMS) messages sent by the MPE device as well as any ACK messages received from an SMS Center (SMSC) server or its equivalent. You can configure the severity as well as the destination IP address(es) of messages that are written to the SMS log.

The SMPP Log

The SMPP log is a policy action-generated notification that contains all Short Message Peer-to-Peer Protocol notifications sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server. In SMPP or XML mode, SMPP info appears on the **Logs** tab of the **Policy Server Administration** page, under the **Policy Server: Configuration: MPE** menu. Using the **Modify** button, you can configure the severity of messages that are written to the SMPP log and set a forwarding address.

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, SMTP log info appears on the **Logs** tab of the **Policy Server Administration** page, under the **Policy Server: Configuration: MPE** menu. Using the **Modify** button, you can configure the severity of messages that are written to the SMTP log.

Configuring Log Settings

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

1. From the **Logs** tab, click **Modify**.
   The editable fields open 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** (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: 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 could cause you to miss important notifications.

3. 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** (the default) — Only messages designating potentially harmful situations are recorded.

4. In the **Modify Policy Syslog Forwarding Settings** section of the page, configure the syslog forwarding settings. You can direct notifications to up to five remote systems. For each system, enter the following:

   a) **Hostname/IP Addresses** — Remote system hostname or IP or address.

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

   b) **Facility** — Select from Local0 (the 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** (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.

5. In the **Modify SMS Log Settings** section of the page (which only appears when in SMPP mode), 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** (the 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.

6. In the **Modify SMTP Log Settings** section of the page (which only appears when in SMPP mode), 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. 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** (the 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.

7. When you finish, click **Save** (or **Cancel** to discard your changes).

The log configurations are changed.

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 the *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 (MOS). 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 Protocol Options on the Policy Server*) or policies or policy groups (see the *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:

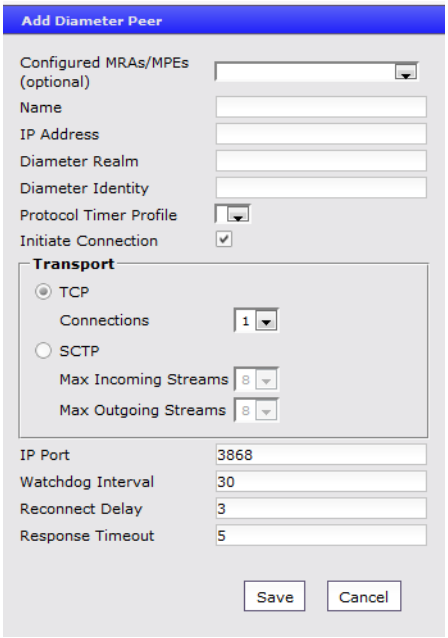
- Diameter applications: Rx, Gq, Ty, Gxx, Gx, Gy, and Sd

Configuring Diameter Peers

Policy Management devices 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 GSSN can establish a session with an MPE device using a Diameter Gx CCR (Credit Control Request) message. The MPE device responds to the request with a Gx CCA (Credit Control Answer) message.

To configure Diameter peers:

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 MPE device.
   The **Policy Server Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Peers**. The **Modify the Diameter Peer Table** page opens. The functions available from this table are as follows:
   - **To add a peer to the table** — Click **Add**; the **Add Diameter Peer** window opens:



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, **`galactel.com`**).
- **Diameter Identity** (required) — Fully qualified domain name (FQDN) of the peer device (for example, **`mpe33.galactel.com`**).
- **Protocol Timer Profie** -- Select from the pulldown menu.
- **Transport** -- Either **TCP** or **SCTP** (shown as Transport Info), for TCP select **Connections** (range 1-8, default 1) or for SCTP the **Max Incoming Streams** and **Max Outgoing Streams**(1-8 connections, default is 8) which will be shown as Connection Info.
- **IP Port** -- Enter the IP Port number.
- **Watchdog Interval** -- Enter in seconds. The default is 30 seconds.
- **Reconnect Delay** -- Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout** -- Enter the interval is seconds. The default is 5 seconds.

When you finish, click **Save** (or **Cancel** to discard your changes).

- **To clone a peer in the table** — Select an existing peer in the table and click **Clone**; the Clone **Diameter Peer** window opens with the information for the peer device. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To edit a peer in the table** — Select an existing peer in the table and click **Edit**; the **Edit Diameter Peer** window opens with the information for the peer device. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To delete a peer from the table** — Select an existing peer in the table and click **Delete**; you are prompted, "Are you sure you want to delete the selected Diameter Peer(s)?" Click **Delete** (or **Cancel** to cancel your request). The peer entry is removed.

5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Diameter peer is added to the table.

You have defined a Diameter peer.

Configuring Diameter 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.

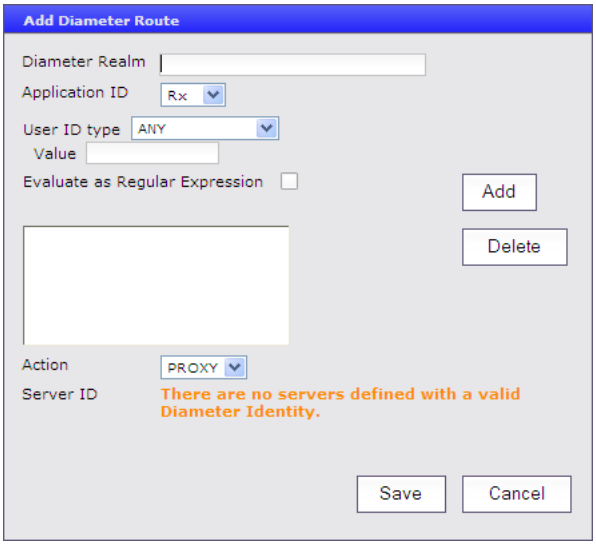
To configure the **Diameter route** table:

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 server.
   The **Policy Server Administration** page opens in the work area.
3. On the **Policy Server Administration** page, select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Routes**.

   The **Modify the Diameter Route Table** page opens.

The functions available from this table are as follows:

- **To add a route to the table** — Click **Add**; the **Add Diameter Route** window opens:



  The fields are as follows:

  - **Diameter Realm** — For example, **`galactel.com`**.
  - **Application ID** — Select **Rx** (the default), **Gq**, **Ty**, **Gx**, **Gy**, **Gxx**, **Sh**, **Sy**, or **All**.

    Note: You can include only one application per route rule. For multiple applications, create multiple rules.

  - **User ID type** — Select **ANY** (the default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
  - **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use an asterisk (*) as a wildcard character. To add the user ID to the list, click **Add**; to remove one or more user IDs from the list, select them and click **Delete**.
  - **Evaluate as Regular Expression** — The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards.
  - **Action** — Select **PROXY** (stateful route, the default), **RELAY** (stateless route), or **LOCAL** (process on this device).
  - **Server ID** — Select a destination peer from the list.

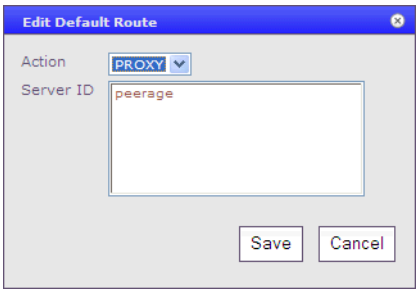
    Note: You can define a server with a Diameter identity.

  When you finish, click **Save** (or **Cancel** to abandon your changes).

- **To change the order of a route in the table** — Select an existing route in the table and click **Up** or **Down**. The order of routes is changed.
- **To clone a route in the table** — Select an existing route in the table and click **Clone**; the **Clone Diameter Route** window opens with that route's information filled in. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To edit a route in the table** — Select an existing route in the table and click **Edit**; the **Edit Diameter Route** window opens with that route's information. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).

- **To delete a route from the table** — Select one or more existing routes and click **Delete**; you are prompted, "Are you sure you want to delete the selected Diameter Route(s)?" Click **Delete** (or **Cancel** to cancel your request). The route entry is removed.

5. To define the default route, click **Edit** in the **Default Route** section.
   The Edit Default Route window opens:



   Enter the default action (**PROXY**, **RELAY**, or **LOCAL**) and peer server ID. When you finish, click **Save** (or **Cancel** to discard your changes).

6. To delete the default route, click **Delete**.
7. When you finish, click **Save** (or **Cancel** to discard your changes).

The Diameter routes are configured.

Chapter 6

Configuring Advanced Device Settings

Topics:

Configuring Advanced Device Settings describes how to configure and manage expert settings, service overrides, and load shedding options.

Configuring Expert Settings

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

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the device.
   - For an MPE device, select the **Policy Server** tab.
   - For an MRA device, select the **MRA** tab.

   The configuration settings for the device display.
3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Modify**.
   The advanced configuration settings can be edited.
5. Select a configuration key in the **Expert Settings** table and click **Edit**.
   The **Edit Expert Setting Value** dialog opens.
6. Modify the settings and click **OK** to save (or **Cancel** to abort the request). See *Table 5: Expert Settings for MPE* and for information about the configurations keys.

Table 5: Expert Settings for MPE

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

Category	Configuration Key	Description	Default
		AF session can be considered stale and purged. Specified in seconds. Valid range is 0-86400.	
Diameter	DIAMETER.AF.MinAuthLifetime	The minimum lifetime of an AF session. Otherwise the corresponding AF session would be purged subject to the configured grace period. Specified in seconds.	300
Diameter	DIAMETER.Cleanup.AuditRxSessions	If enabled, an RAR message is sent for auditing. **This is for future releases and has not been implemented yet.**	False
Diameter	DIAMETER.Cleanup.AuditSySendEmptyPolicyCounterList	If enabled, the Policy Counter Identifier subscription list is not sent as part of an SLR (INTERMEDIATE) message to audit stale Sy sessions. If disabled, the current Policy Counter Identifier subscription list is sent as part of an SLR (INTERMEDIATE) message to audit stale Sy sessions.	True
Diameter	DIAMETER.Cleanup.AuditSySessions	If enabled, an SLR (INTERMEDIATE) message is sent for auditing. If disabled, the Sy session is checked for an association with an IP-CAN session. If there are no IP-CAn associations, the Sy session is considered active; otherwise, the session is deleted. **This is for future releases and has not been implemented yet.**	False
Diameter	DIAMETER.Cleanup.CleanupStaleRxSessions	Determines if the MPE should consider AF sessions in the regular cleanup cycles. If enabled, AF sessions are considered expired if they have lived longer than the specified AFSessionValidityTime. **At that point, in future releases, if AuditAFSessions is set to true, an RAR will be sent for auditing the session.**	True
Diameter	DIAMETER.Cleanup.MaxDurationForSessionIteration	The maximum duration in seconds to iterate through the sessions. Valid range is 1-86400.	7200 (2 hours)
Diameter	DIAMETER.Cleanup.MaxSessionCleanupRate	The rate (in sessions/sec) at which the cleanup task attempts to clean stale sessions.Valid range is 1- 5000.	50
Diameter	DIAMETER.Cleanup.MaxSessionIterationRate	The rate (in sessions/sec) at which the cleanup task iterates through the sessions database. Valid range is 1-100000.	1000

Category	Configuration Key	Description	Default
Diameter	DIAMETERDRA.Cleanup.MaxSessionValidityTime	The maximum amount of time in seconds after which the session is cleaned up on any error. Specified in seconds. Valid range is 1-8640000.	172800 (2 days)
Diameter	DIAMETER.Cleanup.MaxSySessionValidityTime	The maximum amount of time in seconds after which the Sy session is cleaned up on any error.	172800 (2 days)
Diameter	DIAMETER.Cleanup.OverrideCleanupAudit	This specifies if the regular audit processing for cleaning up a stale session is overridden. When enabled, the cleanup task bypasses the audit process and deletes all sessions that are stale for the session validity time.	False
Diameter	DIAMETER.Cleanup.RXSessionValidityTime	The amount of time (in seconds) after which the session is expired and is purged if EnabledAFSessionCLeanup is enabled.	86400 (1 day)
Diameter	DIAMETER.Cleanup.SessionCleanupInterval	The amount of time (in seconds) after which the cleanup task will run to look for stale sessions.	21600 (5 hours)
Diameter	DIAMETER.Cleanup.SessionCleanupStartTime	Schedules the cleanup task once a day at a specified time. If the start time is specified, then it is scheduled to run once a day at the given time. The value can be specified in either a 24-hr format (HH:mm) or an exact date and time (YYYY-MM-ddThh:mm:ss) of when it will first run and then repeat at the interval specified.	undefined
Diameter	DIAMETERDRA.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Specified in seconds. Valid range is 1- 8640000.	432000 (5 days)
Diameter	DIAMETER.Cleanup.SySessionValidityTime	The amount of time (in seconds) after which the session is declared stale and deemed a candidate for cleanup.	36000 (10 hours)
Diameter	DIAMETER.EnableSessionCleanUp	Enables the DiameterSessionCleanUp Task.	True
PCMM	PCMM.Cleanup.CleanupStalePcmmSessions	Enables the inclusion of PCMM sessions in regular cleanup cycles. If enabled, PCMM sessions are considered expired if they have lived longer than the specified PcmmSessionValidityTime or license timeout duration configured in the application.	

Category	Configuration Key	Description	Default
PCMM	PCMM.Cleanup.PcmmSessionValidityTime	The amount of time (in seconds) after which the session is deemed expired and is purged if EnabledAFSessionCLeanup is enabled.	86400 (1 day)

Table 6: Expert Settings for MRA

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

Category	Configuration Key	Description	Default
		stale bindings. Valid range is 1-40000.	
Diameter	DIAMETERDRA.Cleanup.MaxBindingIterationRate	The rate (in bindings/sec) at which the cleanup task iterates through the binding database. Valid range is 1-100000.	1000
Diameter	DIAMETERDRA.Cleanup.MaxDurationForBindingIteration	The maximum duration in seconds to iterate through the bindings. Valid range is 1-2147483647.	21600 (5 hours)
Diameter	DIAMETERDRA.Cleanup.MaxSessionValidityTime	The maximum amount of time in seconds after which the session is cleaned up on any error. Specified in seconds. Valid range is 1-8640000.	864000 (10 days)
Diameter	DIAMETERDRA.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Specified in seconds. Valid range is 1- 8640000.	432000 (5 days)
Diameter	DIAMETERDRA.StaticMigrationModeEnabled	Enables the static to stateful MRA migration mode. While in this mode, static routes are used for MPE selection only.	False

7. When finished making changes, click **Save** (or **Cancel** to discard changes).
   The settings are applied to the selected device.

Configuring Service Overrides

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

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

Make service override changes as follows:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the device.
   - For an MPE device, select the **Policy Server** tab.
   - For an MRA device, select the **MRA** tab.

The configuration settings for the device display.

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

   - **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)
     - **Comments**—Information about the key.

     When you finish, click **OK** (or **Cancel** to discard your changes). 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. When you finish, click **Save** (or **Cancel** to discard your changes).
   - **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. When you finish, click **Save** (or **Cancel** to discard your changes).
   - **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 (or **Cancel** to cancel your request).

6. When finished making changes, click **Save** (or **Cancel** to discard your changes).
   The settings are applied to the selected 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 7: Default Device Busyness Level 1

Rule Name	Actions
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

Table 8: Default Device Busyness Level 2

Rule Name	Actions
DefaultRule4	Reject Gx CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule5	Reject Gxx CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule6	Reject Gy CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule7	Reject Rx AAR-I messages with DIAMETER_TOO_BUSY

Table 9: Default Device Busyness Level 1

Rule Name	Actions
DefaultRule8	Reject Gx CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule9	Reject Gxx CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule10	Reject Gy CCR-I messages with DIAMETER_TOO_BUSY
DefaultRule11	Reject Rx AAR-I messages with DIAMETER_TOO_BUSY
DefaultRule12	Reject Sh PNR messages with DIAMETER_TOO_BUSY
DefaultRule13	Reject Sy SNR 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 MOS for assistance.

Configure the load shedding rules as follows:

1. View the device list.

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

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

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

   The configuration settings for the device display.
3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Modify**.
   The advanced configuration settings can be edited.
5. In the **Load Shedding Configuration** section of the page, select the enabled state.
   - **true** (default)—Enables load shedding.
   - **false**—Disables load shedding.
   - **undefined**— The value for this field is taken from the associated Configuration Template. If there is not a configuration template associated, then the default value is used.
6. Configure the rules for the busyness levels:
   a) Click ▶ (right arrow) next to the level to expand the level.
   b) Click **Add** and select the category.
      The **Add Load Shedding Rule** dialog appears.
   c) Enter the values for the load shedding rule:
      - **Name** — Name of the rule.
      - **Application** — Select the application the rule applies to. You can select **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** (or **Cancel** to discard your changes).
      The rule is displayed in the table.
7. Once a rule is defined, you can clone, edit, or delete it by selecting the rule and clicking the appropriate button.
8. When finished making changes, click **Save** (or **Cancel** to discard your changes).

The settings are applied to the selected device.

Resetting Configuration Keys to Defaults

All the configuration keys in the Expert Settings table can be reset to the defaults. The configuration keys in the Service Overrides table cannot be reset.

To reset the configuration keys in the Expert Settings table:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the device.
   - For an MPE device, select the **Policy Server** tab.
   - For an MRA device, select the **MRA** tab.

   The configuration settings for the device display.
3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Modify**.
   The advanced configuration settings can be edited.
5. Click  **Set to Default**.
   A confirmation message displays.
6. Click **OK** (or **Cancel** to abandon the request).
   All the configuration keys for Expert Settings are set to default values.

Filtering the Configuration Keys

To limit the number of configuration keys in the Expert Settings or Service Overrides tables, use the filter option.

To filter the configuration key table:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the device.
   - For an MPE device, select the **Policy Server** tab.
   - For an MRA device, select the **MRA** tab.

   The configuration settings for the device display.

3. Click **Advanced**.
   The advanced settings for the device display.
4. (Optional) Click **Modify**.
   The advanced configuration settings can be edited.
5. Click **Filters** to open the filtering popup.
   The filtering popup opens.
6. Specify the filtering parameters using any of the following fields.

Option	Description
Change Status	The change status of the configuration key. • **All** (default)—All keys are listed. • **Changed**—Lists the configuration keys that have been modified from the default setting. • **Unchanged**—Lists the configuration keys that have not been modified from the default setting.
Category	The category for the configuration key.
Configuration Key	Enter all or part of a configuration key name.

7. Click **Filter Result**.
   The filtered list of configuration keys displays.

Exporting the Configuration Keys

The expert Settings or Service Overrides configuration keys can be exported to a comma delimited list (CSV) or to a printable version.

To export the configuration key table:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the device.
   - For an MPE device, select the **Policy Server** tab.
   - For an MRA device, select the **MRA** tab.

   The configuration settings for the device display.
3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Export**.
   The export list opens.
5. Select the export type.

Option	Description
Save as CSV	A comma-separated value (CSV) file named `CSV_report.csv` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
Printable Format	The configuration key list displays in a separate window for printing.

Chapter 7

Managing Protocol Timer Profiles

Topics:

Managing Protocol Timer Profiles describes how to define and manage protocol timer profiles within the CMP system.

A protocol timer profile configures the Diameter response timeout values for specific applications and the different message types within an application.

About Protocol Timer Profiles

A Protocol Timer profile contains the configuration of Diameter response timeout values for specific applications and message types within an application. A Protocol Timer profile is associated at both the global level for an MPE or MRA, as well as for a specific diameter peer. For example, a peer with the identity of **`ggsn.realm.com`** can have a response timeout of 4500ms for an RAR message sent over Gx from the MPE. You can also configure the maximum amount of time a received Diameter request can be processed by the MPE or MRA. If an answer is not generated within the configured amount of time, then the request is discarded. This value is global to the entire MPE or MRA. The values allow for a granularity of a tenth of a second. A timer configured at the peer level takes precedence over a value configured at the global level.

Profile can be associated with any MPE, MRA, pooled MPE, backup MRA, associated MRA, Diameter peer, network element, or data source (Sh and Sy). Any profile associated with a MPE or MRA is considered the global timer profile for that element. Therefore, each MPE or MRA has only one global timer profile.

In the deployment of an MRA, it is possible that both the MRA and MPE could have the same network elements associated with them through the CMP. In this case, the Protocol Timer profile configured for the network element would only apply to the MRA since the MRA is the only one with direct connections to the network elements. The MPE would be directly communicating with the MRA and therefore the values configured in the global timer profile for the MPE would apply. Specific values for a peer level profile pertaining to the MPE to MRA communication can be defined by adding the MRA to the diameter peer table for the MPE. See the *Policy Front End User's Guide* for more information about diameter peer tables.

The following table lists the Diameter applications and message types supported.

Table 10: Supported Diameter Applications and Messages

Application / Interface	Message
Gx	CCR, RAR
Rx	AAR, RAR, STR, ASR
S9 over S9	CCR, RAR
Rx over S9	AAR, RAR, ASR, STR
Sh	UDR, SNR, PNR, PUR
Sy	SLR, STR, SNR
Gy	CCR, RAR, ASR
Sd	CCR, TSR, RAR
Gxx	CCR, RAR
VZr	SDR

Viewing a Protocol Timer Profile

To view a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
   The content tree displays the **Protocol Timer Profiles** folder.
2. Select a profile.
   The configuration for the profile displays in the Work Area.

   You can change the view of the list using the following options.

   - When the list is expanded, click **Collapse All** to show the list of applications/interfaces only.
   - When the list is collapsed, click ▶ (right arrow) to the left of the interface/application to view the settings for an individual application/interface.
   - When the list is collapsed, click **Expand All** to show list of settings for all the applications/interfaces.
   - When the list is expanded, click ▼ (down arrow) to the left of the interface/application to close the settings view for an individual application/interface.

The Protocol Timer Profile configuration displays.

Creating a Protocol Timer Profile

A Protocol Timer Profile defines timeout values for messages in applications/interfaces.

To create a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
   The content tree displays the **Protocol Timer Profiles** folder.
2. Click **Create Protocol Timer Profile**.
   The **Protocol Timer Profile Adminstration** page opens.
3. Enter the following information:
   a) **Name** — Name of the profile. A name is subject to the following rules:
      - Is case insensitive (uppercase and lowercase are treated as the same)
      - Must be no longer than 255 characters
      - Must not contain quotation marks (") or commas (,)

   b) **Description** (optional) — Information that defines the profile.
   c) Set the timeout values. The following table lists the defaults:

      Note: The timeout value must be in a multiple of 100. For example, 4955 is not a valid value and displays a validation error.

Table 11: Supported Diameter Applications and Messages

Application / Interface	Message	Default (msec)
Gx	CCR	5000
	RAR	5000
Rx	AAR	5000
	RAR	5000
	STR	5000
	ASR	5000
Sh	UDR	3000
	SNR	3000
	PNR	3000
	PUR	3000
Sy	SLR	3000
	STR	3000
	SNR	3000
Gy	CCR	5000
	RAR	5000
	ASR	5000
Sd	CCR	5000
	TSR	5000
	RAR	5000
Gxx	CCR	5000
	RAR	5000
VZr	SDR	5000

4. When you finish, click **Save** (or **Cancel** to discard your changes).

The profile appears in the list of Protocol Timer Profiles and can be associated with any MPE, MRA, pooled MPE, backup MRA, associated MRA, Diameter peer, network element, or data source (Sh and Sy).

Modifying a Protocol Timer Profile

A Protocol Timer Profile defines timeout values for messages in applications/interfaces.

To modify a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
   The content tree displays the **Protocol Timer Profiles** folder.
2. Select a profile.
   The configuration for the profile displays in the Work Area.

   You can change the view of the list using the following options.

   - When the list is expanded, click **Collapse All** to show the list of applications/interfaces only.
   - When the list is collapsed, click ▶ (right arrow) to the left of the interface/application to view the settings for an individual application/interface.
   - When the list is collapsed, click **Expand All** to show list of settings for all the applications/interfaces.
   - When the list is expanded, click ▼ (down arrow) to the left of the interface/application to close the settings view for an individual application/interface.
3. Click **Modify**.
   The **Protocol Timer Profile Adminstration** page opens with editable fields.
4. Modify the information.

   See *Creating a Protocol Timer Profile* for more information on the fields.

   Note: The timeout value must be in a multiple of 100. For example, 4955 is not a valid value and displays a validation error.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The profile is updated.

Deleting a Protocol Timer Profile

A Protocol Timer Profile defines timeout values for messages in applications/interfaces.

To delete a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
   The content tree displays the **Protocol Timer Profiles** folder.
2. You can delete a profile using one of the following methods.

   - Select the **Protocol Timer Profiles** folder and then click 🗑 (trash can). A confirmation message displays. Click **OK** to delete or **Cancel** to abort the process.
   - Select a profile from the **Protocol Timer Profiles** folder and then click **Delete**. A confirmation message displays. Click **OK** to delete or **Cancel** to abort the process.

The profile is updated.

Chapter 8

Managing Charging Servers

Topics:

Managing Charging Servers 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 server 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 server 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. On the **Charging Server Administration** page, 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.
      Select **tcp**, **udp**, or **sctp** from the list.
   f) **Protocol** — Specifies the AAA protocol used to communicate with the charging server.
      Select **diameter**, **radius**, or **tacacs+** from the list.

      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. When you finish, click **Save** (or **Cancel** to discard your changes).
   The charging server is displayed in the **Charging Server Administration** page.

   Once you define charging servers, you can select them as default charging servers when configuring an MPE device (see *Configuring Protocol Options on the Policy Server*) or use them in policy actions in the policy wizard (see the *Policy Wizard Reference*).

Modifying a Charging Server

To modify the definition of a charging server:

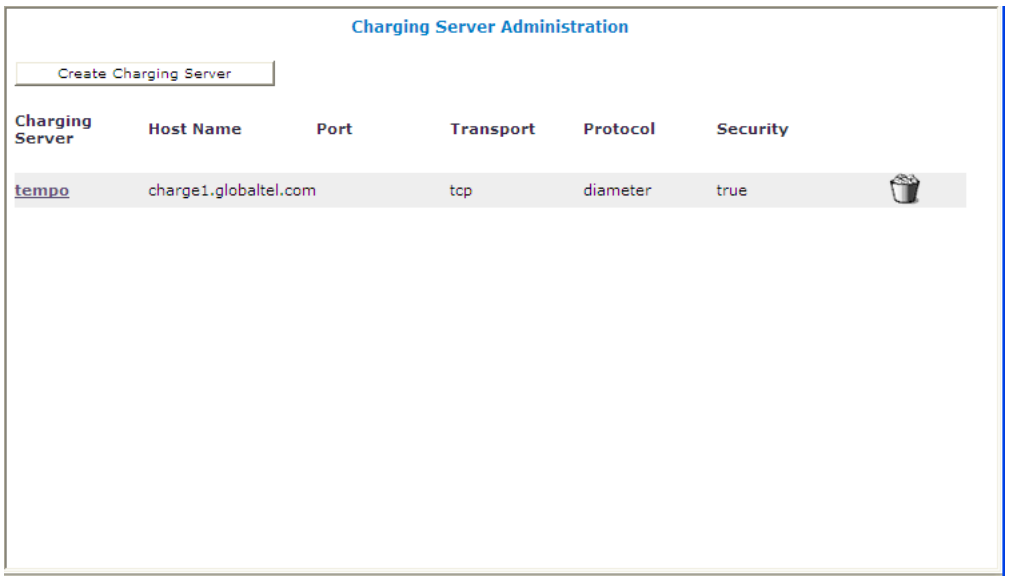
1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.
   The **Charging Server Administration** page opens in the work area, listing the defined charging servers.
2. On the **Charging Server Administration** page, select the charging server you want to modify.
   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. When you finish, click **Save** (or **Cancel** to discard your changes).

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; for example:



2. Delete the charging server using one of the following methods:

- From the work area, click the Delete icon, located to the right of the charging server you wish to delete.
- From the content tree, select the charging server and click **Delete**.

You are prompted: "Are you sure you want to delete this Charging Server?"

3. Click **OK** to delete the charging server (or **Cancel** to cancel the request).

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. On the **Policy Server Administration** page, 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 Primary Online Server, the Primary Offline Server, the Secondary Online Server, and the Secondary Offline Server from the lists.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The selected charging servers are defined as serving this MPE device.

Chapter 9

Mapping Serving Gateways to MCCs/MNCs

Topics:

Mapping Serving Gateways to MCCs/MNCs describes how to map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs) in the CMP system.

About Mapping Serving Gateways to MCCs/MNCs

An SGSN (Serving GPRS Support Node) may 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. Once 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. On the **Serving Gateway/MCC-MNC Mappings Administration** page, 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, type it and click **Add**. To remove one or more mappings from the list, select them and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

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 opens.
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. When you finish, click **Save** (or **Cancel** to abandon your changes).

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 opens.
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 the Delete icon, located to the right of the mapping you want to delete.
   - From the content tree, select the mapping and click **Delete**. You are prompted, "Are you sure you want to delete this Serving Gateway/MCC-MNC mapping?"
4. Click **OK** to delete the Serving Gateway/MCC-MNC mapping (or **Cancel** to cancel the request).

The mapping is deleted.

Chapter 10

Managing Subscriber Profile Repositories

Topics:

Managing Subscriber Profile Repositories 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 ESPR documentation.

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 may 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 (API) for XML provisioning of subscriber profile data, as well as an interactive user interface through the CMP system using a proprietary RESTful API interface.

  The SDM 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 SDM provides both a storage and notification platform for policy operations, as well as a platform for operator provisioning.

  For detailed information on the SDM, see the SDM documentation.

- The Oracle Communications User Data Repository (UDR) is a highly-scalable, consolidated database back end for subscriber and profile data. UDR 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 ESPR for creating, retrieving, modifying, and deleting subscriber and pool data.

  For detailed information on the UDR, see the UDR documentation.

- A customer specified SPR.

  See the SPR documentation for more information.

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 (MOS). 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, complete the following:

1. From the **Help** section of the navigation pane, select **About**.
   The **About** page opens, displaying the CMP software version number.
2. Click the **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 admin** page is displayed.

You are now ready to define an SPR cluster profile and manage SPR subscriber data.

Configuring the SPR Connection

You must define the operation mode and connection details for the SPR before you can look up subscriber information from the CMP system.

To configure the CMP connection to an SPR database:

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 pulldown list:
      - **SDM RESTful API** (the 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) **Enable Custom Fields for Data Entry**—Select to show the custom fields on the **Service**, **User Session Policy**, and **User Location** tabs.
   e) **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**.
   f) **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. When you finish, click **Save** (or **Cancel** to discard your changes).

The connection definition is added to the CMP database.

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. On the **SPR Connection Configuration** page, click **Modify**.
   The **Configuration** page opens.
3. Modify the configuration information as necessary. See *Configuring the SPR Connection* for information on the fields on this page.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

The SPR connection configuration is modified.

Finding a Subscriber Profile

Once you have defined SPR devices, 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)** (the 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. When you finish, click **Back to Search Page**.
   The **Subscriber Profile Administration** page opens.

Creating a Subscriber Profile

If an SPR device 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. Enter a number between 0 and 31. If you enter 0 or leave this field blank, then the default global value configured for this MPE device is used instead.
   - **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 entitlement(s). Enter the entitlement name(s); 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. Click **Add** to create additional fields as needed.

4. When you finish, click **Save** (or **Cancel** to discard your changes).

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. When you finish, click **Save** (or **Cancel** to discard your changes).
   The page displays the message "Subscriber profile updated successfully."

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. Find 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**.
   You are prompted, "Are you sure you want to delete this subscriber profile?"
4. Click **OK** to delete the subscriber profile (or **Cancel** to abandon the request).
   The page displays the message "Subscriber profile successfully deleted."

The subscriber profile is deleted.

Viewing Subscriber Entity States

Subscriber entity states are a set of name-value pairs associated with a subscriber.

To view the 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. 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. Click the **State** tab.
   Entity state information is displayed.
4. When you finish, 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. 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 **State** tab.
   Entity state information is displayed.
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** (or **Cancel** to discard your changes).
   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 wish to add more; click **Yes** to continue, or **No** to stop.
8. When you finish, 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. 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 **State** tab.
   Entity state information is displayed.
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. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The page displays the message "Properties updated successfully."

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. 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 **State** tab.
   Entity state information is displayed.
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**.
   You are prompted, "Delete selected properties?"
6. Click **OK** (or **Cancel** to abandon your request).
   The property or properties are removed from the list, and the page displays the message "Properties deleted successfully."

The subscriber entity state properties are deleted.

Viewing Subscriber Quota Information

To view the quotas associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select the subscriber profile.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on locating a subscriber profile.)
3. Select the **Quota** tab.

The **Subscriber Profile Quota Usage** page is displayed. 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. When you finish, 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. 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 **Quota** tab.
   The Quota Usage information appears in the work area.
4. Click **Create**.
   The **Quota Usage** page opens. If you exceed 10 quotas, you are prompted whether you wish to add more; click **Yes** to continue, or **No** to stop.
5. 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). When you finish, click **OK** (or **Cancel** to discard the date/time).
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.

Note: This field is an internal identifier, and you should not change it.

6. When you finish, click **Save** (or **Cancel** to discard your changes).
The page displays the message "Quota created successfully."

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. 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 **Quota** tab.
The **Subscriber Profile Quota Usage** page is displayed.
4. Click the name of the quota you want to modify.
The **Quota Usage** page opens, displaying information about the quota.
5. Modify subscriber quota information as required.
For a description of the fields contained on this page, see *Adding a Subscriber Quota Category*.
6. When you finish, click **Save** (or **Cancel** to discard your changes).
The page displays the message "Quota updated successfully."

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. 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 **Quota** tab.
   Entity quota information is displayed.
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**.
   You are prompted, "Delete selected properties?"
6. Click **OK** (or **Cancel** to abandon your request).
   The quota or quotas are removed from the list, and the page displays the message "Quota deleted successfully."

The subscriber quota categories are deleted.

Adding a Member to a Pooled Quota Group

You can add a member and associate a subscriber when creating a pooled quota group. You can include up to 20 subscribers in a pooled quota group.

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select **Create Pooled Quota Group**.
   The **New Pooled Quota Group Profile** page opens.
3. In the **Data Source Primary Diameter Identity** section of the page, select one of the configured ProfileV3 or ProfileV4 data sources.
4. In the **Key Fields** section of the page, enter the **Pool ID**.

   The pool ID is an alphanumeric string of up to 255 characters that can contain hyphens (-) and underscores (_) but no spaces. **`0`** is invalid.
5. (Optional) In the **Subscriber Information** section of the page, enter the following:
   a) **Billing Day** — The billing day of the subscriber pool. This field is used only for monthly billing.
   b) **Tier** — Enter the name of a tier defined in the CMP database; or click **Manage** to select a tier.
   c) **Entitlements** — Click **Manage** and select one or more entitlement names defined in the CMP database.
   d) **Custom 1, Custom 2, Custom 3, Custom 4, Custom 5** — Enter name value fields. You can refer to them in policies.

e) **Custom N** — If you click **Add**, you can add additional custom fields.

6. (Optional) In the **Membership Information** section of the page, to add a member or associate a subscriber to the quota, select the **Key Type** and add a **Key String**.

   Note: When associating a subscriber, you must enter the subscriber key string.

   a) **Key Type** — The type of Pool ID. Click **Add** to add a Pool ID search value. You can select one of the following:

   - **E.164 (MSISDN)**
   - **IMSI**
   - **NAI**

   b) **Key String** — Enter the key string or click **Add** to add a Pool ID search value.

7. When you finish, click **Save** (or **Cancel** to discard your changes).

The member is added to the pooled quota group.

Querying by Pool ID

You can query a new quota by specifying the Pool ID Key Type and Key String value.

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select **Pool ID** in the **Key Type** pulldown and enter a **Key String**. Click **Search**.
   The **Pool Group Quota Profile** page opens with the search results. The following tabs are displayed:

   - **Pool Profile**
   - **Pool Quota**
   - **Pool State**

3. You can select the **Modify**, **Delete**, or **Back to Search Page** options.

Creating a Pool Quota Profile

A pool quota profile can be created for the purpose of tracking and displaying usage threshold events.

To create a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
   The **Quota Usage** section displays.
5. Click **Create**.

6. Enter the following:
   a) **Name** — Select the name of the pool state.
   b) **Type** — Select the quota being assigned to the pool. You can select **quota** (plan), **pass**, **top-up**, **roll-over**, or **roll-over-def**.

      If you select **roll-over-def**, rollover units are consumed before top-up units unless the highest priority top-up expires in the next 24 hours.
   c) **Time** (seconds) — The amount of time attributed to the quota in seconds.
   d) **Total Volume** (bytes) — The amount of volume attributed to a length of time.
   e) **Upstream Volume** (bytes) — Traffic from the handset (or other device) to the network.
   f) **Downstream Volume** (bytes) — Traffic directed to the handset or other device.
   g) **Service Specific Event** — Tracks text information.
   h) **Next Reset Time** — The reset date and time of the subscriber or pool quota usage.

      Note: This is typically the billing day, although for a daily quota the usage is normally reset at midnight or shortly thereafter.

7. When you finish, click **Save** (or **Cancel** to discard your changes).

The pool quota profile is created.

Modifying a Pool Quota Profile

A pool quota profile can be modified if you want to make changes to the subscriber information or membership information.

To modify a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens with **Pool Profile** as the default.
4. Click **Pool Quota Profile**.
   The **Pool Quota Profile** view displays.
5. Select the profile that you want to modify.
6. Modify any of the fields.

   Note: The **Name** field cannot be changed.

7. When you finish, click **Save** (or **Cancel** to discard your changes).

The pool quota profile is modified.

Deleting a Pool Quota Profile

A pool quota profile can be deleted.

To delete a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.
   The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
   The Quota Usage section displays.
5. Select the name of the properties you want to delete, then click **Delete**.
   You are prompted, "Delete selected properties?"
6. Click **OK**.
   The selected properties are deleted.

Modifying a Pool Profile

A pool profile can be modified if you want to make changes to the subscriber information or membership information.

To modify a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens with Pool Profile as the default.
4. Click **Modify**.
   The **Subscriber Profile Configuration** page opens.
5. Modify any of the field information.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The pool profile is modified.

Deleting a Pool Profile

A pool profile can be deleted.

To delete a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.

The **Pool Profile** page opens with **Pool Profile** as the default.

4. Click **Delete**.
   You are prompted, "Are you sure you want to delete this pool profile?"
5. Click **OK**.

The pool profile is deleted.

Creating a Pool State

A pool state can be created when an Sh ProfileV3 or ProfileV4 data source is selected. For more information, see *Configuring Protocol Options on the Policy Server* .

To create a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens.
4. Click **Pool State**.
5. Click **Create**.
   The Create Property section is displayed.
6. Enter the following:
   - **Name** — The name of the pool state.
   - **Value** — The value can be any string; for example, **`Profile V3`**, **`V4`**.
7. When you finish, click **Save** (or **Cancel** to discard your changes).
   The **Pool Entity State Properties** section is displayed, with the Pool Quota Group Key Fields and the searched Pool ID.

The pool state is created.

Modifying a Pool State

A pool profile can be modified if you want to make changes to the subscriber information or membership information.

To modify a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens with **Pool Profile** as the default.

4. Click **Pool State**.
   The **Pool Entity State Properties** section displays.
5. Select the **Name** of the pool state that you want to modify.
   The **Modify Property** section displays.
6. The **Name** and **Value** fields are displayed. You can only modify the **Value** field.
7. Modify the **Value** field.
8. When you finish, click **Save** (or **Cancel** to discard your changes).

The pool state content is modified.

Deleting a Pool State

A pool state can be deleted.

To delete a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens.
4. Click **Pool State**.
   The **Pool Entity State Properties** section is displayed.
5. Select one or more properties to delete, then click **Delete**.

The properties are deleted.

Chapter 11

Managing Subscribers

Topics:

Managing Subscribers describes how to create and manage subscriber tiers and quota usage within the CMP system.

Note: The actual options you see depend on whether or not your CMP system is configured to operate with a (SPR). For information about the Oracle Communications Subscriber Database Management product, see the SDM documentation. For information about the Oracle Communications User Data Repository product, see the UDR documentation.

Creating a Tier

Tiers are categories that you can define and then apply to groups of subscribers. For example, you can create a series of tiers with different bandwidth limits. Once you define tiers, you can use them in policy rules.

To create a subscriber tier:

1. From the **Subscriber** section of the navigation pane, select **Tiers**.
   The content tree displays the **Tiers** folder.
2. Select the **Tiers** folder.
   The **Tier Administration** page opens.
3. Click **Create Tier**.
   The **New Tier** page opens.
4. Enter information as follows:
   a) **Name** (required) — Name of the tier.
      The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
      Enter up to 250 characters.
   c) **Downstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the downstream direction in bits per second.
      You can enter a value followed by M or G; for example, 4G for 4 gigabits per second.
   d) **Upstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the upstream direction in bits per second.
      You can enter a value followed by M or G; for example, 10M for 10 megabits per second.
5. When you finish, click **Save** (or **Cancel** to cancel the request).
   The tier is added to the CMP database, and the message "Tier created successfully" is displayed.

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 the Delete icon, located to the right of the tier you wish to delete.
   - From the content tree, select the tier and click **Delete**.

   You are prompted, "Are you sure you want to delete this Tier?"
3. Click **OK** (or **Cancel** to cancel the request).
   The message "Tier deleted successfully" is displayed in green on the page.

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. Once 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. When you finish, click **Save** (or **Cancel** to cancel the request).

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 the Delete icon, located to the right of the entitlement you wish to delete.
   - From the content tree, select the entitlement and click **Delete**.

   You are prompted, "Are you sure you want to delete this Entitlement?"
3. Click **OK** (or **Cancel** to abandon your request).

The entitlement is deleted.

Managing Sessions

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 V7.5.

To view a session:

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 are interested in.
   The **Policy Server Administration** page opens in the work area.
3. Select the **Session Viewer** tab.
   The **Session Viewer** tab 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 IndexByNAI 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 is displayed. *Figure 25: 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

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.

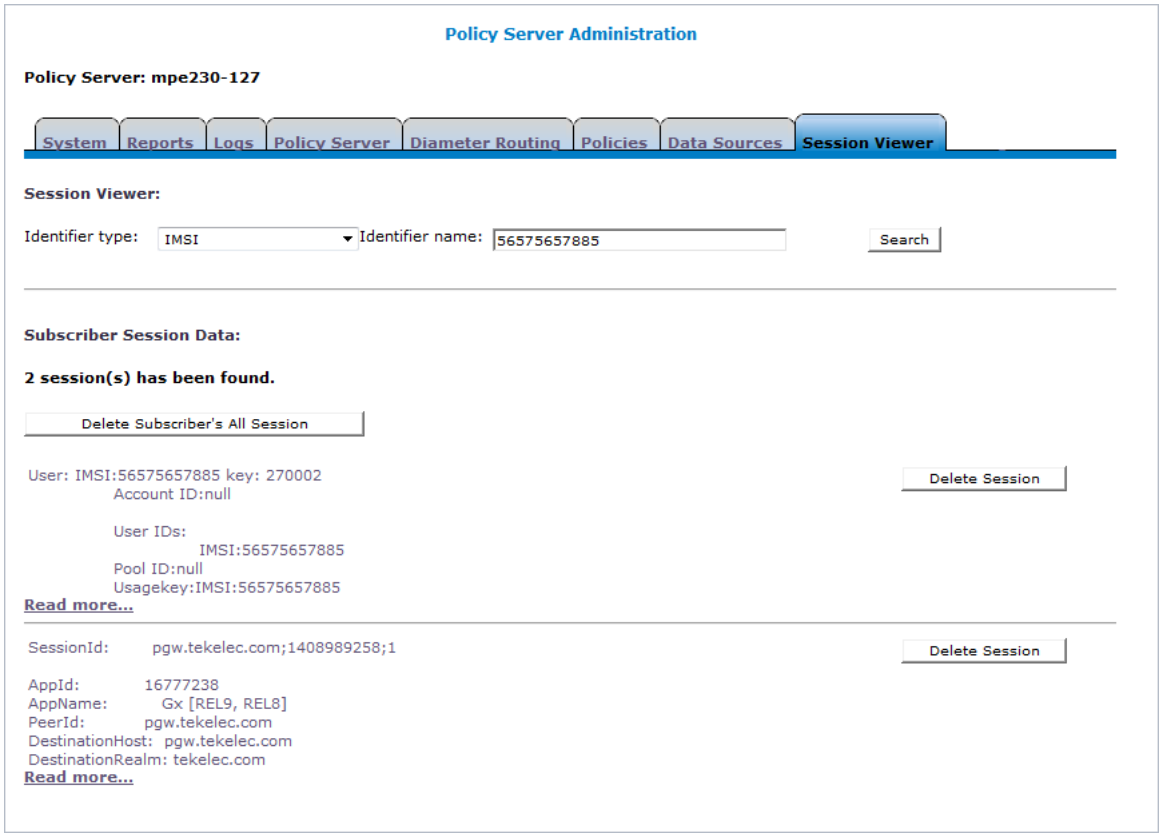


Figure 25: Session Viewer Page

Chapter 12

Managing Network Elements

Topics:

Managing Network Elements 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

Once 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 once 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, once you define network elements, 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 **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 in which you want to define the network element.

   (See *Creating a Network Element Group* for information on creating network element groups.)

   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Create Network Element**.
   The **New Network Element** page opens.
4. Enter information as appropriate for the network element:
   a) **Name** (required) — The name you assign to the network element.

      Enter up to 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 network element's primary address 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:

Note: This list varies depending on the configuration of the CMP

- **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** (default) — Gateway GPRS Support Node
- **HSGW** — HRPD Serving Gateway
- **PGW** — Packet Data Network Gateway
- **SGW** — Serving Gateway
- **DPI** — Deep Packet Inspection device
- **DSR** — Diameter Signaling Router device
- **NAS** — Network Access Server device

f) **Protocol Timer Profile**—select a protocol timer profile. For information on creating Protocol Timers, see *Managing Protocol Timer Profiles*.

g) **Capacity** — Not applicable.

5. Select one or more policy servers (MPE devices) to associate with this network element.
6. Select one or more MRA devices to associate with this network element.
7. To add a network element to a network element group, select the group (see *Adding a Network Element to a Network Element Group*).
8. When you finish, click **Save** (or **Cancel** to discard your changes).
The network element is displayed in the **Network Element Administration** page.

You have created the definition for a network element.

Modifying a Network Element

To modify a network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element.
The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Modify**.
The **Modify Network Element** page opens.
4. Modify network element information.
For a description of the fields contained on this page, see *Defining a Network Element*.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

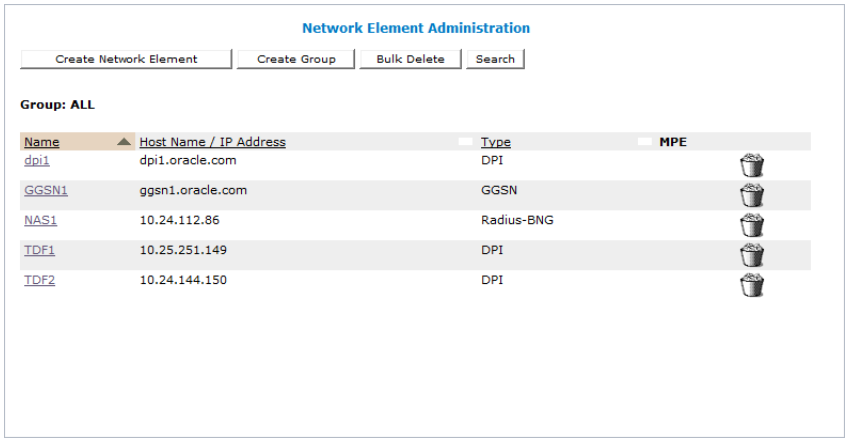
The network element definition is modified.

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 **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, displaying all defined network elements.
3. From the work area, click (trashcan icon), located to the right of the network element you want to delete:



   You are prompted: "Are you sure you want to delete this Network Element?"
4. Click **OK** to delete the network element (or **Cancel** to cancel the request).
   The network element is removed from the list.

You have deleted the definition of the network element.

Bulk Delete

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

1. From the **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 **ALL**.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Bulk Delete**.
   The **Bulk Delete Network Elements** page opens.
4. Select the network elements or network element groups to delete.

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

5. Click **Bulk Delete** (or **Cancel** to cancel the request).
   You are prompted: "Are you sure you want to delete all the selected Network Elements?"
6. Click **OK** to delete the network elements (or **Cancel** to cancel the request).
   The system displays the message "*m* Folder(s) and *n* Network Element(s) were deleted successfully."

The selected network element(s) or group(s) are deleted from the CMP database and all associated MPE devices.

Finding a Network Element

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

1. From the **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 **ALL**.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Search**.
   The **Network Element Search Criteria** window opens.
4. Enter the search criteria. Searches are not case sensitive. You can use the asterisk (*) and question mark (?) wildcard characters.
   - **Name** — The name assigned to the network element.
   - **Host Name/IP Address** — The domain name or IP address, in IPv4 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.
5. After entering search criteria, click **Search** (or **Cancel** to cancel the request).
   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 subsections describe how to configure options for a given network element type. The network elements types available 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.

PDSN

To configure options for a 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 following:
   a) Diameter Features
      - **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **`galactel.com`**).
      - **Diameter Identity** — Specifies the fully qualified domain name (FQDN) of the network element (for example, **`ne.galactel.com`**). Click **Add** to add the identity to the list; select an identity from the list and click **Delete** to remove it.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The PDSN device is defined.

GGSN

To configure interface information for a 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 FQDN of the network element (for example, **`ggsn1024.galactel.com`**).
      Click **Add** to define multiple identities used by the network element. To delete one of the identities, select it from the list and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The GGSN device is defined.

Home Agent

To configure options for a 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 following:
   a) Diameter Features
      - **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **`galactel.com`**).
      - **Diameter Identity** — Specifies the fully qualified domain name (FQDN) of the network element (for example, **`ne.galactel.com`**). Click **Add** to add the identity to the list; select an identity from the list and click **Delete** to remove it.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The Home Agent device is defined.

HSGW

To configure interface information for an 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) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **`galactel.com`**).
   b) **Diameter Identity** — Specifies the FQDN of the network element (for example, **`hsgw1024.galactel.com`**).
      Click **Add** to define multiple identities used by the network element. To delete one of the identities, select it from the list and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The HSGW device is defined.

PGW

To configure interface information for a 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) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **`galactel.com`**).
   b) **HQDN** --- Fully Qualified Domain Name (IP address) provides another identifier for the network element.
   c) **Diameter Identity** — Specifies the FQDN of the network element (for example, **`pgw1024.galactel.com`**).

      Click **Add** to define multiple identities used by the network element. To delete one of the identities, select it from the list and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The PGW device is defined.

SGW

To configure interface information for a signaling 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) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **`galactel.com`**).
   b) **Diameter Identity** — Specifies the FQDN of the network element (for example, **`sgw1024.galactel.com`**).

      Click **Add** to define multiple identities used by the network element. To delete one of the identities, select it from the list and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The SGW device is defined.

DPI

To configure interface information for a 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.
   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) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, **`galactel.com`**).
b) **Diameter Identity** — Specifies the FQDN of this network element (for example, **`dpi56.galactel.com`**) and click **Add**.

   Repeat this step to define multiple identities if multiple identities are used by this network element. To delete one of the identities, select it from the list and click **Delete**.
c) **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.
d) **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).
e) **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.
f) **Watch Dog Interval** (available if DPI capability is **TDF-Solicit**) — Enter the watchdog timer interval in seconds. The default is 30 seconds.
g) **Response Timeout** (available if DPI capability is **TDF-Solicit**) — Enter the response timeout interval in seconds. The default is 5 seconds.
h) **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.
i) **Associated MRA identity** (available if DPI capability is **TDF-Solicit**) — Select the MRA device from the drop-down list.
   You cannot associate a DPI device with an MRA device if you have selected **Allow direct connection from MPE**.
j) **Backup TDF Identity** (available if DPI capability is **TDF-Solicit**) — Select the backup TDF device from the drop-down list.

5. When you finish, click **Save** (or **Cancel** to discard your changes).

The DPI device is defined.

DSR

To configure interface information for 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.na.com`**).
   b) **Diameter Identity** — Enter the FQDN of this network element (for example, **`dsr56.galactel.com`**) and click **Add**.

      Repeat this step to define multiple identities if multiple identities are used by this network element. To delete one of the identities, select it from the list and click **Delete**.

5. When you finish, click **Save** (or **Cancel** to discard your changes).

The DSR device is defined.

NAS

To configure interface information for a NAS network element:

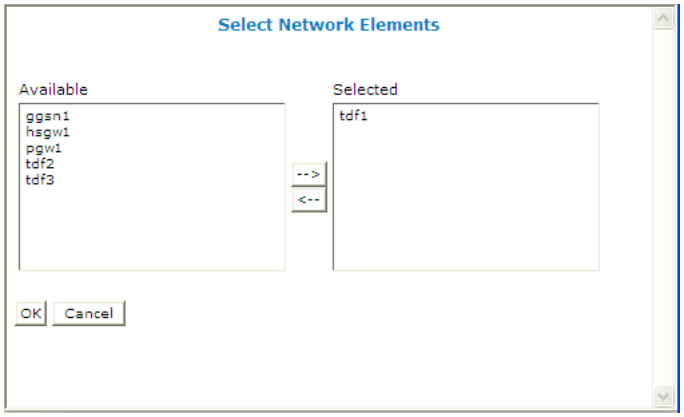
1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **NAS** tab and then click **Modify**.
   The **Modify Network Element** page opens.
4. Configure the following information:
   a) **Passphrase** — Specifies the passphrase (RADIUS shared secret) for this network element.
      Enter 1–255 characters. If the source IP address of a received message matches one of the IP addresses configured for the NAS device, then the MPE device will attempt to decode the message using this default passphrase. If not specified, the default passphrase configured on the MPE device (see *Managing Multimedia Policy Engine Devices*) is used.
   b) **IP Address** — Specifies up to 20 IPv4/IPv6 addresses supported by this device.
      To add an address to the list, enter it and click **Add**. To delete an address, select it from the list and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The NAS 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. On the **Policy Server Administration** page, select the **Policy Server** tab.
   In 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:



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 ?. When you finish, 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 multiple entries, use the Ctrl and Shift keys.

7. When you finish, click **OK** (or **Cancel** to discard your changes).
   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. When you finish, click **Save**, located at the bottom of the page (or **Cancel** to discard your changes).

The network element is associated with this MPE device.

Working with Network Element Groups

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

Creating a Network Element Group

To create a network element group:

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. On the **Network Element Administration** page, click **Create Group**.

The **Create Group** page opens.

4. Enter the name of the new network element group.

   The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).

5. Enter a text description of the network group.
6. When you finish, click **Save** (or **Cancel** to discard your changes).
   The new group appears in the content tree.

You have created a network element group.

Adding a Network Element to a Network Element Group

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

1. From the **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. On the **Network Element Administration** page, click **Add Network Element**.

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

   - If there are 25 or fewer network elements defined, the page displays the network elements not already part of the group. (*Figure 26: Add Network Element Page* shows an example.)
   - If there are more than 25 network elements defined, the page does not display any of them. Instead, use the **Search Pattern** field to filter the list. Enter an asterisk (*) to generate a global search, or a search pattern to locate only those network elements whose name matches the pattern (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. When you finish, click **Save** (or **Cancel** to cancel the request).

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

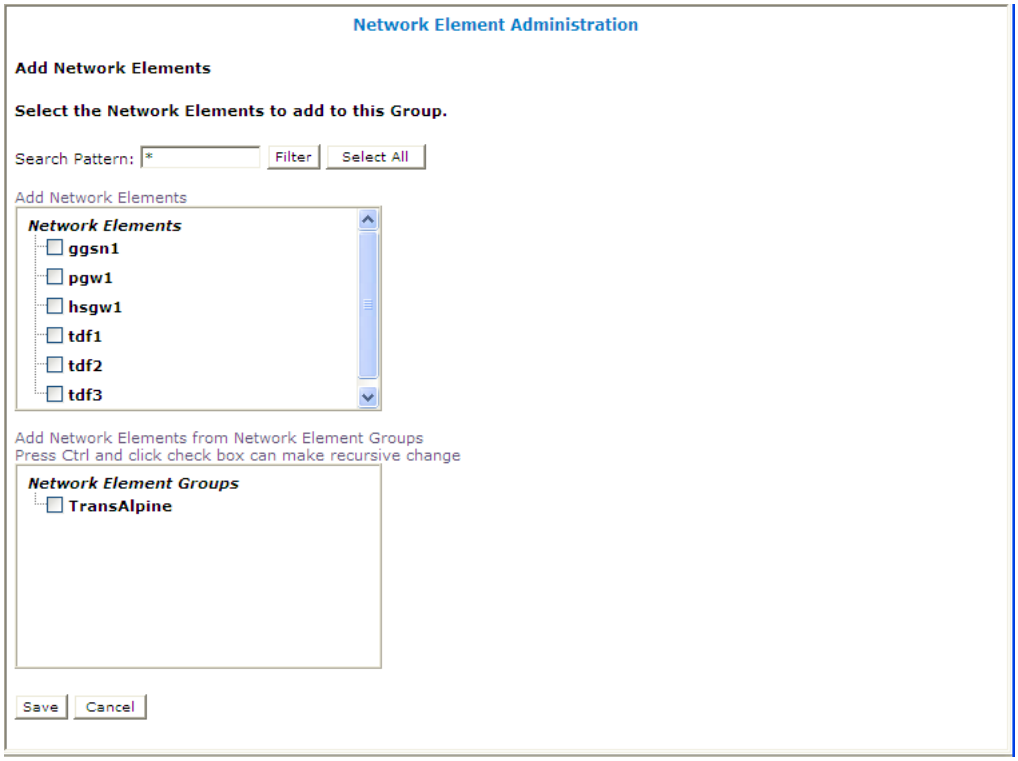


Figure 26: Add Network Element Page

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. On the **Network Element Administration** page, 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. When you finish, click **Save** (or **Cancel** to discard your changes).

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 **Delete** icon, located to the right to the network element you want to remove. You are prompted, "Are you sure you want to delete this Network Element from the group?" Click **OK** (or **Cancel** to cancel your request). The network element is removed from the group or sub-group, and a message indicates the change; for example, "Network Element deleted successfully."
   - From the content tree, select the network element; the **Network Element Administration** page opens. Click the **System** tab and then click **Remove**.

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

Modifying a Network Element Group

To modify a network element group or sub-group:

1. From the **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. On the **Network Element Administration** page, click **Modify**.
   The **Modify Group** page opens.
4. Modify the name or description.
5. When you finish, click **Save** (or **Cancel** to cancel the request).

The group is modified.

Deleting a Network Element Group or Sub-group

Deleting a network element group also deletes any associated sub-groups. However, any network elements associated with the deleted groups or sub-groups remain in the **ALL** group, from which they can be used again if needed. 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**.
   You are prompted, "Are you sure you want to delete this Group?"
4. Click **OK** to delete the group (or **Cancel** to cancel the request).

The network element group or sub-group is deleted.

Chapter 13

Managing Policy Front End Devices

Topics:

Managing Policy Front End Devices 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. The CMP system is used to manage all MRA functions. Before this can occur, the CMP operating mode must support managing MRA clusters.

To reconfigure the CMP operating mode, complete the following:

Caution: CMP operating modes should only be set in consultation with My Oracle Support (MOS). 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 version number.
2. Click the **Mode** button.
   Consult with My Oracle Support for information on this button.
   The **Mode Settings** page opens.
3. At the bottom of the page, select **Manage MRAs**.
4. Click **OK**.
   The browser page closes and you are automatically logged 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

You must define a 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. On the **MRA Administration** page, 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 pulldown 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.
      Enter up to 250 characters.

d) **Secure Connection** — Select to enable a secure HTTP connection (HTTPs) instead of a normal connection (HTTP).

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 stateless routing.

5. When you finish, click **Save** (or **Cancel** to discard your changes).
The MRA cluster profile is displayed in the **MRA Administration** page.

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

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. From the content tree, select the MRA cluster profile.
The **MRA Administration** page opens in the work area.
3. On the **System** tab of the **MRA Administration** page, click **Modify**.
The **Modify System Settings** page opens.
4. Modify MRA system settings as required.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The MRA cluster profile settings are modified.

Configuring Protocol Options for an MRA Device

To configure protocol options on an MRA device:

1. From the **MRA** section of the navigation pane, select **Configuration**.
2. From the content tree, select the MRA device.
The **MRA Administration** page opens.
3. On the **MRA Administration Administration** page, select the **MRA** tab.
The current configuration options are displayed.
4. Click **Modify** and define options as necessary.

MRA Protocol Configuration Options defines available options that pertain specifically to MRA devices. (The options may vary depending on the configuration mode of the system.)

5. When you finish, click **Save** (or **Cancel** to discard your changes).

Table 12: MRA Protocol Configuration Options

Attribute	Description
Subscriber Indexing	**Note:** The indexing parameters to use depend on what user IDs are needed for correlating various messages to ensure they all end up on the same MPE device for the same user. If you are unsure which indexing method(s) to configure, contact My Oracle Support (*https://support.oracle.com*).
Index by Username	Select if the MRA devices in the association should index by account ID.
Index by NAI	Select if the MRA devices in the association should index by network access ID.
Index by E.164 (MSISDN)	Select if the MRA devices in the association should index by E.164 phone number.
Index by IMSI	Select if the MRA devices in the association should index by IMSI number).
Index by Session ID	Select if the MRA devices in the association should index by session ID.
Primary Indexing	Select from the pull-down list to set to the type of index that is expected for messages that create bindings, for example Gx CCR-I. **Note:** The type of index selected for primary indexing must also be selected either as an "Index by IMSI" or "Index by E.164" depending on the configuration. CAUTION: Primary Index cannot be changed on a system that has already created bindings without suffering data loss.
Index by IP Address	Select if the MRA devices in the association should index by IP address. You can select **Index by IPv4**, **Index by IPv6**, or both formats.
Overrides by APN	Select to perform subscriber indexing for a specific IP address and a specific APN name. In the **Overrides by APN** section, click **Add**. Enter the APN name 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.

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

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. On the **MRA Administration** page, click **Create Group**.
   The **Create Group** page opens.
4. Enter the name of the new CMP group.

   The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. When you finish, click **Save** (or **Cancel** to abandon your request).
   The new group appears in the content tree.

The MRA group is created.

Adding an MRA Cluster Profile to an MRA Group

Once 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. On the **MRA Administration** page, click **Add Multi-protocol Routing Agent**.
   The **Add Multi-protocol Routing Agent** page opens.
4. Select the MRA cluster profile you want to add; use the Ctrl or Shift keys to select multiple MRA cluster profiles.
5. When you finish, click **Save** (or **Cancel** to abandon the request).

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 an MRA group.
   The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.

3. Remove the MRAcluster profile using one of the following methods:
   - On the **MRA Administration** page, click the **Delete** 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

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. 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**.
   The content tree displays a list of 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**.
   You are prompted: "Are you sure you want to delete this Group?"
4. Click **OK** to delete the selected group (or **Cancel** to abandon the request).

The MRA group is deleted.

Enabling Stateless Routing

To hide configuration relevant to a stateful MRA device in the CMP display, select **Stateless Routing** (*Figure 27: Enabling Stateless Routing* shows an example).

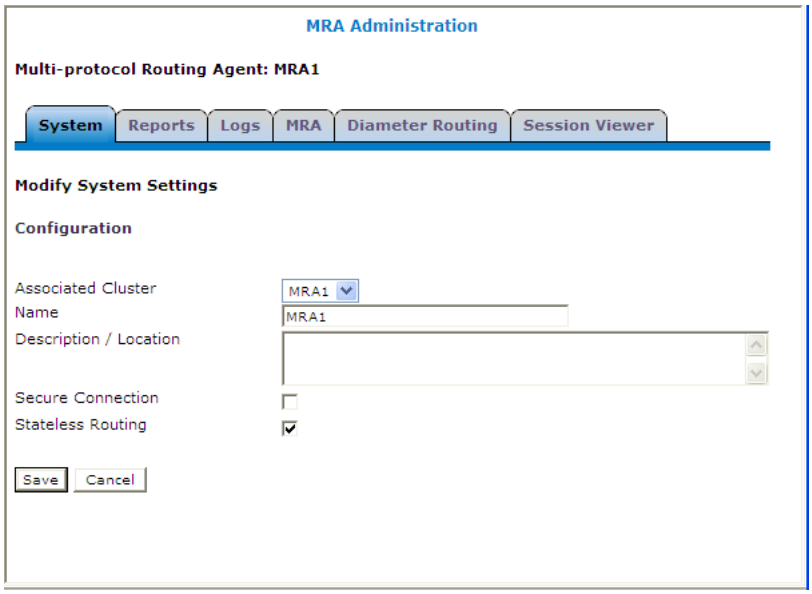


Figure 27: Enabling Stateless Routing

Reapplying the Configuration to Policy Management Devices

You can reapply the configuration to an individual MPE or MRA device (server), or to all MPE or MRA devices in a group. When you reapply the configuration, the CMP system completely reconfigures the server with topology information, ensuring that the configuration matches the data in the CMP system. This action is not needed during normal operation but is useful in the following situations:

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

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. To reapply the configuration for an individual MPE or MRA device:
   a) From the content tree, select the **ALL** group.
      The **Policy Server Administration** page opens in the work area.
   b) From the **ALL** group, select the server.
      The **Policy Server Administration** page opens to the **System** tab, displaying information for that server.
   c) Click **Reapply Configuration**.
      An in-progress message appears. When the operation is complete you are prompted, "The configuration was applied successfully."

The individual server or all of the servers in a group are synchronized with the CMP system.

Resetting Counters

The **Reset Counters** option is included in the **Operations** menu when the **Stats Reset Configuration** option is set to **Interval**. The **Reset All Counters** option is included in the **Operations** menu when the **Stats Reset Configuration option** is set to **Manual**. See *Setting Stats Settings* for more information.

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

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the group that contains the servers of interest.
   The **Policy Server Administration** page opens in the work area.
3. From the **Operations** menu, select **Reset Counters** or **Reset All Counters**.
   The **Bulk Reset All Counters** or **Bulk Reset Counters** dialog displays showing the number of servers affected.

4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.

The counters are reset.

Chapter 14

Managing S-CMP Devices

Topics:

Managing S-CMP Devices describes how to use the NW-CMP system to configure and manage S-CMP devices in a tiered CMP system. The S-CMP devices manage the MPE and MRA devices in a tiered the Policy Management policy server.

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

About S-CMP Devices

A System Configuration Management Platform (S-CMP) device manages MPE and MRA devices in a tiered Network CMP system. The Network CMP system contains one or more S-CMP. The S-CMP can view, but not modify anything that is created, edited, or deleted at the Network Configuration Management Platform (NW-CMP) level. The S-CMP blocks users from changing associations set at the NW-CMP layer in order to maintain data integrity between the NW-CMP and the S-CMP devices.

The S-CMP can create the following associations to the MPE device:

- Applications
- Network Elements
- Network Element Groups
- Policies
- Policy Groups

The S-CMP can create the following associations to the MRA device:

- MPE and MRA Pools
- Network Elements
- Network Element Groups

Creating an S-CMP Device

To create an S-CMP device:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
   The **S-CMP Administration** page opens in the work area.
3. Click **Create S-CMP**.
   The **New S-CMP** page opens.
4. Enter information for the S-CMP:
   a) **Name** (required) — The name you assign to the S-CMP.
      The name can be up to 255 characters long and must not contain colons (:), quotation marks ("), or commas (,).
   b) **Site One VIP** (required) — The first Virtual IP Address (VIP) for the S-CMP.
   c) **Site Two VIP** — The second VIP for the S-CMP. If the S-CMP has is in a georedundant cluster, then both VIP sites (1 and 2) must be specified. These VIP addresses are populated in the NW-CMP and are used by the NW-CMP when querying or pushing data to the S-CMP.
   d) **Secure Connection** — Indicates that this S-CMP has https enabled, therefore, the NW-CMP connects to the S-CMP using a secure connection secure connection (https).
   e) **Description** — Free-form text that identifies the S-CMP device within the network.
      Enter up to 250 characters.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The S-CMP device is displayed in the **S-CMP Administration** page.

Opening an S-CMP Device from an NW-CMP

To open an S-CMP device from an NW-CMP:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
   The **S-CMP Administration** page opens in the work area.
3. Select an S-CMP.
   The configuration for the S-CMP displays in the Work Area.
4. If the server is active, click the S-CMP name in the work area.

The S-CMP opens in a new browser tab.

Modifying an S-CMP Device

To modify an S-CMP device:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
   The **S-CMP Administration** page opens in the work area.
3. Select an S-CMP.
   The configuration for the S-CMP displays in the work area.
4. Click **Modify**.
   The **Modify S-CMP** page opens in the work area.
5. Make configuration changes.
   See *Creating an S-CMP Device* for information about the fields.
6. When you finish, click **Save** (or **Cancel** to discard your changes).
   The S-CMP device is updated with the new configuration.

Reapplying the Configuration to S-CMP Devices

You can reapply the configuration to an individual S-CMP device. You must reapply the configuration after the S-CMP is modified.

To reapply the configuration to the S-CMP device:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
   The **S-CMP Administration** page opens in the work area.
3. Select an S-CMP.

The configuration for the S-CMP displays in the work area.

4. Click **Reapply Configuration**.
   The current setting for the S-CMP are applied.

The individual server is synchronized with the configuration on the NW-CMP device.

Deleting an S-CMP Device

To delete an S-CMP:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. You can delete a profile using one of the following methods.
   - Select the **S-CMPs** folder and then click (trash can) in the work area for the device. A confirmation message displays. Click **OK** to delete or **Cancel** to abort the process.
   - Select a device from the **S-CMPs** folder and then click **Delete**. A confirmation message displays. Click **OK** to delete or **Cancel** to abort the process.

The profile is updated.

About S-CMP Groups

For organizational purposes, you can aggregate the S-CMP devices in your tiered network into groups. The following subsections describe how to manage S-CMP groups.

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

Creating an S-CMP Group

To create an S-CMP group:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the **S-CMPs** group.
   The **S-CMP Administration** page opens in the work area.
3. Click **Create Group**.
   The **Create Group** page opens.
4. Enter the name of the new S-CMP group.
   The name cannot contain quotation marks (") or commas (,).
5. (Optional) Enter a description for the group.
   The description must not exceed 250 characters.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

You have created a an S-CMP group.

Adding S-CMP Devices to a Policy Server Group

To add S-CMP devices to an S-CMP group:

Note: You must be in NW-CMP mode to configure and manage S-CMP devices.

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. From the content tree, select the S-CMP group.
   The **S-CMP Administration** page opens in the work area displaying the contents of the selected S-CMP group.
3. Click **Add S-CMP**.
   The **Add S-CMP** page opens, displaying the S-CMP devices not already part of the group.
4. Click the S-CMP device you want to add; use Ctrl or Shift-Ctrl to select multiple S-CMP devices.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The S-CMP devices are added to the selected group.

Creating an S-CMP Sub-group

You can create sub-groups to further organize your tiered CMP network. To add an S-CMP sub-group to an existing S-CMP group:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. From the content tree, select the S-CMP group.

   The **S-CMP Administration** page opens in the work area, displaying the contents of the selected S-CMP group.
3. Click **Create Sub-Group**.

   The **Create Group** page opens.
4. Enter the name of the new sub-group.

   The name cannot contain quotation marks (") or commas (,).
5. (Optional) Enter a description for the group.
   The description must not exceed 250 characters.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The sub-group is added to the selected group.

Renaming an S-CMP Group

To modify the name assigned to an S-CMP group or sub-group:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the policy server group or sub-group.
   The **S-CMP Administration** page opens in the work area.
3. Click **Modify**.

The **Modify Group** page opens.

4. Enter the new name in the **Name** field.
   The name cannot contain quotation marks (") or commas (,).
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The group is renamed.

Deleting an S-CMP Group

Deleting an S-CMP group also deletes any associated sub-groups. You cannot delete the ALL group.

To delete an S-CMP group or subgroup:

1. From the **S-CMP** section of the navigation pane, select **Configuration**.
   The content tree displays the **S-CMPs** group.
2. Select the S-CMP group or sub-group.
   The **S-CMP Administration** page opens in the work area, displaying the contents of the selected S-CMP group or sub-group.
3. Click **Delete**.
   A confirmation message displays.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

The S-CMP group is deleted.

Chapter 15

System-Wide Reports

Topics:

System-Wide Reports 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.

Note: When you are in a NW-CMP, the KPI Dashboard lists the S-CMP servers only. Click an S-CMP name to open the KPI Dashboard for that specific server.

Figure 28: 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 28: 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 checkbox 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 *Policy Management Troubleshooting Guide* for this release.

Click the name of an MPE or MRA device to display detailed statistics. For more information on detailed device statistics, see the description on the **Reports** tab for the device.

Mapping Display to KPIs

The following tables explain how each of the columns in the KPI dashboard are mapped to a specific statistic in the KPI statistics. On the initial KPI Dashboard window, KPIs for each MRA and MPE device are shown. Since the tables contain row entries for the active, standby and spare servers (if georedundancy is configured), the mapping is described for all three servers. *Table 13: KPI Definitions for MRA Devices* shows the mappings for MRA devices; *Table 14: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System* shows the mappings for MPE devices when the MRA devices are managed by the CMP system; and *Table 15: KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System* shows the mappings for MPE devices when the MRA devices are not managed by the CMP system.

Table 13: KPI Definitions for MRA Devices

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby and spare server (spare only shows Status, CPU % and Memory%)**
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None

KPI Dashboard Column	Mapping to Statistics	
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	None
Active Subscribers	CurrentMRABindingCount and CurrentMRABindingPercentageOf Capacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
MPE Connections	A value in the form "X of Y", where: X is CurrentMPEConnectionCount Y is ConfiguredMPEConnectionCount	None
MRA Connections	A value in the form "X of Y", where: X is CurrentMRAConnectionCount Y is ConfiguredMRAConnectionCount	None
Network Element Connections	A value in the form "X of Y", where: X is CurrentConnectedNECount Y is ConfiguredNECount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Table 14: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
Name	Not derived from statistics	Not derived from statistics

KPI Dashboard Column	Mapping to Statistics	
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	None
Active Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
MRA Connections	A value in the form "X of Y", where: X is CurrentMRAConnectionCount Y is ConfiguredMRAConnectionCount	None
Data Sources	A value in the form "X of Y", where: X is CurrentSPRConnectionCount Y is ConfiguredSPRConnectionCount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Table 15: KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
Name	Not derived from statistics	Not derived from statistics

KPI Dashboard Column	Mapping to Statistics	
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
Active Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
SPR Connections	A value in the form "X of Y", where: X is CurrentSPRConnectionCount Y is ConfiguredSPRConnectionCount	None
Network Element Connections	A value in the form "X of Y", where: X is CurrentConnectedNECount	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.

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

Table 16: Policy Statistics

Display	MPE	MRA	Name
Peg Count	Y	N	Policy Count
Evaluated	Y	N	Evaluated Count
Executed	Y	N	Executed Count
Ignored	Y	N	Ignored Count
Policy Details Stats:			
Name	Y	N	Policy Name
Evaluated	Y	N	Eval Count
Executed	Y	N	Trigger Count
Ignored	Y	N	Ignore Count
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	(Data for each installed rule)

Table 17: Quota Profile Statistics Details

Display	MPE	MRA	Name
Peg Count	Y	N	Quota Count
Activated	Y	N	Quota Activated Count
Volume Threshold Reached	Y	N	Quota Volume Threshold Reached Count
Time Threshold Reached	Y	N	Quota Time Threshold Reached Count
Event Threshold Reached	Y	N	Quota Event Threshold Reached Count

Table 18: Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count

Display	MPE	MRA	Name
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
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

Display	MPE	MRA	Name
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
Diameter AF Peer Stats (in Diameter AF Stats window)	N	Y	
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 19: Diameter Policy Charging Enforcement Function (PCEF) Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count (SCTP or TCP)
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count

Display	MPE	MRA	Name
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

Table 20: 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

Display	MPE	MRA	Name
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
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 21: 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

Display	MPE	MRA	Name
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
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

Display	MPE	MRA	Name
Max active sessions	Y	N	Max Active Session Count
Diameter BBERF connections	Y	Y	

Table 22: 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
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

Display	MPE	MRA	Name
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 23: Diameter Sh Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
Messages retried	Y	N	
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count
UDR messages timeout	Y	N	UDRTimeout Count
UDR messages retried	Y	N	
UDA success messages received/sent	Y	N	UDA Success Messages Received Count\UDA Success Messages Sent Count
UDA failure messages received/sent	Y	N	UDA Failure Messages Received Count\UDA Failure Messages Sent Count
PNR messages received/sent	Y	N	PNR Messages Received Count\PNR Messages Sent Count
PNA success messages received/sent	Y	N	PNA Success Messages Received Count\PNA Success Messages Sent Count
PNA failure messages received/sent	Y	N	PNA Failure Messages Received Count\PNA Failure Messages Sent Count

Display	MPE	MRA	Name
PUR messages received/sent	Y	N	PUR Messages Received Count\PUR Messages Sent Count
PUR messages timeout	Y	N	PURTimeout Count
PUR messages retried	Y	N	
PUA success messages received/sent	Y	N	PUA Success Messages Received Count\PUA Success Messages Sent Count
PUA failure messages received/sent	Y	N	PUA Failure Messages Received Count\PUA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SNR Messages Sent Count
SNR messages timeout	Y	N	SNRTimeout Count
SNR messages retried	Y	N	
SNA success messages received/sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/send	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
Currently active sessions	Y	N	Active Sessions Count
Max active sessions	Y	N	Maximum Active Sessions Count
Diameter Sh connections			

Table 24: Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently okay peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
DBR messages received/sent	N	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	N	Y	DBRTimeout Count
DBA success messages received/sent	N	Y	DBARecv Success Count\DBASend Success Count

Display	MPE	MRA	Name
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	
DBA-T failure messages received/sent	N	Y	
DBR-S messages received/sent	N	Y	

Display	MPE	MRA	Name
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: Diameter DRA statistics apply only to MRA devices.

Table 25: 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 26: 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 27: 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	

Display	MPE	MRA	Name
Accounting Stop received	Y	Y	Accounting Stop Count
Accounting Stop received for unknown reason	Y	Y	
Accounting On sent	Y	Y	
Accounting On received	Y	Y	
Accounting Off sent	Y	Y	
Accounting Off received	Y	Y	
Accounting Response sent	Y	Y	Accounting Response Count
Accounting Response received	Y	Y	
Duplicates detected	Y	Y	Duplicated Message Count
Unknown/Unsupported messages received	Y	Y	
Interim Update Received	Y	Y	Accounting Update Count
Interim Update Received for unknown reason	Y	Y	
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	

Display	MPE	MRA	Name
Average Parse Time	Y	Y	
Maximum Parse Time	Y	Y	
Unknown BNG. Message dropped	Y	Y	Unknown Gateway Request Count
Unknown BNG. Account Start dropped	Y	Y	
Unknown BNG. Account Stop dropped	Y	Y	
Unknown BNG. Interim Update dropped	Y	Y	
Stale sessions deleted	Y	Y	
Stale sessions deleted due to missed Interim Update	Y	Y	
Stale sessions deleted on Account-On or Account-Off	Y	Y	
Invalid subscriber key. Message dropped	Y	Y	
Invalid subscriber identifier specified. Message dropped	Y	Y	Unknown Subscriber Request Count

Table 28: 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 28: 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

Display	MPE	MRA	Name
			Processing Time [40-60] ms Processing Time [60-80] ms Processing Time [80-100] ms Processing Time [100-120] ms Processing Time [120-140] ms Processing Time [140-160] ms Processing Time [160-180] ms Processing Time [180-200] ms Processing Time [>200] ms

Table 29: 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 30: 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 31: 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

Display	MPE	MRA	Name
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 32: 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 33: Sh Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Number of search errors that triggered the retry	Y	N	
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time
Number of successful updates	Y	N	Update Hit Count
Number of unsuccessful updates	Y	N	Update Miss Count
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

Display	MPE	MRA	Name
Number of subscriptions that failed because of errors	Y	N	Subscription Err Count
Number of subscription errors that triggered the retry	Y	N	
Time spent on successful subscriptions (ms)	Y	N	Subscription Total Hit Time
Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Total Miss Time
Max Time spent on successful subscriptions (ms)	Y	N	Subscription Max Hit Time
Max Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Max Miss Time
Average time spent on successful subscriptions (ms)	Y	N	Subscription Avg Hit Time
Average time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Avg Miss Time
Number of successful unsubscriptions	Y	N	Unsubscription Hit Count
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 34: Sy Data Source Statistics

Display	MPE	MRA	Name
Number of successful searches	Y	N	Search Hit Count
Number of unsuccessful searches	Y	N	Search Miss Count
Number of searches that failed because of errors	Y	N	Search Err Count
Max Time spent on successful search (ms)	Y	N	Search Max Hit Time
Max Time spent on unsuccessful search (ms)	Y	N	Search Max Miss Time
Average time spent on successful searches (ms)	Y	N	Search Avg Hit Time
Average time spent on unsuccessful searches (ms)	Y	N	Search Avg Miss Time

Table 35: 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

Color Threshold Configuration

The Color Threshold Configuration popup window is brought up when you click the **Change Thresholds** button, located in the top right corner of the KPI Dashboard.

The values displayed in the dialog boxes are the current settings. The user can modify the values and click **Save** to put the new values into effect. The values is saved so the next time the dashboard is opened it uses the same values.

Note: Saving the thresholds affects other users that may be viewing the dashboard at the same time.

The **Cancel** button closes the popup dialog without any changes to the KPI dashboard display. The **Reset** button restores the values to their defaults. The TPS and session limits for the Policy Management device will be set to the officially supported rates for the current software release.

Viewing Active Alarms

The Active Alarms summary provides an aggregate view of timestamped 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 29: Sample Active Alarms Report shows a sample active alarm report.

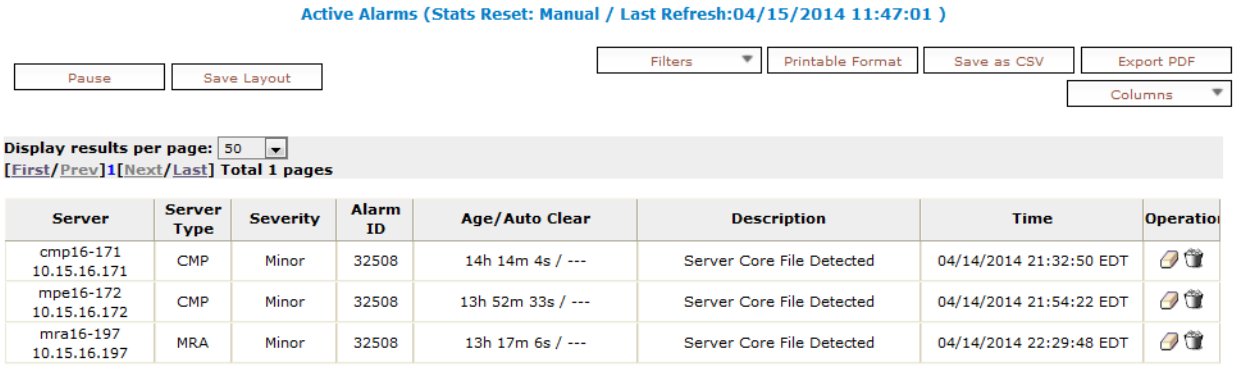


Figure 29: Sample Active Alarms Report

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 before V7.5 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 "---" 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 (trash can), located to the right of each row. You are prompted, "This alarm will be cleared. Are you sure?" Click **OK** (or **Cancel** to abandon your request).
- 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 pulldown list.
- To control what alarms and alarm classes are displayed on the page, click **Filters** and select from the pulldown menu:
  - The **Search Filter** tab has three controls. The **Server** control lets you display alarms from all servers (the default) or a specific server. The **Server Type** control lets you display alarms from all Policy Management products (the default) or just **CMP**, **MRA**, or **MPE** systems. The **Severity** control lets you display alarms of all severities (the 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 the delete icon, 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.

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 system 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 in the **System Wide Reports** menu:

- 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 10 subscribers can be enabled for logging.
- 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** drop-down list to display messages that appear during a specific time period.
- Select a message type from the **Activity Type** drop-down list to filter messages in the window by message type: **All** (the default), **Gx**, **GxLite**, **Gxx**, **Gy**, **Rx**, **Sd**, **Sh**, **Sy**, **LDAP**, or **Policy**.
- Enable or disable the **Automatic Scroll** checkbox. 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) **Severity** — Select the level of messages written to the log: **INFO** (the default), **NOTIFY**, or **DEBUG**.
   c) **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** to save the settings (or **Cancel** to discard your changes).
   The Subscriber Activity Log is configured.

You have defined and saved the Subscriber Activity Log configuration.

Adding Subscriber Identifiers

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. Click **Modify**.
   A new **Subscriber Activity Log Settings** page opens, containing fields for configuring the log.
3. 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 name of the identifier:
      - **IMSI** (the 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{}!#$%'^/=`|~-.

c) Enable the subscriber trace.
d) Click **Save** (or **Cancel** to discard your changes).
The subscriber is displayed in the table.

4. After adding the first subscriber, you can edit the subscriber information, clone the subscriber to create a new subscriber, or delete the subscriber:
   - To edit a subscriber, select the subscriber, and click **Edit**. The **Edit Subscriber Identifier** window opens. Edit the information. Click **Save** to save the edits. Click **Cancel** to exit the popup without saving the information.
   - To add a new subscriber by cloning an existing subscriber, select the subscriber and click **Clone**. The **Edit Subscriber Identifier** window opens, containing the information that was used to create the selected subscriber. Edit the information to create a subscriber. Click **Save** to create a subscriber (or **Cancel** to discard your changes).
   - To delete a subscriber, select the subscriber and click **Delete**. You are asked if you want to delete the subscriber. Click **Delete** to delete the subscriber (or **Cancel** to discard your changes).
5. Click **Save** to save the identifier list (or **Cancel** to discard your changes).
The Subscriber Identifier List is populated with the defined subscribers.

You have defined and saved the subscribers.

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) Set the start time for the backup. The date must be in the future. In the **First Running Time**, enter a date and time to start the backup in the format *mm/dd/yyyy hh:mm* (for example, **`01/01/2015 12:15`**).
   Alternatively, click (calendar) and select a date. When you finish, 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** to save the settings (or **Cancel** to discard your changes).
   The backup settings are configured.

You have defined and saved the Subscriber Activity Log configuration.

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. Click **Save** to save the edits (or **Cancel** to discard your changes).
5. Click **Save** to save the changes (or **Cancel** to discard your changes).
   The Subscriber Identifier is modified.

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; use the Ctrl or Shift keys to select multiple subscribers. Click **Delete**.
   You are prompted, "Are you sure you want to delete the selected Subscriber Identifier(s)?"
4. Click **Delete** to delete the subscriber identifier(s) (or **Cancel** to discard your changes).
   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 pulldown list provides the following options:
    - **24 hours** (the 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 pulldown list provides the following options:
    - **24 hours** (the 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 pulldown list provides the following options:
  - **24 hours** (the 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 pulldown list provides the following options:
    - **24 hours** (the 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 (*Figure 30: Trending Report Definition Configuration Page* shows a sample).

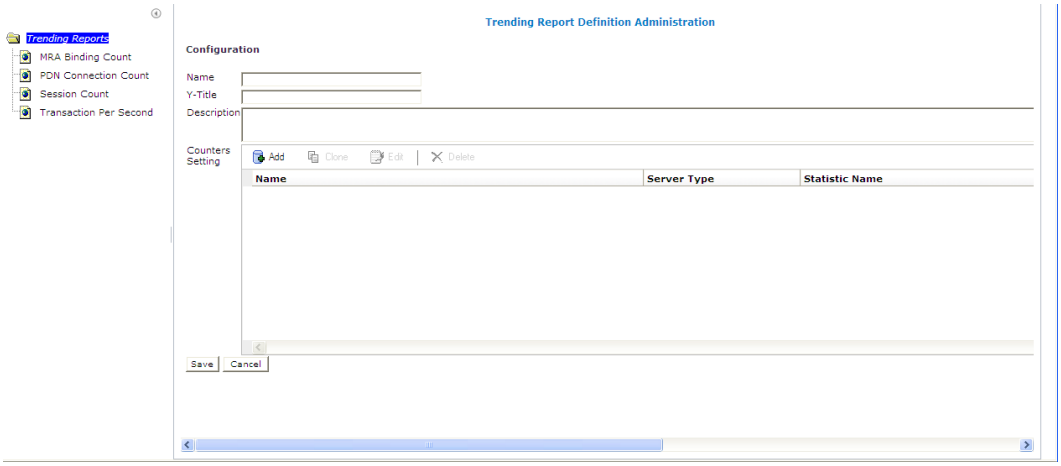


Figure 30: Trending Report Definition Configuration Page

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. Click **Cancel** to exit the popup without adding a counter.
   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. After adding the first counter to the trending report, you can edit the counter information, clone the counter to create a new counter, or delete the counter.
   - To edit a counter, select the counter, and click **Edit**. The **Edit Stats Definition** popup appears. Edit the information. Click **Save** to save the edits. Click **Cancel** to exit the popup without saving the information.
   - To add a new counter by cloning an existing counter, select the counter and click **Clone**. The **Clone Stats Definition** popup displays, containing the information that was used to create the selected counter. Edit the information to create a counter. Click **Save** to create a counter. Click **Cancel** to exit the popup without creating a new counter.
   - To delete an existing counter, select the counter and click **Delete**. You are asked if you want to delete the counter. Click **Yes** to delete the counter. Click **No** to exit the popup without deleting the counter.
6. Click **Save** at the bottom of the **Trending Report Definition** page to save the report. Click **Cancel** to exit the **Trending Report Definition** page without saving the report.
   The custom trending report appears, in alphabetical order by name, in the list of custom trending reports.

You have defined and saved a custom trending report.

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**.
   You are prompted, "Are you sure you want to delete this Trending Report?"
5. Click **OK** (or **Cancel** to abandon the request).
   The report name is removed from the list.

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 timestamped 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 31: Sample Active Alarms Report shows a sample active alarm report.

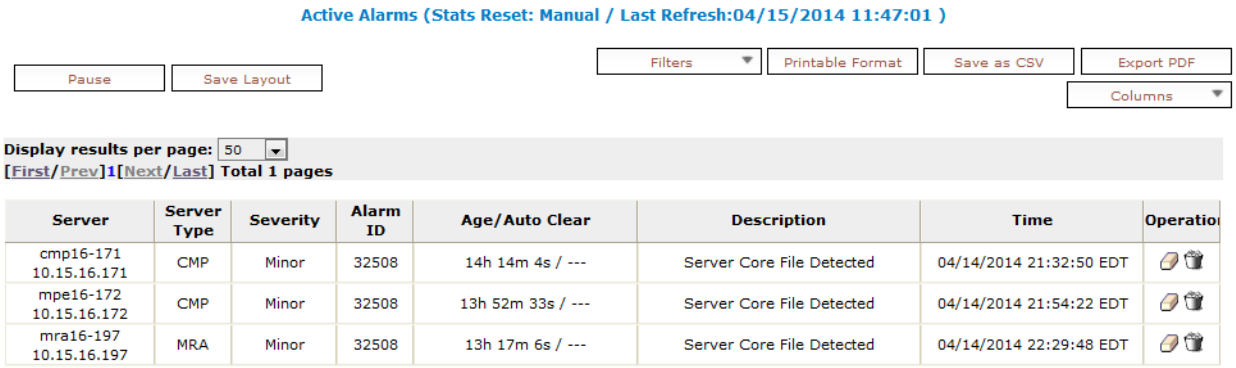


Figure 31: Sample Active Alarms Report

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 before V7.5 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 "---" 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 (trash can), located to the right of each row. You are prompted, "This alarm will be cleared. Are you sure?" Click **OK** (or **Cancel** to abandon your request).
- 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 pulldown list.
- To control what alarms and alarm classes are displayed on the page, click **Filters** and select from the pulldown menu:

  - The **Search Filter** tab has three controls. The **Server** control lets you display alarms from all servers (the default) or a specific server. The **Server Type** control lets you display alarms from all Policy Management products (the default) or just **CMP**, **MRA**, or **MPE** systems. The **Severity** control lets you display alarms of all severities (the 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 the delete icon, 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 (the default is **All**) from the list.
   - **Cluster or Server** — Select the cluster or server within the cluster whose alarms you want to view.
   - **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.

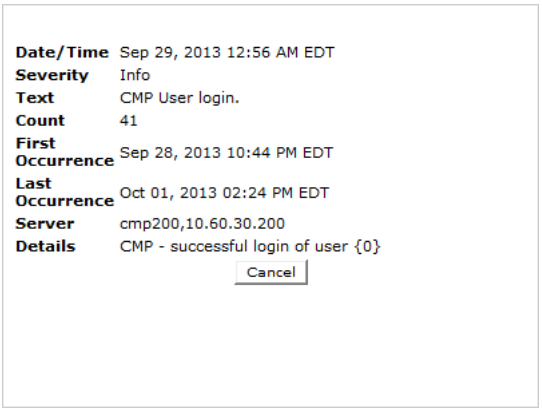
5. When you finish, click **Close** to close the window.

Alarms contain the following information:

- **Occurrence** — The most recent time this alert was triggered.
- **Severity** — The severity of the alert:
  - **Critical** — Service is being interrupted (displays in red).
  - **Major** — Service may be interrupted if the issue is not corrected (displays in orange).
  - **Minor** — Non service affecting fault (displays in yellow).
  - **Info** — Informational message only.
  - **Clear** — Alarm has been cleared.

  Note: Alarms generated by Policy Management systems running software before V7.5 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:



Click **Cancel** to close the window.

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** pulldown menu. 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** pulldown menu. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (the default), server totals only, or one specific server.
- **Server Type** — Filter in all server types (the default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA** — Filter in all MRA devices (the 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** pulldown menu. 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** pulldown menu. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (the default), server totals only, or one specific server.
- **Server Type** — Filter in all server types (the default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA** — Filter in all MRA devices (the 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** pulldown menu. 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** pulldown menu. 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, from the **System Wide Reports** section of the navigation pane, select **Others** and then select **Connection Status**.

Figure 32: Sample Connection Status Report shows a sample connection status report.

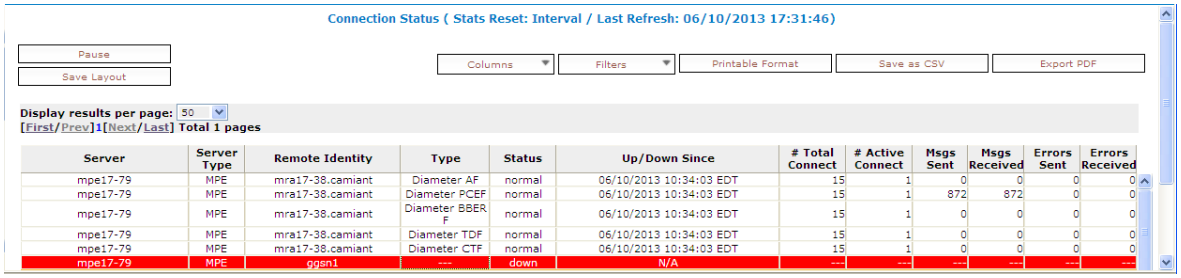


Figure 32: Sample Connection Status Report

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** pulldown menu. 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** pulldown menu. You can define filtering criteria using the following fields:

- **Server** — Filter in all servers (the default) or one specific server.
- **Server Type** — Filter in all server types (the default), totals only, MPE devices only, or MRA devices only.
- **Remote Identity** — Filter in all remote devices (the default) or one specific device.

- **Type** — Filter in all remote device types (the 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 (the 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, from the **System Wide Reports** section of the navigation pane, select **Others** and then 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** pulldown menu. 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** pulldown menu. You can define filtering criteria using the following fields:

- **Server** — Filter in all servers (the default) or one specific server.
- **Server Type** — Filter in all server types (the default), totals only, MPE devices only, or MRA devices only.
- **Remote Identity** — Filter in all remote devices (the default) or one specific device.
- **Error** — Filter in all remote error types (the 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** pulldown menu. 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** pulldown menu. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (the default) or one specific server.
- **Policy Name** — Filter in all policies (the 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 33: Sample MPE/MRA Replication Statistics Report shows a sample replication report.

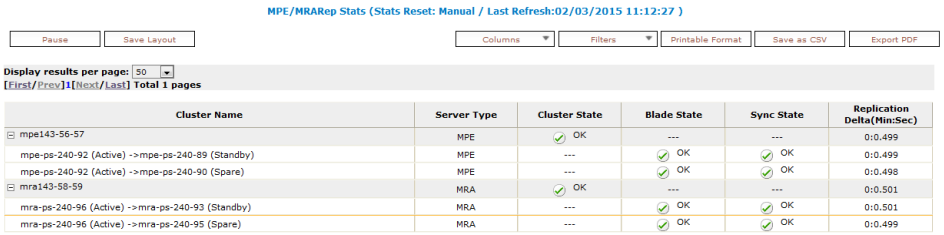


Figure 33: Sample MPE/MRA Replication Statistics Report

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** pulldown menu. The following columns are available:

- **Cluster Name** — the name of the cluster and the blades participating in the Replication as well as their 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 36: 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
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 37: Sync State Values in MPE/MRA Replication Stats Report

Sync Status	Description	Value Displayed on the CMP	Icon Used in the User Interface
Down	The link is down and there is no current attempt to restore it.	Critical	Red "X"
DownListening	The incoming link is down awaiting the other side to initiate the connect attempt.	Critical	Red "X"
DownConnecting	The link is down by this side is trying to connect.	Critical	Red "X"
DownRejected	The link is down because a connect attempt was rejected in the "handshake" phase.	Critical	Red "X"
DownHandshake	The link is connected but not ready for application use (so it is "down" logically). The links is being validated in a "handshake" as legitimate.	Critical	Red "X"
Connected	Connected and ready for use.	Critical	Red "X"
ConnectedReinit	Connected and ready for use, but after an application error where the recovery is "start over" w/o either a link drop or a complete application restart.	Critical	Red "X"
ConnectedIncompat	Connected but the schema are incompatible and replication cannot run until (1) the schema has the needed upgrade information or (2) problematic tables are excluded from replication.	Critical	Red "X"
RegisterSent	RegisterSent means the link is exchanging application level credentials and information (such as data dictionary information). In this state, registration has been sent from one side and it is being awaited from the other side.	Critical	Red "X"
RegisterAcked	In this state, registration has been sent acknowledged from the other side. In most configurations, it is a transitory state, but the end application can hold the link in this state before permitting an "audit".	Critical	Red "X"
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" 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 database(s) 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 w/o an audit if the states of the databases allow it.	Major	Red Exclamation Mark
ActivePostAudit	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 the Sync State columns. The value for the Cluster State will be selected based on the maximum severity.

  Table 38: Priority Table in MPE/MRA Replication Stats Report

Priority	Value	Icon Used in the User Interface
1	Critical	Red "X"
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** pulldown menu. You can define filtering criteria using the following fields:

- **App Type**— Filter in all applications (the default) or filter by **MPE** or **MRA**.
- **Server Name** — Filter in all servers (the default) or one specific server.
- **Cluster Name** — Filter in all clusters (the default) or one specific cluster.

You can display the report in a format suitable for printing. Click **Printable Format**; an **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 16

Upgrade Manager

Topics:

The Upgrade Manager lets you manage upgrade files, 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 *User Management* for more information.

Before upgrading, always contact My Oracle Support. See *https://support.oracle.com* for more information.

About ISO Files on Servers

Policy Management software upgrade procedures are distributed and stored for use as ISO files, which are archive files of optical (DVD) discs. ISO files are also called ISOs. You can distribute, or "push," ISO files to either servers or clusters. ISO files contain both upgraded software and files that direct the upgrade process.

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

ISO Maintenance 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 appear in the table on this page. You can collapse or expand the display of servers by clicking the [-] or [+] icons in the first column of the table. The display is updated every ten seconds. *Figure 34: Sample ISO Maintenance Page* shows a sample **ISO Maintenance** page.

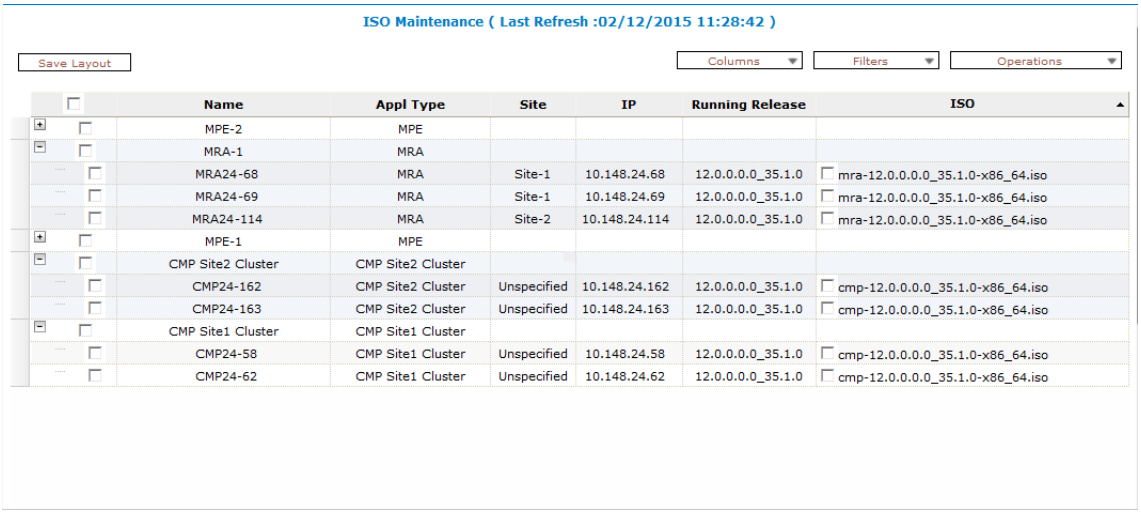


Figure 34: Sample ISO Maintenance Page

The following types of elements appear on the **ISO Maintenance** page:

- Checkboxes to select clusters or servers on which to perform operations
- The table of filtered clusters and servers
- Pulldown menus (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for selecting operations

Table 39: ISO Maintenance Page Elements describes the elements that appear on the **ISO Maintenance** page.

Table 39: 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 appears 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** pulldown menu 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** pulldown menu also lets you display **Unspecified** or **All** sites. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column. **Note:** This column only appears for a georedundant Policy Management network.
IP	Displays the OAM server IP address of each server. The **Filters** pulldown menu 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** pulldown menu 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** pulldown menu to change the columns that appear in this table. The **Name** column is mandatory. By default, all columns appear. To change which columns appear, 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** pulldown menu to select a subset of clusters and servers to appear 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 appear. 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 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 that appear in the pulldown menu depend on the state of the servers that are selected; that is, if you select more than one server, only the operations that are valid for all selected servers appear. 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 (click **OK** or **Cancel**). Once you click **OK**, the operation is performed; a progress bar displays the status of the command execution in a pop-up window. **Note:** Once an operation is confirmed, it cannot be cancelled.

Pushing a Script to a Server

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.

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
   The **ISO Maintenance** page opens.
2. Select the server(s) receiving the upgrade script.
3. Click the **Operations** pulldown menu and select **Push Script**.
   You are prompted, "Are you sure you want to execute Push Script?"
4. Click **OK** (or **Cancel** to abandon your request).
   A progress bar displays the progress of the operation.

The upgrade scripts are downloaded to the selected server(s).

Adding an ISO File to a Server

Use this procedure to load an upgrade ISO file onto a remote server for a software upgrade.

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
   The **ISO Maintenance** page opens.
2. Select the cluster(s) or server(s) to receive the ISO file.
3. Click the **Operations** pulldown menu 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. Once the process completes, the icon disappears.

The ISO file is distributed to the server(s).

Deleting an ISO File from a Server

Use this procedure to delete an ISO file from a server.

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
The **ISO Maintenance** page opens.
2. Select the cluster(s) or server(s).
3. Select the ISO file to be removed.
4. Click the **Operations** pulldown menu and select **Delete ISO**.
You are prompted, "Are you sure you want to execute Delete ISO?"
5. Click **OK** (or **Cancel** to abandon your request).
A progress bar displays the progress of this operation.

The selected ISO files are deleted from the selected cluster(s) or server(s).

About Performing an Upgrade

The information in this section is a general overview of the Upgrade Manager and the steps you take to upgrade a cluster. Specific details are provided by My Oracle Support. See *My Oracle Support (MOS)* for more information.

When you upgrade a cluster, the Upgrade Manager uses upgrade scripts to automate the process wherever possible. The Upgrade Manager performs pre-upgrade checks, monitors and reports detailed progress of an upgrade, and prevents you from specifying invalid or unnecessary operations at each step in the process (by graying out invalid operations). You control an upgrade from the **Upgrade Manager** page. The Upgrade Manager automatically handles replication, synchronization, and the order in which servers are upgraded and failed over.

During the upgrade process, the Upgrade Manager reports on the progress of the upgrade on each server.

Though the upgrade process is automated, you retain control over actions that require operator approval. You can pause an upgrade at an operator action, resume the process later at your convenience, or roll back the upgrade from that point. You can also specify optional, advanced actions. (The Upgrade Manager prevents you from selecting invalid optional actions.)

During an upgrade, the Upgrade Manager asserts (that is, generates) and displays appropriate alarms, such as when servers go out of service, and clears the alarms when appropriate, such as when servers return to service. The Upgrade Manager will also assert an alarm if an unexpected error prevents it from continuing the upgrade.

Note: An upgrade typically triggers minor, major, and critical alarms as servers are taken out of service or failed over. This is normal and to be expected.

In addition to recording all user and system upgrade activity in the audit log, the Upgrade Manager maintains a separate upgrade log so that you can track the history of an upgrade.

You can upgrade up to four MPE or MRA clusters in parallel.

Upgrade Manager Page Elements

On the **Upgrade** section of the navigation pane, **Upgrade Manager** is an option. All clusters and servers in the Policy Management network appear in the table on this page. Servers display in groups by cluster; you can collapse or expand cluster information by clicking the [-] or [+] icons in the first column of the table. The table is updated every ten seconds. *Figure 35: Sample Upgrade Manager Page* shows a sample.

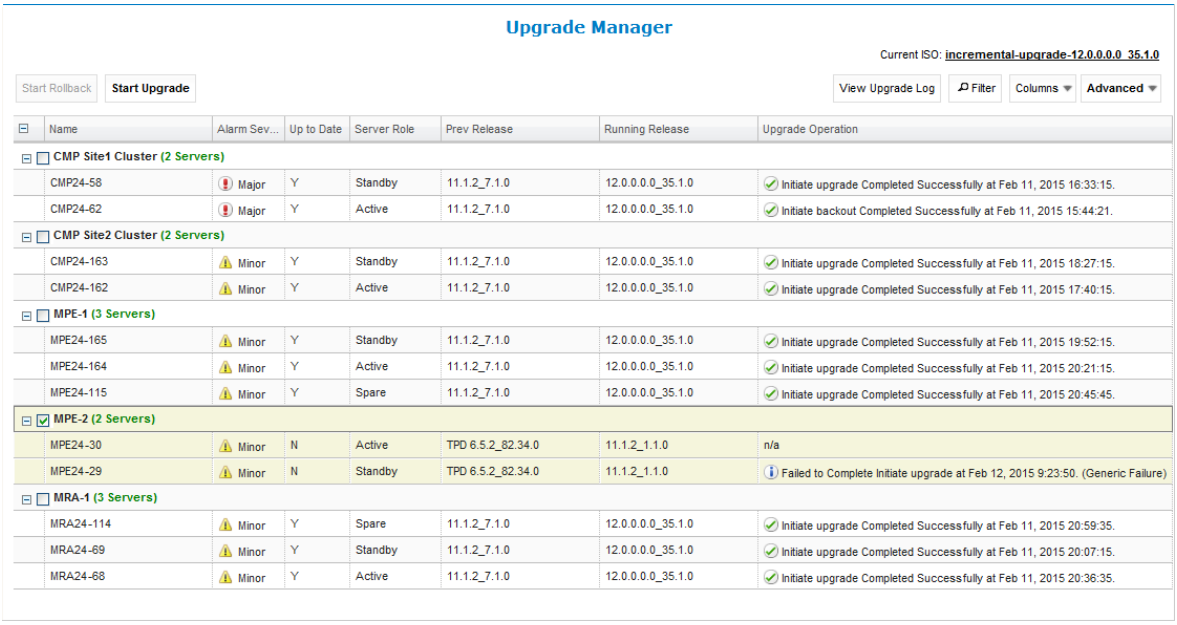


Figure 35: Sample Upgrade Manager Page

The following types of elements appear on the **Upgrade Manager** page:

- ☐ (checkboxes) to select clusters to upgrade or roll back
- Buttons (context-sensitive actions such as **Start Rollback** or **Start Upgrade**); **View Upgrade Log**; **Filter**; and the name of the current ISO
- The table of filtered clusters and servers
- Pulldown menus (**Columns** and **Advanced**) for changing what rows appear in the table and for selecting optional advanced operations, respectively

Table 40: Upgrade Manager Page Elements describes these elements.

Table 40: Upgrade Manager Page Elements

Element	Description
☐ (checkbox)	Use the ☐ (checkbox) column to select the cluster on which an operation is to be performed. All servers in the selected cluster will be affected by the operation. **Note:** You must select a cluster before you can select an operation.
Name	Displays the name of each cluster and server. You can drag the edge of the heading to resize the column.
Alarm Severity	Displays the highest level severity of alarm, if any, on the server: **Critical**, **Major**, or **Minor**. This indicates that at least one alarm of this severity has been raised on the server (there may be more than one), but none at any higher level of severity. If there are no alarms for the server, the severity is blank. You can drag the edge of the heading to resize the column. **Note:** An upgrade typically triggers minor, major, and critical alarms as servers are taken out of service or failed over. This is normal and to be expected.
Up to Date	Displays whether a server is up to date, that is, running the most recent version of Policy Management software available: • **Y** — the server is running the most recent software • **N** — the server is running a previous version of software • **n/a** — the server cannot be updated, because either the current ISO file does not apply to the server, no ISO file is loaded, or there is a problem with the server
Server Role	Displays the server's role in the cluster. You can drag the edge of the heading to resize the column. **Note:** Roles are changed automatically during the course of an upgrade or rollback. • **Active** • **Standby** • **Spare** • **Offline** — the server cannot be reached • **OOS** (out of service) — the server is in Standby mode, either because of operator action or as part of an upgrade
Prev Release	Displays the previous Policy Management software release of each server, if known. The **Filter** menu lets you display a specific release only or All releases. You can drag the edge of the heading to resize the column.
Running Release	Displays the current Policy Management software release operating on each server. The **Filter** menu lets you display servers running a specific release only or all releases. You can drag the edge of the heading to resize the column.

Element	Description
Upgrade Operation	Displays details of the last or current operation performed on each server. You can drag the edge of the heading to resize the column.
Upgrade Log	Includes a **View** button; click it to view the upgrade log for that cluster. (By default, this column is not visible.) You can drag the edge of the heading to resize the column.
View Upgrade Log	Displays an Upgrade Log window for the selected cluster.
Filter	Use the **Filter** button to select a subset of clusters or servers to appear in the table. You can filter by column(s): **Name**, **Alarm Severity**, **Up to Date**, **Server Role**, **Prev Release**, and **Running Release**. These filters are initially set to filter out nothing.
Columns	Use the **Columns** pulldown menu to change the columns that appear in the table. By default, all columns except **Upgrade Log** appear. To remove the display of a column, uncheck it.
Current ISO	Displays the upgrade procedure available, or **n/a** if no ISO file is available. If multiple ISOs are available, click on the name to select a different ISO.
Advanced	Use the **Advanced** menu to select an optional advanced upgrade operation to perform at a point of operator intervention. You must select a cluster (in the first column of the table) before you can select an optional operation. **Note:** The operations that appear in this menu depend on the current release, the cluster selected, the cluster's state, and the current state of an upgrade or rollback in progress. In some cases there may be no options available, in which case the menu is disabled. As a protective feature, when you select an optional operation, you are prompted whether 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 operation. Once you confirm an operation, it cannot be cancelled.

The actions available are determined by the Upgrade Manager based on the current release, the cluster you select, the cluster's current state, and its upgrade status. Invalid actions are disabled (grayed out). For example, in *Figure 35: Sample Upgrade Manager Page*, **Start Upgrade** is a valid action for the selected cluster, but **Start Rollback** is not. Common actions include the following:

- **Start Upgrade** (once a new ISO file is available)
- **Continue Upgrade** (when the upgrade process has reached a point of user intervention)
- **Start Rollback** (once a system is upgraded)
- **Continue Rollback** (when the rollback process has reached a point of user intervention)

You should normally be able to complete an upgrade by clicking only **Start Upgrade** and **Continue Upgrade**.

Selecting an ISO for Upgrade

You must distribute an ISO file beforehand to all servers that will use it (see *Adding an ISO File to a Server*). Once distributed, you must select the ISO file to use in an upgrade before beginning the process. If you have multiple ISO files available for an upgrade (for example, if you have a major version and an update version, or an update version and a patch), you can select which one to use. If you have multiple clusters to upgrade, you only have to select the ISO file once.

To select an ISO:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** page appears.
2. Click on the name of the file listed as the current ISO (which may appear as "**Install Kit**").
   The **Select ISOs** window opens, listing the available ISO file(s).
3. (Optional) You can click on a column heading to sort the rows on that column. You can click **Filter** to filter out rows based on the data in one or more columns. You can click the **Columns** pulldown menu to select which columns are displayed (by default, all columns are displayed). You can resize columns.
4. Select which ISO file to use and click the **Select** button at the bottom of the window.

   You are prompted, "Loading this ISO will cause the upgrade manager to abandon the current upgrade and start a new one. Are you sure you want to continue loading this ISO?" Click **OK** (or **Cancel** to discard your request).

   The **Select ISOs** window closes, and the selected ISO file is listed as the current ISO.

The ISO file is selected, and you can now use it to upgrade clusters.

Upgrading the Primary-site CMP Cluster

If you are upgrading an entire Policy Management network, you must upgrade the primary-site CMP cluster (designated "CMP Site1 cluster") first. This upgrade procedure is different from the upgrade procedure for other clusters because you must use the Upgrade Manager for Version 11.1 to install Version 12. Once a primary-site CMP server is running Version 12 software, you can use the procedures described in this chapter to upgrade the remaining Policy Management systems.

Note: Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this version, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

Caution: Once you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

Before upgrading the primary-site CMP cluster:

1. Use **Delete ISO** to remove any old upgrade files from all servers in the Policy Management network.
2. Use **Upload ISO** to distribute the upgrade ISO file to all servers in the Policy Management network.

To upgrade the primary-site CMP cluster:

1. Log in to the active server of the primary-site CMP cluster as **`root`**.
   The system displays the root-level prompt (#).

2. Enter the command **`mount -o loop /var/TKLC/upgrade/`*`iso_name`*` /mnt/upgrade`** (where *iso_name* is the name of the ISO file).
   The ISO file is mounted.
3. Enter the command **`cp /mnt/upgrade/upgrade/policyScripts/*.pl /opt/camiant/bin`**.
   Script files are copied to the target directory on the active server.
4. Enter the command **`umount /mnt/upgrade`**.
   The ISO file is unmounted.
5. Enter the command **`qpSSHKeyProv.pl -prov`**.
   SSH keys for the account **`admusr`** are provisioned on the active server.

   Note: This step is always required.

6. Enter the command **`logout`**.
   You are logged out of the active server.
7. Log in to the active CMP server as an administrator with upgrade privileges.
   You have access to the **Upgrade Manager** menu in the navigation pane.
8. From the **Upgrade Manager** section of the navigation pane, select **System Maintenance**.
   The **System Maintenance** page opens.
9. Select all servers, and from the **Operations** pulldown menu select **Push Script**.
   You are prompted, "Are you sure you want to execute Push Script?"
10. Click **OK** (or **Cancel** to discard your request).
    Upgrade scripts are distributed to all servers.
11. Select the standby server of the **CMP Site1 Cluster**, and from the **Operations** pulldown menu, select **Force Standby**.
    You are prompted, "Are you sure you want to execute Force Standby?"
12. Click **OK** (or **Cancel** to discard your request).
    The server's state changes to **Force Standby**.
13. Select the forced standby server of the **CMP Site1 Cluster**, and from the **Operations** pulldown menu, select **Start Upgrade**.
    You are prompted, "CAUTION! Please make sure the remote server is not being either Upgraded or Backed-out at this moment!"
14. Click **OK** (or **Cancel** to discard your request).
    The server is upgraded, restarts, and rejoins the cluster.

    Note: This process, which involves disk repartition, can take 40 minutes or more, depending on the amount of data on the server. Wait for the server to rejoin the cluster before proceeding.

15. Select the primary (**CMP Site1 Cluster**) site, and from the **Operations** pulldown menu, select **Switch ForceStandby**.
    You are prompted, "Are you sure you want to execute Switch ForceStandby?"
16. Click **OK** (or **Cancel** to discard your request).
    The forced standby server becomes the active server and the active server becomes forced standby.
    You are logged out of the CMP system.
17. Log in to the active (upgraded) CMP server as an administrator with upgrade privileges.
    You have access to the **Upgrade** menu in the navigation pane.
18. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
    The **Upgrade Manager** page opens.
19. Click the current ISO.
    The **Select ISOs** window opens.

20. Select the version 12.0 ISO and click **Select ISO**.
    You are prompted, "Loading this ISO will cause the upgrade manager to abandon the current upgrade and start a new one. Are you sure you want to continue loading this ISO?"
21. Click **OK** (or **Cancel** to discard your request).
    The ISO is selected for upgrade. The data in the **Up to date** column changes, and the alarms SYSTEM_MIXED_VERSION and CLUSTER_MIXED_VERSION are asserted.
22. Select the primary (Site1) cluster.
    The **Continue Upgrade** button becomes available.
23. Click **Continue Upgrade**.
    You are prompted, "Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)"
24. Click **OK** (or **Cancel** to discard your request).
    The remaining CMP system is upgraded. When the alarm CLUSTER_MIXED_VERSION is cleared, the upgrade is complete.

The primary-site CMP cluster is upgraded. You must now upgrade the secondary (Site2) CMP cluster, using the Version 12.0 Upgrade Manager as described in the rest of this chapter, before you can upgrade any other Policy Management clusters. Once all CMP clusters are upgraded, you can upgrade the remaining clusters of the Policy Management network.

Upgrading a Cluster

Before upgrading any cluster in the Policy Management network:

1. Use **Delete ISO** to remove any old upgrade files from remote servers.
2. Use **Upload ISO** to distribute upgrade ISO files to remote servers.
3. Use **Push Script** to distribute upgrade script files to remote servers.

If you are upgrading an entire Policy Management network, you must upgrade the primary-site CMP cluster first, then the secondary-site CMP cluster (if present). See *Upgrading the Primary-site CMP Cluster*.

The default, preferred sequence followed by the Upgrade Manager to upgrade a georedundant (three-server) cluster is as follows:

1. Upgrade the standby server
2. Fail over to the standby server
3. Reapply the configuration to the cluster
4. Upgrade the remaining server in the primary site
5. Upgrade the spare server

An optional action lets you change this order if required. You can also upgrade the second and third server in the cluster simultaneously.

The default, preferred sequence followed by the Upgrade Manager to upgrade a two-server cluster is as follows:

1. Upgrade the standby server
2. Fail over to the standby server
3. Reapply the configuration to the cluster
4. Upgrade the remaining server

You can upgrade up to four MPE or MRA clusters in parallel. (You must manually start the process for each cluster.)

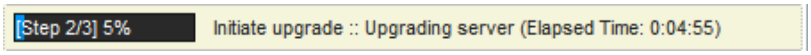
You can roll back from an upgrade from any point of operator intervention. Whenever the action **Continue Upgrade** is available, the action **Start Rollback** is also available.

Caution: Once you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

To upgrade a georedundant cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** page opens.
2. Select the cluster to be upgraded and click **Start Upgrade**.
   You are prompted, "Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)"
3. Click **OK** to continue (or **Cancel** to abandon your request).

   The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the standby server, in the primary site. The **Upgrade Operation** column displays the progress of the action; for example:

   Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

   When the standby server is upgraded, the **Upgrade Operation** column displays the message "Initiate upgrade Completed Successfully at *date_time*." Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

   Tip: Review alarms associated with each action before proceeding with the next action.

4. Select the cluster again and click **Continue Upgrade**.
   You are prompted, "Are you sure that you want to perform this action? Failover to new version *cluster_name* (next)"
5. Click **OK** to continue (or **Cancel** to stop the upgrade at this point).

   If you stop an upgrade at a point of operator intervention, you can resume it later, or roll it back from there.

   The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.
6. Reapply the configuration to the cluster:

   - (For an MPE cluster) From the **Policy Server** section of the navigation pane, select **Configuration**, select the cluster, and in the **Policy Server Administration** page, click **Reapply Configuration**.
   - (For an MRA cluster) From the **MRA** section of the navigation pane, select **Configuration**, select the cluster, and in the **MRA Administration** page, click **Reapply Configuration**.

   The configuration information is synchronized.
7. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** page opens.

8. Select the cluster again and click **Continue Upgrade**.
   You are prompted, "Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)"
9. Click **OK** to continue (or **Cancel** to stop the upgrade at this point).

   The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the second server in the primary site. The **Upgrade Operation** column displays the progress of the current action.

   When the second server is upgraded, the **Upgrade Operation** column displays the message "Initiate upgrade Completed Successfully at *date_time*."
10. Select the cluster again and click **Continue Upgrade**.
    You are prompted, "Are you sure that you want to perform this action? Initiate upgrade *server_name* (next)"
11. Click **OK** to continue (or **Cancel** to stop the upgrade at this point).

    The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the spare server, in the secondary site. The **Upgrade Operation** column displays the progress of the current action.

    When the spare server is upgraded, the **Upgrade Operation** column displays the message "Initiate upgrade Completed Successfully at *date_time*." Alarm 70501 is cleared.

The cluster is upgraded. For each server, the **Prev Release** column displays the release installed before the upgrade, and the **Up to Date** column displays "Y" (yes).

If the upgrade fails, a diagnostic message describes the problem. Try the upgrade again; if it fails again, contact My Oracle Support.

Note: If the upgrade fails and also leaves a server in an unrecoverable state (designated "Zombie" in the **Upgrade Operation** column, plus alarm 70508), the Upgrade Manager cannot resolve the issue. Contact My Oracle Support immediately.

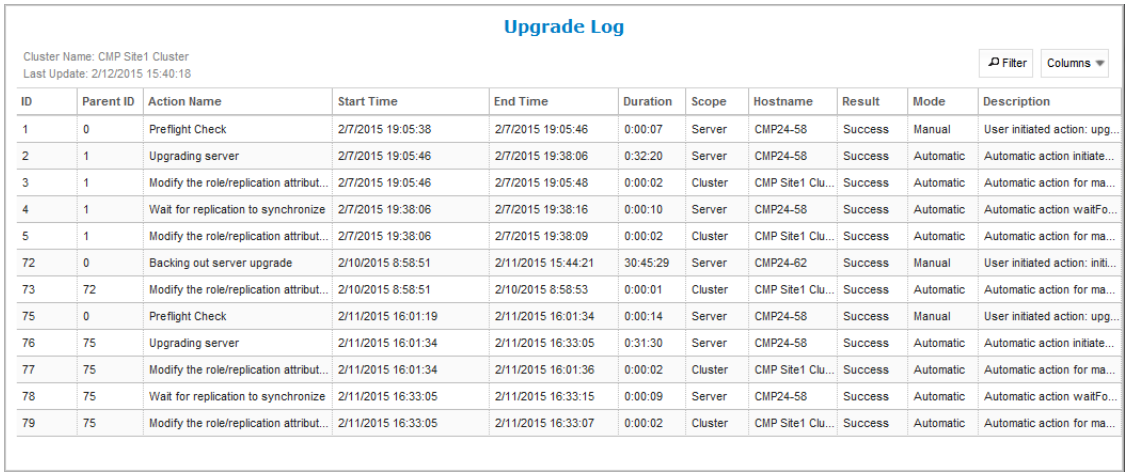
Viewing the Upgrade Log

You can view the upgrade log for an individual cluster. The log includes both automatic and manual actions taken during an upgrade. To view the upgrade log:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** window opens.
2. Select the cluster and then click **View Upgrade Log**.
   The **Upgrade Log** window opens.

The upgrade log is displayed. *Figure 36: Sample Upgrade Log* shows a sample upgrade log.

You can click on a column heading to sort the log on that column. You can drag the end of a heading to resize the column. You can click **Filter** and filter the rows on a value in any column. You can click **Columns** and select which columns appear in the log.



Upgrade Log

Cluster Name: CMP Site1 Cluster
Last Update: 2/12/2015 15:40:18

Filter | Columns

ID	Parent ID	Action Name	Start Time	End Time	Duration	Scope	Hostname	Result	Mode	Description
1	0	Preflight Check	2/7/2015 19:05:38	2/7/2015 19:05:46	0:00:07	Server	CMP24-58	Success	Manual	User initiated action: upg...
2	1	Upgrading server	2/7/2015 19:05:46	2/7/2015 19:38:06	0:32:20	Server	CMP24-58	Success	Automatic	Automatic action initiate...
3	1	Modify the role/replication attribut...	2/7/2015 19:05:46	2/7/2015 19:05:48	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
4	1	Wait for replication to synchronize	2/7/2015 19:38:06	2/7/2015 19:38:16	0:00:10	Server	CMP24-58	Success	Automatic	Automatic action waitFo...
5	1	Modify the role/replication attribut...	2/7/2015 19:38:06	2/7/2015 19:38:09	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
72	0	Backing out server upgrade	2/10/2015 8:58:51	2/11/2015 15:44:21	30:45:29	Server	CMP24-62	Success	Manual	User initiated action: initi...
73	72	Modify the role/replication attribut...	2/10/2015 8:58:51	2/10/2015 8:58:53	0:00:01	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
75	0	Preflight Check	2/11/2015 16:01:19	2/11/2015 16:01:34	0:00:14	Server	CMP24-58	Success	Manual	User initiated action: upg...
76	75	Upgrading server	2/11/2015 16:01:34	2/11/2015 16:33:05	0:31:30	Server	CMP24-58	Success	Automatic	Automatic action initiate...
77	75	Modify the role/replication attribut...	2/11/2015 16:01:34	2/11/2015 16:01:36	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...
78	75	Wait for replication to synchronize	2/11/2015 16:33:05	2/11/2015 16:33:15	0:00:09	Server	CMP24-58	Success	Automatic	Automatic action waitFo...
79	75	Modify the role/replication attribut...	2/11/2015 16:33:05	2/11/2015 16:33:07	0:00:02	Cluster	CMP Site1 Clu...	Success	Automatic	Automatic action for ma...

Figure 36: Sample Upgrade Log

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. The overall sequence is the reverse of the upgrade sequence:

1. Roll back MPE and MRA clusters.
2. Roll back all CMP systems except for the last CMP server. (You cannot begin this operation until all MPE and MRA clusters are rolled back.)
3. Using the version 11.1 **System Maintenance** page, roll back the last CMP server.

In the same way that you can roll back from an upgrade from any point of operator intervention, you can also upgrade from a rollback from any point of operator intervention. Whenever the action **Continue Rollback** is available, the action **Resume Upgrade** is also available.

Rolling Back an Upgrade

The default, preferred sequence followed by the Upgrade Manager to roll back a georedundant (three-server) cluster is as follows:

1. Roll back the spare server
2. Roll back the standby server
3. Fail over to the standby server
4. Reapply the configuration to the cluster
5. Roll back the remaining server

An optional advanced action lets you change this order if required. You can also roll back the second and third server in the cluster simultaneously.

The default, preferred sequence followed by the Upgrade Manager to roll back a two-server cluster is as follows:

1. Roll back the standby server
2. Fail over to the standby server

3. Reapply the configuration to the cluster
4. Roll back the remaining server

You can roll back up to four MPE or MRA clusters in parallel. (You must manually start the process for each cluster.)

Note: Before beginning a rollback, contact My Oracle Support and inform them of your plans.

Caution: By default, the rollback process does not preserve the state of in-memory subscriber session data, including sessions stored on MPE devices and bindings stored on MRA devices, that existed when the rollback began. However, the Upgrade Manager includes an optional advanced operation to minimize the loss of in-memory subscriber session data. If you wish to preserve session data, choose this operation before rolling back the last server in a cluster.

To roll back a georedundant cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** page opens.
2. Select the cluster to be rolled back and click **Start Rollback**.
   You are prompted, "Are you sure that you want to perform this action? Initiate backout *server_name* (back)"
3. Click **OK** to continue (or **Cancel** to abandon your request).

   The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the spare server, in the secondary site. The **Upgrade Operation** column displays the progress of the current action.

   Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

   When the spare server is rolled back, the **Upgrade Operation** column displays the message "Initiate backout Completed Successfully at *date_time*." Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

   Tip: Review alarms associated with each action before proceeding with the next action.

4. Select the cluster again and click **Continue Rollback**.
   You are prompted, "Are you sure that you want to perform this action? Initiate backout *server_name* (back)"
5. Click **OK** to continue (or **Cancel** to stop the rollback at this point).

   If you stop a rollback at a point of operator intervention, you can continue it later, or resume upgrading it from there.

   The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the standby server, in the primary site. The **Upgrade Operation** column displays the progress of the current action. When the standby server is rolled back, the **Upgrade Operation** column displays the message "Initiate backout Completed Successfully at *date_time*."
6. Select the cluster again and click **Continue Rollback**.
   You are prompted, "Are you sure that you want to perform this action? Failover to old version *cluster_name* (next)"
7. Click **OK** to continue (or **Cancel** to stop the rollback at this point).
   The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.
8. Reapply the configuration to the cluster:

- (For an MPE cluster) From the **Policy Server** section of the navigation pane, select **Configuration**, select the cluster, and in the **Policy Server Administration** page, click **Reapply Configuration**.
- (For an MRA cluster) From the **MRA** section of the navigation pane, select **Configuration**, select the cluster, and in the **MRA Administration** page, click **Reapply Configuration**.

The configuration information is synchronized.

9. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** page opens.
10. (Optional) If you wish to preserve in-memory subscriber session data, select the cluster again and from the **Advanced** pulldown menu, select **Preserve SSDP *cluster_name* (back) (Optional)**.
    In the **Upgrade Operation** column, the active server displays the progress of exporting data; when that step is completed it displays the message "Preserve SSDP Completed Successfully at *date_time*." Then the standby server displays the progress of importing data; when that step is completed it displays the message "Import SSDP Completed Successfully at *date_time*." Then the cluster automatically fails over to the old version.
11. Select the cluster again and click **Continue Rollback**.
    You are prompted, "Are you sure that you want to perform this action? Initiate backout *server_name* (back)"
12. Click **OK** to continue (or **Cancel** to stop the rollback at this point).

    The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then rolls back the remaining server, in the primary site. The **Upgrade Operation** column displays the progress of the current action.

    When the remaining server is rolled back, the **Upgrade Operation** column displays the message "Initiate backout Completed Successfully at *date_time*." Alarm 70501 is cleared.

The cluster is rolled back to the previous release. For each server, the **Running Release** column displays the release to which you rolled the system back, and the **Up to Date** column displays "N" (no).

If the rollback fails, a diagnostic message describes the problem. Try the rollback again; if it fails again, contact My Oracle Support.

Note: If the rollback fails and also leaves a server in an unrecoverable state (designated "Zombie" in the **Upgrade Operation** column, plus alarm 70508), the Upgrade Manager cannot resolve the issue. Contact My Oracle Support immediately.

Rolling Back the Primary-site CMP Cluster

If you are rolling back an entire Policy Management network, you must roll back the primary-site CMP cluster (designated "CMP Site1 cluster") last. This rollback procedure is different from the rollback procedure for other clusters because you must use the Upgrade Manager for Version 11.1 to roll back the last Version 12 CMP system.

Note: You cannot begin this operation until all other Policy Management clusters are rolled back.

Note: Before beginning a rollback, contact My Oracle Support and inform them of your plans.

To roll back the primary-site CMP cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.
   The **Upgrade Manager** page opens.
2. Select the primary-site CMP cluster (the CMP Site1 cluster) and click **Start Rollback**.

You are prompted, "Are you sure that you want to perform this action? Initiate backout *server_name* (back)"

3. Click **OK** to continue (or **Cancel** to abandon your request).

   The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the standby server. The **Upgrade Operation** column displays the progress of the current action.

   Note: The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

   When the standby server is rolled back, the **Upgrade Operation** column displays the message "Initiate backout Completed Successfully at *date_time*." Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

   Tip: Review alarms associated with each action before proceeding with the next action.

4. Verify that all CMP servers except the active server are rolled back.
5. Select the cluster again and click **Continue Rollback**.
   You are prompted, "Are you sure that you want to perform this action? Failover to old version *cluster_name* (next)"
6. Click **OK** to continue (or **Cancel** to stop the rollback at this point).
   The confirmation window closes and the cluster fails over to the standby server, which becomes the active server. You are logged out of the CMP system.

   Note: The active server will be running Version 11.1.

7. Log in to the active CMP server as an administrator with upgrade privileges.
   You have access to the **Upgrade Manager** menu in the navigation pane.
8. From the **Upgrade Manager** section of the navigation pane, select **System Maintenance**.
   The **System Maintenance** page opens.
9. Select the last CMP server and from the **Operations** pulldown, select **Other Operations > Backout**.
   You are prompted, "Are you sure you want to execute Backout?"
10. Click **OK** to continue (or **Cancel** to abandon your request).
    The last CMP server is backed out.
11. When the backout is marked complete, select the last CMP server and from the **Operations** pulldown, select **Other Operations > Cancel Force Standby**.
    You are prompted, "Are you sure you want to execute Cancel Force Standby?"
12. Click **OK** to continue (or **Cancel** to abandon your request).
    The confirmation window closes and the forced standby state is canceled. The **Server State** column displays the server state as "Standby."

The CMP cluster is rolled back to the previous release.

If the rollback fails, a diagnostic message describes the problem. Try the rollback again; if it fails again, contact My Oracle Support.

Note: If the rollback fails and also leaves a server in an unrecoverable state (designated "Zombie" in the **Upgrade Operation** column, plus alarm 70508), the Upgrade Manager cannot resolve the issue. Contact My Oracle Support immediately.

Chapter 17

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, 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 **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. When you finish, click **Save** (or **Cancel** to discard your changes).
   The **Precedence Range Configuration** page closes.

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, and 301–4,294,967,295.

Range changes do not automatically cause deployed rules to be redeployed with new precedence values. Also, range changes do not automatically cause revalidation 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. See *Importing an XML File to Input Objects* for more information.

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. When you finish, click **Save** (or **Cancel** to discard your changes).
   The **UE-Initiated Procedures** page closes.

The UE-initiated attributes are configured.

Setting Stats Settings

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

To change stats settings, 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 **Stats Settings** folder.
   The **Stats Settings** page opens in the work group area.
3. Click **Modify**.
   The fields become editable.
4. Enter values for the configuration attributes:
   a) **Stats Reset Configuration** — From the pulldown menu, select **Manual** or **Interval**. 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. When configured for Interval mode, numeric values are reset at regular intervals, controlled by the Stats Collection Period variable. In 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.
   b) **Stats Collection Period** — When the Stats Reset Configuration variable is set to Interval, specify the time interval after which stats are written to the Policy Management devices. Options are 5, 10, 15, 20, 30, and 60 minutes. The default value is 15.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

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

The **Stats Settings** page closes.

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 **Modify Quota Settings** page opens.
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 and/or pool entity states.

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/time value of a pass to be extended to match a later expiration date/time value of a pass that has the same name or is in the same pass group.

5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The **Quota Settings** page closes.

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 pulldown 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 pulldown list. The default is **Disable**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The **eMPS ARP Settings** page closes.

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. Once 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** (or **Cancel** to cancel your changes). the PDN APN suffix is added to the list.

The 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 20 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** (or **Cancel** to discard your changes).
   Subscriber tracing is enabled.

Configuring Custom APNs

Custom Access point name (APN) configuration on the MPE device, when the setting is set to "true", overrides the behavior of the DIAMERTER.ENF.AFDirectReply setting on a "per APN" basis.

When the DIAMERTER.ENF.AFDirectReply setting is set to "true", all Rx processing can be synchronous for specific APNs.

The **Custom APNs Configuration** display has three screens:

- **Synchronous APNs**
- **Session Recovery APNs**— allows a session recovery.
- **Session Synch APNs**—allows you to enable/disable "Gx Session-Sync" on a "per APN per MPE" basis.

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Custom APNs Configuration** folder.
3. Click **Modify**.
4. Managing Synchronous APNs
   a) On the **Custom APNs Configuration** page, select the **Synchronous APNs** section.
   b) Enter a **Synchronous APN** (for example, **`xyz1.oracle.com`**).
   c) Click **Add** to add the new APN to the list. To delete an APN, highlight the APN in the list and click **Delete**.
   d) Click **Save** (or **Cancel** to cancel your changes).
5. Managing Synchronous APNs
   a) On the **Custom APNs Configuration** page, select the **Session Recovery APNs**section.

b) Enter the name of the **Session Recovery APN**.
c) Click **Add** to add the session recover APN. To delete a Session Recovery APN, highlight the APN in the list and click **Delete**.

6. Adding a Session Synch APN

a) On the **Custom APNs Configuration** page, select the **Session Synch APNs**section.
b) Enter a **Session Synch APN**.
c) Click **Add**. To delete a Session Synch APN, highlight the APN in the list and click **Delete**.

Chapter 18

System Administration

Topics:

System Administration describes functions reserved for CMP system administrators.

Note: Some options are visible only when you are logged in with administrative rights to the CMP system. However, the **Change Password** option is available to all users.

Configuring System Settings

Within the CMP system you can define the settings that control system behavior.

To define system settings:

1. From the **System Administration** section of the navigation pane, select **System Settings**.
   The **System Settings** page opens in the work area, displaying the current system settings.
2. Click **Modify**.
   The **System Settings** page opens.
3. In the **Configuration** section, define the following:
   a) **Idle Timeout (minutes; 0=never)** — The interval of time, in minutes, that a session is kept alive.
      The default value is 30 minutes; a value of zero indicates the session remains active indefinitely.
   b) **Account Inactivity Lockout (days; 0=never)** — The maximum number of days since the last successful login after which a user is locked out.
      If the user fails to log in for the defined number of days, the user is locked out and cannot gain access to the system until an administrator resets the account. The default value is 21 days; a value of zero indicates no limit (the user is never locked out for inactivity).
   c) **Maximum Concurrent Sessions Per User Account (0=unlimited)** — The maximum number of times a defined user can be logged in simultaneously. A value of zero indicates no limit.
      If more than the configured number of concurrent users try to log in (for example, a second user if this value is set to 1), they are blocked at the login page with the message "Your account already has the maximum number of concurrent sessions."
   d) **Password Expiration Period (days; 0=never)** — The number of days a password can be used before it expires. Enter a value from 7 to 365, or 0 to indicate that the password never expires.
   e) **Password Expiration Warning Period (days; default=3)** — The number of days before a password expires to begin displaying a window to users after login warning that their password is expiring.
   f) **Admin User Password Expiration** — By default, the password for the admin user never expires.
      If you select this option, the **admin** user is subject to the same password expiration policies as other users.
   g) **Block users when password expires** — By default, once a password expires, the user must immediately change it at the next login.
      If you select this option, if their password expires, users cannot log in at all. (If you select **Admin User Password Expiration** and the **admin** user's password expires, the user can still log in but must immediately select a new password.)
   h) **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 GUI menu. 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; clear the check box to disable this feature.

   b) **Invalid Login Threshold Value** — Defines the maximum number of consecutive failed logins after which action is taken.

      Enter a value from 1 through 500; the default is 3 attempts.

   c) **Action(s) 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 letter(s) (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 letter(s) (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 numeral(s) (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 character(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 nonalphabetic characters in their passwords.
   - **Force users with weak password to change password at their next login** — By default, this setting is 0 (disabled). Select it to require users to conform to a new password policy effective the next time they log in.

6. When you finish, click **Save** (or **Cancel** to discard your changes).

The system settings are configured.

Figure 37: 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.

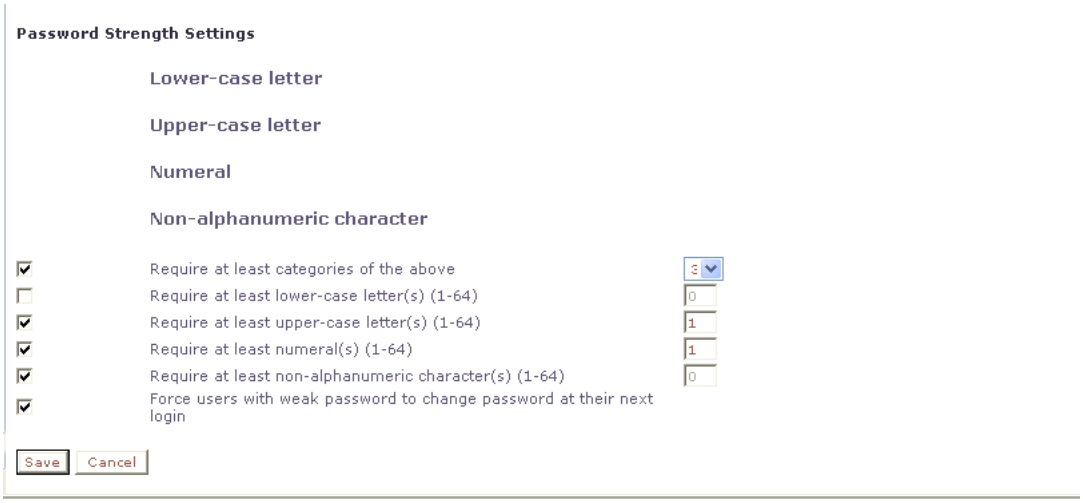


Figure 37: Sample Password Strength Policy

Importing to and Exporting from the CMP Database

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.

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
- **AVP definitions** — Allows you to define, save, and restore third-party AVP definitions within the system
- **Policy Tables** — Allows you to export policy tables, and import them to add, edit, replace or delete a table

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

Importing an XML File to Input Objects

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

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

Note: Export the existing database of objects before starting an import operation to ensure that you can recreate the previous state if necessary (see *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, or click **Browse** and, from the standard file open window that appears, locate it.
3. Select what to import:

   - * (specifies import all types) (default value)
   - **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**
   - **Policy Table**
   - **Applications**
   - **Roles**
   - **Scopes**
   - **Users**

   If you select **Network Elements**, additional filtering fields appear to help you manage the volume of data being imported. You can filter by network element name 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 appears. You can specify up to six logical combinations of filtering statements.

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

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

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

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

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

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** (the 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**
- **Applications**
- **Roles**
- **Scopes**
- **Users**

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 appear 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 operators **AND**, **OR**, **AND NOT**, or **OR NOT**; if you select an operator, an additional statement field appears. You can specify up to six logical combinations of filtering statements.

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

3. Click **Export**.
   A standard file download window opens, and you are prompted, "Do you want to open or save this file?"
4. Click **Save** to save the file (or **Cancel** to abandon the request).
   Data exported to an XML file. If the operation takes more than five seconds, a progress bar appears.

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

The Manager Report

The Manager Report provides information about the CMP cluster itself. This information is similar to the Cluster Information Report for MPE and MRA clusters. The display is refreshed every ten seconds.

To view the Manager Report, select **Reports** from the **System Administration** section of the navigation pane.

The fields that are displayed in the Manager Report section include the following:

- **Cluster Name and Designation** — The name of the cluster, and also whether it is the primary (P) or secondary (S) site.
- **Cluster Mode** — The status of the cluster:
  - **Active**: The cluster is managing the Policy Management network.
  - **Standby**: The cluster is not currently managing the Policy Management network.

  To pause refreshing the display, click **Pause**. To resume refreshing, click **Resume**. To reset the display counters, click **Reset All Counters**.

- **Cluster Status** — The status of the servers within the cluster:
  - **On-line**: If one server, it is active; if two servers, one is active and one is standby.
  - **Degraded**: One server is active, but the other server is not available.
  - **Out-Of-Service**: Neither server is active.
  - **No Data**: The CMP system cannot reach the server.

Also within the Manager Report is a listing of 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, or Forced-Standby), number of server (blade) failures, and total uptime (time providing active or standby GUI service). For the definitions of these states, see *Server Status*.
- **Utilization** — Displays the percentage utilization of disk (of the /var/camiant filesystem), average value for the CPU utilization, and memory.

The **Actions** buttons let you restart the CMP software on the server or restart the server.

The Trace Log

The Trace Log is part of system administration records notifications for management activity on the CMP system. For information on configuring the severity level of messages written to the Trace Log, see *Configuring Log Settings*.

To view log information using the Trace Log Viewer:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The **Trace Log** page opens in the work area.
2. Click **View Trace Log**.

   The **Trace Log Viewer** window opens. While data is being retrieved, the in-progress message "Scanning Trace Logs" appears.

   All events contain the following information:

   - **Date/Time** — Event timestamp. This time is relative to the server time.
   - **Code** — The event code. For information about event codes and messages, see the *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.

   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** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.
- **First/Last** — Once the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.

3. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search**.
   The trace log for the selected server displays.
4. To filter the log, see *Filtering the Trace Log*.
5. When you finish, click **Close**.
   The **Trace Log Viewer** window closes.

When you are finished viewing the trace log, 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 different fields.

To filter the log information using the Trace Log Viewer:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The **Trace Log** page opens in the work area.
2. Click **View Trace Log**.
   The **Trace Log Viewer** window opens. While data is being retrieved, the in-progress message "Scanning Trace Logs" appears.
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 Code(s)** — 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 the server not the CMP system time.
   - **Severity** — Select the lowest level message to include in the log. All message levels above the message level selected are included in the log.
   - **Contains** — Specify a character string to search for in the message field of the log. This field does not use wildcards and is not case specific.
   - **Trace Code(s)** — 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. For example, if you enter "connection," all events containing the word "connection" appear.

  Note: The **Start Date/Time** setting overrides the **Contains** setting. For example, if you search for events happening this month, and search for a string that appeared in events last month and this month, only results from this month appear.

5. Click **Search**.
   The filtered log displays.
6. When you finish, click **Close**.
   The **Trace Log Viewer** window closes.

Configuring the Trace Log

You can configure the severity level of messages written to the Trace Log.

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The **Trace Log** page opens in the work area.
2. Click **Modify**.
   The **Modify Trace Log Settings** page opens.
3. Select the Trace Log Level.

   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: 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 could cause you to miss important notifications.

4. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Trace log level is set.

Viewing the Audit Log

You can track and view configuration changes within the CMP system. Using the audit log, you can track and monitor each configuration event, affording you better system control. The audit log is stored in the database, so it is backed up and can be restored.

To display the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. On the **Audit Log** page, click **Show All**.
   The Audit Log opens. (*Figure 38: Audit Log* shows an example.)

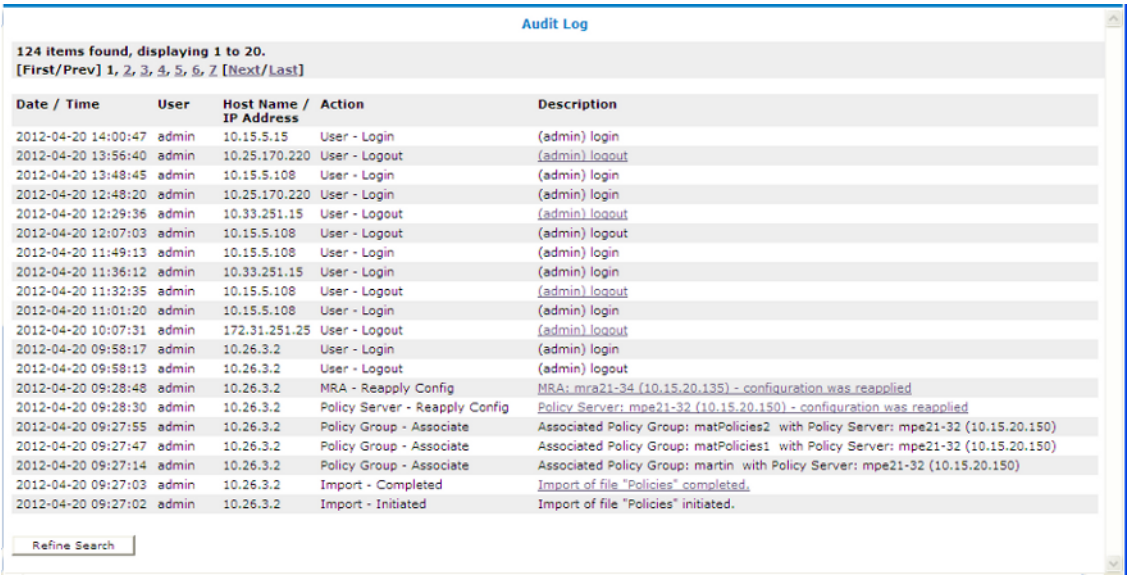


Figure 38: Audit Log

For a detailed description of an item, click the underlined description. The details of the event display. (*Figure 39: 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*.)

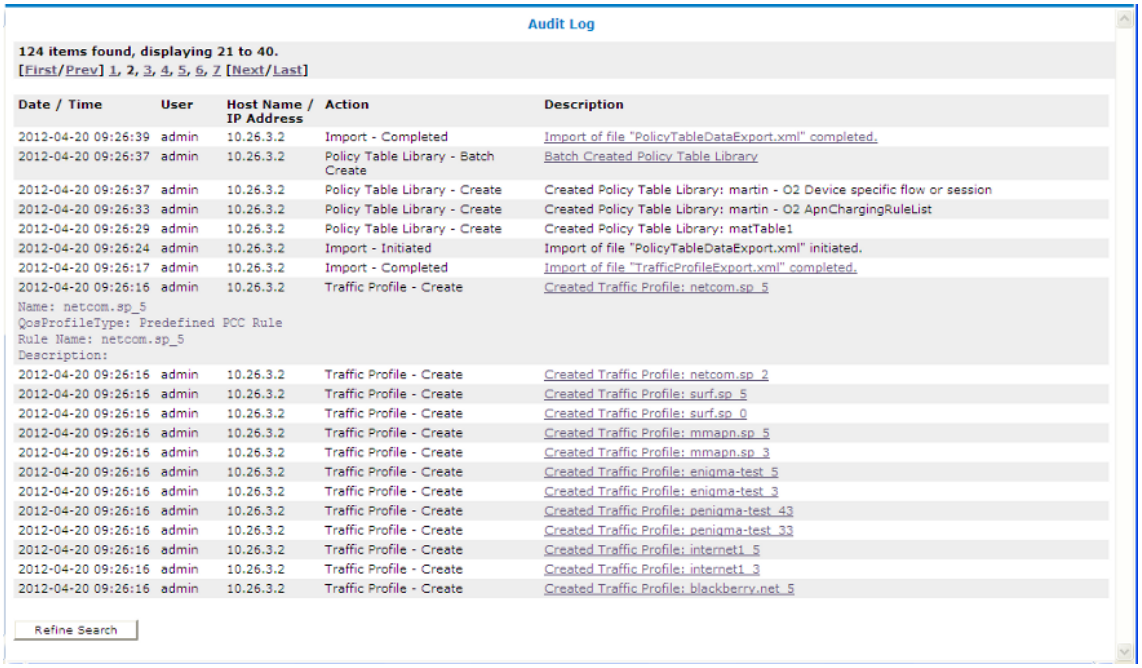


Figure 39: Audit Log Details

Searching for Audit Log Entries

To search for entries in the Audit Log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. Click **Search**.
   The **Audit Log Search Restrictions** page opens.
3. Define the following items, depending on how restrictive you want the audit log search to be:
   - **From/To** — Enter the start and end dates and times for this search.
   - **Action by User Name(s)** — Enter the name of the user or users to audit.
   - **Action on Policy Server(s) / MRA(s)** — Enter the name of the Policy Management device to audit.
   - **Audit Log Items to Show** — Specifies a category of items to audit for display:
     - **Policy Server**
     - **Network Element**
     - **Network Element Group**
     - **Application**
     - **MRA**
     - **Policy**
     - **Policy Group**
     - **Account**
     - **Tier**
     - **Entitlement**

- **Alert**
- **User**
- **Audit**
- **Alarm**
- **OM Statistics**
- **Quota**
- **Quota Convention**
- **Charging Server**
- **Service**
- **Rating Group**
- **Time Period**
- **MPE Manager**
- **Upgrade Manager**
- **Topology Setting**
- **Global Configuration Settings**
- **Trending Report**
- **User Layout**
- **Upsync Log Alarm Threshold**

When you select some categories, a **Name** field appears, which lets you enter a search string; leave the field blank to include all items. When you select any category, an **Action(s)** link appears, which lets you select individual audit log items within the category. By default all items in the category are selected, but you can select individual items instead. By default you can specify three item categories; click **More Lines** to add an additional item category.

- **Results Forms** — Specifies the number of items per page to display, along with which data to display (most recent or oldest items).

4. When you finish defining the search parameters, click **Search**.
   The Audit Log displays search results.

Exporting or Purging Audit Log Data

You can export the audit log to a text file; the default filename is `AuditLogExport.txt`.

Exporting Audit Log Data

You can export audit log data to a text file. The filename is `AuditLogExport.txt`.

To export data from the audit logs:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. Click **Export/Purge**.
   The **Export and Purge Audit Log Items** page opens.
3. In the **Items to Export** section, select one of the following options:
   a) **Export All Items** — Writes all audit log entries.
   b) **Export Through Date** — Click (calendar icon), and select a date.

4. When you finish, click **Export**.
   A standard File Download window opens; you can open or save the export file.

The audit log is exported.

Purging Audit Log Data

To purge data from the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. Click **Export/Purge**.
   The **Export and Purge Audit Log Items** page opens.
3. In the **Items to Purge** section, click (calendar icon) and select a date.
4. When you finish, click **Purge**.
   You are prompted, "Click 'OK' to purge all audit log items through: *mm/dd/yyyy*."
5. Click **OK** (or **Cancel** to abandon the request).

The data is purged from the audit log.

Managing Scheduled Tasks

The CMP system runs batch jobs to complete certain operations. These tasks are scheduled to run at regular intervals, with some tasks scheduled to run in a certain order. You can change the scheduling of these tasks to better manage network load or to propagate a network element change to the Policy Management devices on demand. You can also abort a running task.

Caution: Oracle recommends that you follow the order in which scheduled tasks are listed. Serious system problems can occur if the order is changed. Consult My Oracle Support before changing the order of task execution.

The tasks include:

- **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.

- **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. The *OSSI XML Interface Definitions Guide* describes the OM Interface and the OM Statistics in detail.

  - **Stats File Generator** — Generates statistics files by extracting the data from the CMP database using the OSSI XML interrface. 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 (the default is 72 hours); File Format, either XML (the default) or CSV; and Stats Type, which lets you select the statistics group(s) to extract. For information on the individual statistics in each available group, see the *OSSI XML Interface Definitions Guide*.

- **Replication Statistics** — Generates replication statistics for MPE and MRA servers.

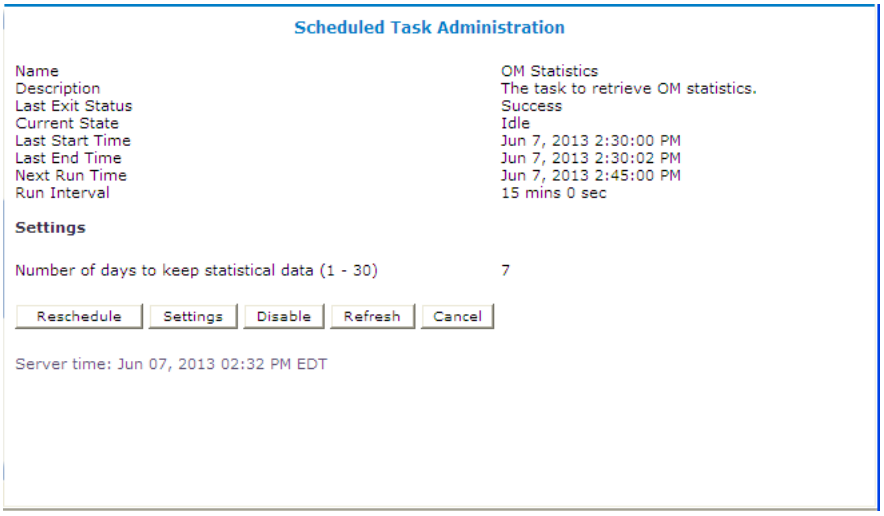
  Note: The run interval should be the same as the Stats Collection Period. For more information, see *Setting Stats Settings*.

- **OSSI Distributor Task** (optional) — Reads from the database topology and subscriber data that has entered the CMP database using the OSSI Interface.
- **Subscriber Distributor** — Reads subscriber data from the CMP database and then distributes it to the appropriate Policy Management devices within the system.

Configuring a Task

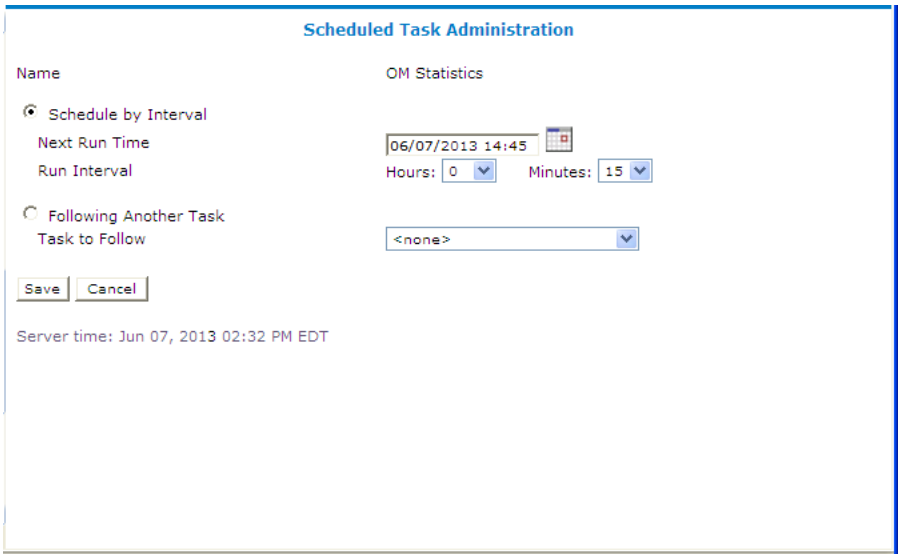
To configure an individual task:

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:



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:



  - **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** — Defines the run time as following the completion of another scheduled task that you select 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, "Click 'OK' to run this task now." Click **OK** to run the task (or **Cancel** to cancel the request).

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

  If you click **Disable**, you are prompted, "Click 'OK' to disable this task." Click **OK** (or **Cancel** to cancel the request); the task is disabled and will not run at its next scheduled time, and the button changes to **Enable**.

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

User Management

The CMP system lets you configure the following user attributes:

- **Roles** — What a user can do within the CMP system.
- **Scopes** — What network element groups and Policy Management device groups a user can control, which provides a context for a role.
- **Users** — Once you define roles and scopes, you can apply them to user profiles.
- **RADIUS Authentication** — Lets the CMP system authenticate users using RADIUS Authentication. These users must match the RADIUS Server account information before access is permitted.

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 accounts. Requests and responses consist of XML documents. You must define a user profile for the external system. The profile is a regular CMP user profile with specific roles and scope.

Assign the profile a role that includes the following privileges:

- Show privilege for XML Import/Export
- Read-Write privilege for User Management

For information on creating a user profile, see *Creating a User Profile*. For more information on the XML application programming interface, see the *OSSI XML Interface Definitions Guide*.

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 what 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 administration.
- **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.

Creating a New Role

To create a new role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
   The **Role Administration** page opens in the work area, displaying existing roles.
3. On the Role Administration page, click **Create Role**.
   The **New Role** page opens. By default, all privileges are set to **Hide** (that is, the functions do not appear to users of the role, so access must be explicitly granted) or **Read-Only** (that is, information can be displayed but not changed).
4. Enter the following information:
   a) **Name** — The name for the new role (up to 64 characters long)
   b) **Description/Location** (optional) — Free-form text
5. **Policy Server Privileges** — Defines access to the following MPE device management functions (assigning each the privilege **Hide**, **Read-Only**, or **Read-Write**):
   - **Configuration**
   - **Application**
   - **Match Lists**
   - **Quotas**
   - **Services & Rating Groups**
   - **Policy Counter ID**
   - **Traffic Profiles**
   - **Retry Profiles**
   - **Charging Server**
   - **Time Period**
   - **Monitoring Key**
   - **AVP Definition**
   - **Global Configuration Settings**
   - **Bulk Operation**
6. **Subscriber Privileges** — Defines access to the subscriber functions (assigning the privilege **Hide**, **Read-Only**, or **Read-Write**):
   - **Entitlements**
   - **Tiers**
   - **Quota Usage**
7. **SPR Privileges** — Defines access to the SPR functions (assigning the privilege **Hide**, **Read-Only**, or **Read-Write**):
   - **Subscriber Data**
8. **Network Privileges** — Defines access to the network management functions (assigning the privilege **Hide**, **Read-Only**, or **Read-Write**):
   - **Network Element**

9. **MRA Privileges** — Defines access to the MRA Configuration functions:
   - **Configuration** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Bulk Operations** (with the privileges **Hide** or **Show**)
10. **Policy Management Privileges** — Defines access to the policy management functions:
   - **Policy Library** (with the privileges **Hide**, **Read-Only**, **Read and Deploy**, or **Read, Deploy, and Write**)
   - **Template Library** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Policy Table Library** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Policy Import/Export** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
11. **System Wide Reports Privileges** — Defines access to the system-wide reports functions:
   - **System Wide Reports Configuration** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
12. **Platform Setting Privileges** — Defines access to the platform setting functions:
   - **Topology Configuration** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Server Operation** (with the privileges **Hide** or **Read-Write**)
13. **Upgrade Manager Privileges** — Defines access to software upgrade functions:
   - **ISO Maintenance** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **System Maintenance** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
14. **System Administration Privileges** — Defines access to system administration functions:
   - **XML Import/Export** (with the privileges **Hide** or **Show**)
   - **Reports** (with the privileges **Hide** or **Show**)
   - **Operational Measurements** (with the privileges **Hide** or **Read-Only**)
   - **User Management** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Scheduled Tasks** (with the privileges **Hide** or **Read-Write**)
   - **Trace Log of Policy Server** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Event Log, Audit Log, & Alerts of Policy Server** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Event Log** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Audit Log** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Audit Log User Info** (with the privileges **Hide** or **Show**)
   - **Alarms** (with the privileges **Hide**, **Read-Only**, or **Read-Write**)
   - **Password Strength** (with the privileges **Read-Only** or **Read-Write**)
   - **Push Method for Statistics** (with the privileges **Read-Only** or **Read-Write**)

     If set to **Read-Only**, the following fields are displayed for the Stats File Generator 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. Defaults to 72 hours.
- **File Format** — Any format can be selected. Defaults to XML.
- **Stats Type** — Any stats type can be selected to generate stats. Defaults to No one. If you do not select a stats type, the task will not run normally.

New tasks are created to synchronize stats files. These tasks will 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**
  - **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.

15. When you finish, click **Save** (or **Cancel** to discard your changes).

Privileges are assigned to the role.

Modifying a Role

To modify a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
   The **Role Administration** page opens in the work area, displaying existing roles.
3. Select the role to modify.
   The **Role** page opens.
4. On the **Role** page, click **Modify**.
   The **Modify Role** page opens.
5. Modify role information as necessary.
   See *Creating a New Role* for a description of the fields contained within this page.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The role is modified.

Deleting a Role

You can delete any role except the Administrator role. You cannot delete a role that is in use.

To delete a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
   The **Role Administration** page opens in the work area, displaying existing roles.

3. Delete the role using one of the following methods:
   - From the work area, click the Delete icon located next to the role to delete.
   - From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

   You are prompted, "Are you sure you want to delete this Role?"
4. Click **OK** (or **Cancel** to abandon the request).

The role's information is deleted from the CMP database.

User Scope

Scope defines which network element groups and Policy Management device groups that a user has access to, which provides operational context for a role.

Creating a New Scope

You can configure scopes that contain selections of network element groups and Policy Management device groups that provide a context for a role. This lets you control what areas or devices in a network a user can manage. The default scope, **Global**, contains all items defined within the CMP database. Once you define a scope you can apply it to a user.

To configure a new scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. In the content tree, click **Scopes**.
   The **Scope Administration** page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. Click **Create Scope**.
   The **New Scope** page opens.
4. Enter the following information:
   a) **Name** — The name for the scope. The name can be up to 64 characters long.
   b) **Description/Location** (optional) — Free-form text.
5. Select the policy server groups included in this scope.
6. Select the network element groups included in this scope.
7. Select the MRA groups included in this scope.
8. When you finish, click **Save** to create the scope (or **Cancel** to discard your changes).

The scope is created.

Modifying a Scope

To modify a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. In the content tree, click **Scopes**.

The **Scope Administration** page opens in the work area, displaying existing scopes. The default scope is **Global**.

3. On the **Scope Administration** page, select the scope you want to modify.
   The scope description opens.
4. Click **Modify**.
   The **Modify Scope** page opens. *Creating a New Scope* describes the fields on this page.
5. Modify scope information as necessary.
6. When you finish, click **Save** (or **Cancel** to discard the request).

The scope is modified.

Deleting a Scope

You can delete any scope except **Global**. To delete a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, click **Scopes**.
   The **Scope Administration** page opens in the work area, displaying existing scopes. (*Figure 40: Deleting a Scope* shows an example.)
3. Delete the role using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the role to delete.
   - From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

   You are prompted, "Are you sure you want to delete this Scope?"
4. Click **OK** (or **Cancel** to discard the request).

The scope is deleted.

Figure 40: Deleting a Scope

User Profiles

A user profile defines a user with a role and one or more scopes.

Creating a User Profile

The User Management functions include the tools necessary to create, modify, or delete system user profiles.

The CMP system is configured initially with the following default user profiles and passwords:

- admin/policies (you cannot delete this profile)
- operator/policies
- viewer/policies

Each default user profile has an associated role assigned to it. The **admin** user is the only profile that cannot be deleted or have its username modified. Also, the **admin** user is the only user who can create, modify, or delete other users. The password assigned to the **admin** user can be changed. For security reasons, it is recommended that you change this value from the default value as soon as the system is installed.

Note: When logging in, the username is not case sensitive; however, the password is case sensitive.

To create a new user profile:

1. Log into the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.

   Note: The **Log Out All Users** button is visible only to the **admin** user.

4. Click **Create User**.
   The **New User** page opens.
5. Define the following information:
   a) **Username** — Assign a name to the user profile of up to 64 characters (this value is not case sensitive).
   b) **Description/Location** (optional) — Free-form text.
   c) **Password** — Assign a password to the user profile.
   This value is case sensitive and must contain at least six characters; alphabetic, numeric, and special characters are allowed. This value must conform to the password strength rules.
   d) **Confirm Password** — Re-enter the password to confirm the value entered above.
   e) **Password Expiration Period(days; 0=never)** — The number of days a password can be used before it expires. (This overrides the system setting.)

   Enter a value from 7 to 365, or 0 to indicate that the password never expires. The default is the system setting.

   f) **Force to Change Password** — If selected, this user must change passwords when he or she next logs in.
   g) **Role** — Select a role from the pulldown list to assign to the user profile.
   h) **Scopes** — Select one or more scopes to assign to the user profile.

6. When you finish, click **Save** (or **Cancel** to discard your changes).

The user profile is created and stored in the **Users** group.

Modifying a User Profile

To modify a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Select the user profile from the content tree.
   The profile information page opens.
5. Click **Modify**.
   The **Modify User** page opens. (*Figure 41: Modify User Page* shows an example.)
6. Modify the user profile.
   For field descriptions, see *Creating a User Profile*.
7. When you finish, click **Save** (or **Cancel** to discard your changes).

The user profile is modified.

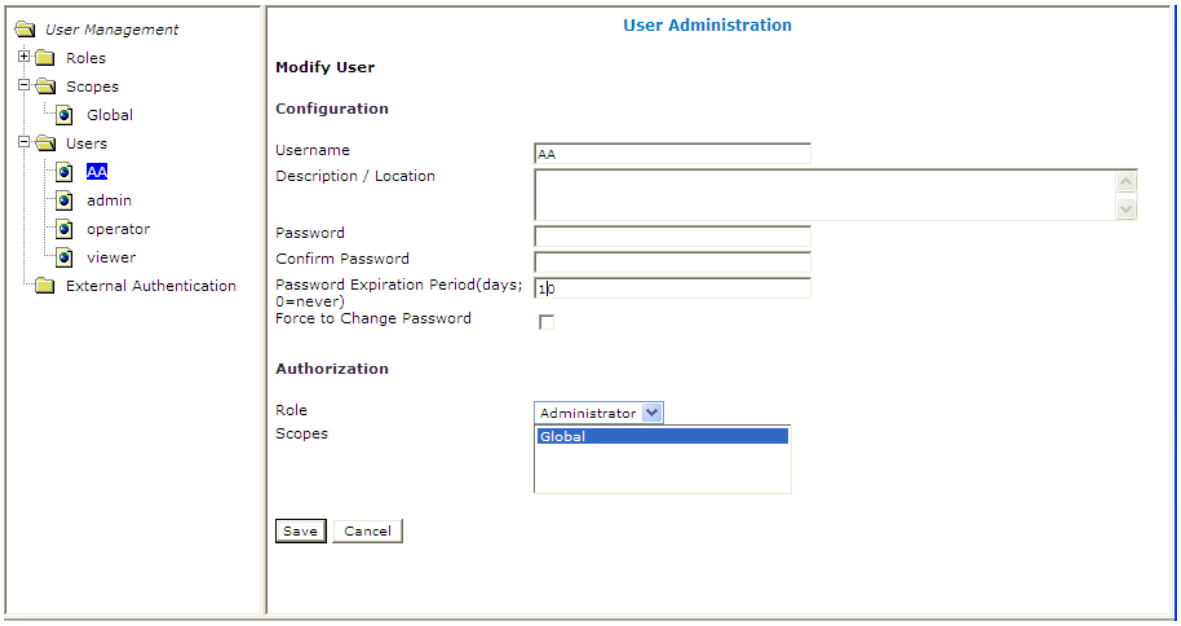


Figure 41: Modify User Page

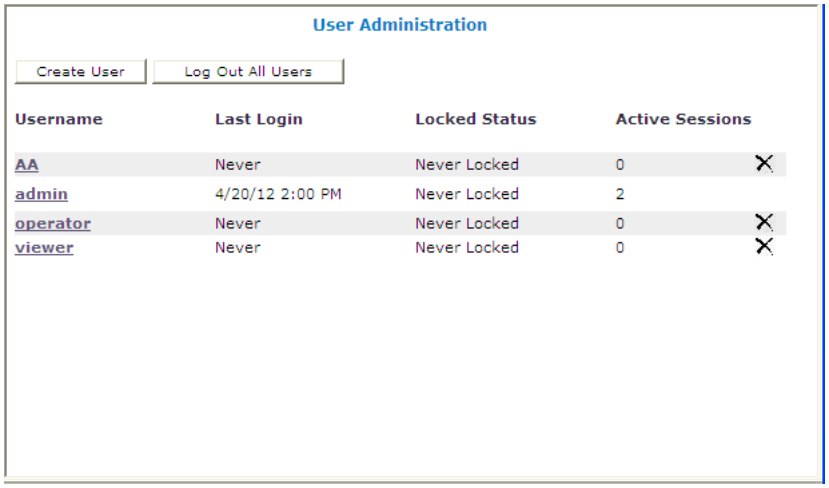
Deleting a User Profile

You can delete any user profile except **admin**. To delete a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.

The content tree displays the **User Management** group.

3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users; for example:



4. Delete the user profile using one of the following methods:
   - From the work area, select the **Delete** icon, located to the right of the profile you want to delete.
   - From the content tree, select the user profile that you want to delete (profile information displays in the work area), then click **Delete**.

   You are prompted, "Are you sure you want to delete this user?"
5. Click **OK** to delete the user profile (or **Cancel** to abandon the request).

The user profile is deleted.

Locking and Unlocking User Accounts

A user is locked out after exceeding the login failure threshold, or if the **admin** user locks the user out. A locked-out user sees the following message on the login page when attempting to log in: "Your account is locked. Please contact the Administrator."

Note: The **admin** account cannot lock the **admin** account.

Locking an Account

To lock a user account:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Select the user profile from the content tree.
   The **User Administration** page opens.
5. Click **Lock**.
   You are prompted, "Are you sure you want to lock out this user?"

6. Click **OK** (or **Cancel** to cancel the request).
   The account is locked. The page displays the message "User account locked successfully." The **Lock** button becomes an **Unlock** button. On the **User Administration** page, the Locked Status for the user changes to **Locked**.

Unlocking an Account

To unlock a user account:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. Select the user profile from the content tree.
   The **User Administration** page opens.
4. Click **Unlock**.
   You are prompted, "Are you sure you want to unlock this user?"
5. Click **OK** (or **Cancel** to cancel the request).
   The account is unlocked. The page displays the message "User account unlocked successfully." The **Unlock** button becomes a **Lock** button. On the **User Administration** page, the Locked Status for the user changes to "Unlocked by Admin."

Logging Out All Users

You can log out all users except admin from the CMP system. 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, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Click **Log Out All Users**
   You are prompted: "Are you sure you want to log out all other users?"
5. Click **OK** to log out all users (or **Cancel** to abandon the request).

Users are logged out.

External Authentication

In addition to the built-in authentication functions, you can configure external authentication, RADIUS authentication, and SANE authentication of CMP users.

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. Configuring the RADIUS server to accept authentication (and accounting, if used)
2. Associating user roles and scopes on the CMP system
3. Configuring the CMP system to work with RADIUS

Configuring the RADIUS Server

The RADIUS server 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 will be aware of the names and locations of the configuration files.)

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 = oracle
        shortname = MPE5
}
client 10.0.10.23 {
        secret = oracle
        shortname = CMP56
}
```

The best practice is to define IP addresses rather than FQDNs. If no netmask is given, the default is /32. The shared secret (in this example, "**oracle**") must be both defined on the RADIUS server and entered into the CMP configuration (see *Enabling 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.

Defining CMP Users to the RADIUS Server

RADIUS 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 (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.

When RADIUS has authenticated a user, it sends back various attributes with the authentication acceptance message. The CMP system uses these attributes to determine what the user can do. The best practice is to use a vendor-specific attribute (VSA) dictionary file to define what attributes to send

back to the client. *Figure 42: 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 42: 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 RADIUS on the CMP System

By default, RADIUS 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 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:

```
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, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**.
   The modify page opens.
5. In the **Configuration** section, select **Enable RADIUS Authentication**.
   Additional fields appear (see *Figure 43: External Authentication Configuration Page*).
6. Edit the following fields:
   a) **Enable RADIUS Accounting** — Enables RADIUS accounting on the CMP system.
   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.
   b) **Destination for Accounting Messages** — Choose the following from the list:
      - **Both Primary and Secondary** (the 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.

c) **NAS IP Address** (required) — IP address, in IPv4 or IPv6 format, of the network access server. By default, this is the local host address.

d) **Use local authentication** — Choose when to use local authentication:

- **When RADIUS servers timeout**
- **When both RADIUS servers timeout or reject**
- **Never** — Fallback to local authentication is never used (however, the user **admin** is always authenticated locally)

e) **Source of User Credentials** — Choose the following from the list:

- **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.

f) **Action if Missing Credentials:**

- **Reject** — If you select this option, a user whose login credentials are missing is not logged in.
- **Use following defaults**:

  1. **Default Role** — Role assigned if the user credentials are missing or mismatched. The default is **Viewer**.
  2. **Default Scope** — Scope assigned if the user credentials are missing or mismatched. The default is **Global**.

7. In the **RADIUS Servers** section, edit the following fields:

a) **Primary RADIUS Authentication Server**

- **Server** — 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** — IP port number of the primary server. The default is port 1812.
- **Timeout (seconds)** — How long the CMP system waits for a response from the server. The default is 3 seconds.
- **Retries** — How many times the CMP system tries to send a message to the server. The default is 3 times.
- **Shared Secret** — A password-like string that must exactly match between the CMP system and the secret configured in the entry for this CMP system in the clients.conf file in the RADIUS server. If it does not match, the server ignores all messages from the CMP system.

b) **Secondary RADIUS Authentication Server**

If configured, the secondary authentication server uses the same fields as the primary server.

c) **Primary RADIUS Accounting Server**

- **Server** — FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary accounting server.
- **Port** — IP port number of the primary server. The default is port 1813.
- **Timeout (seconds)** — How long the CMP system waits for a response from the server. The default is 3 seconds.
- **Retries** — How many times the CMP system tries to send a message to the server. The default is 3 times.
- **Shared Secret** — A password-like string that must exactly match between the CMP system and the secret configured in the entry for this CMP system in the clients.conf file in the RADIUS server. If it does 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 server.

8. When you finish, click **Save** (or **Cancel** to discard your changes).
The window closes.

RADIUS Authentication and Accounting is configured.

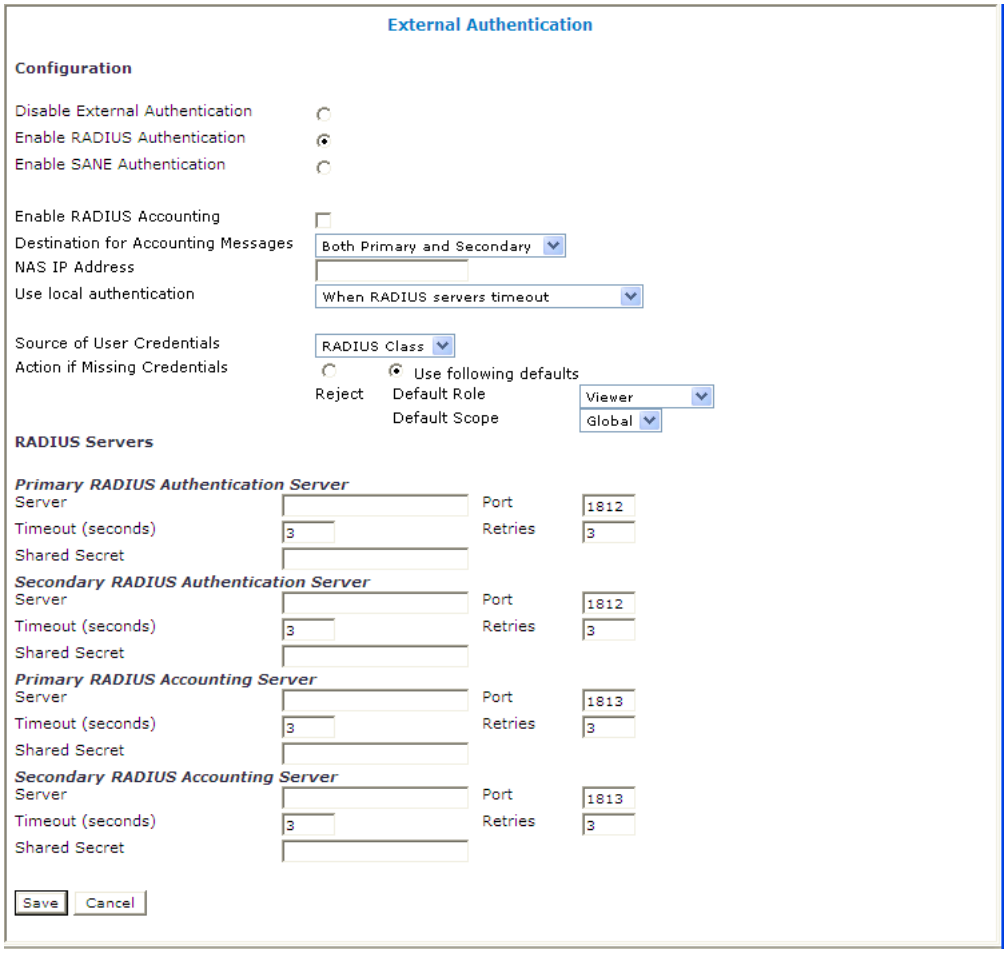


Figure 43: External Authentication Configuration Page

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.)

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 modify page opens.
5. In the **Configuration** section, select **Enable SANE Authentication**.
   Additional fields appear.
6. Edit the following fields:
   a) **Artifact Parameter Name** — Name of the artifact parameter. Enter an alphanumeric string. The default is **artifact**.
   b) **Verification for Account** — Choose the following from the list:
      - **On login only** (the 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 again for each HTTP or HTTPS request. If any request is not authenticated, the user is immediately logged out.
   c) **Action if Missing Credentials:**

- **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:
  1. **Default Role** — Default role assigned to the user. The default role is **Viewer**.
  2. **Default Scope** — Default scope assigned to the user. The default scope is **Global**.

7. In the **SANE Servers** section, edit the following fields:
   a) **SAML Service Name** — Name of the Security Assertion Markup Language service registered with the UDDI server. Enter an alphanumeric string.
   b) **UDDI Inquiry URL** — Universal Description, Discovery and Integration URL, in HTTP or HTTPS format, for the inquiry.
8. When you finish, click **Save** (or **Cancel** to discard your changes).
   The window closes.

SANE authentication is configured on the CMP system.

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 any user's password.

If a system administrator has configured your account for password expiration, you will receive a warning when you log in that you will need to change your password.

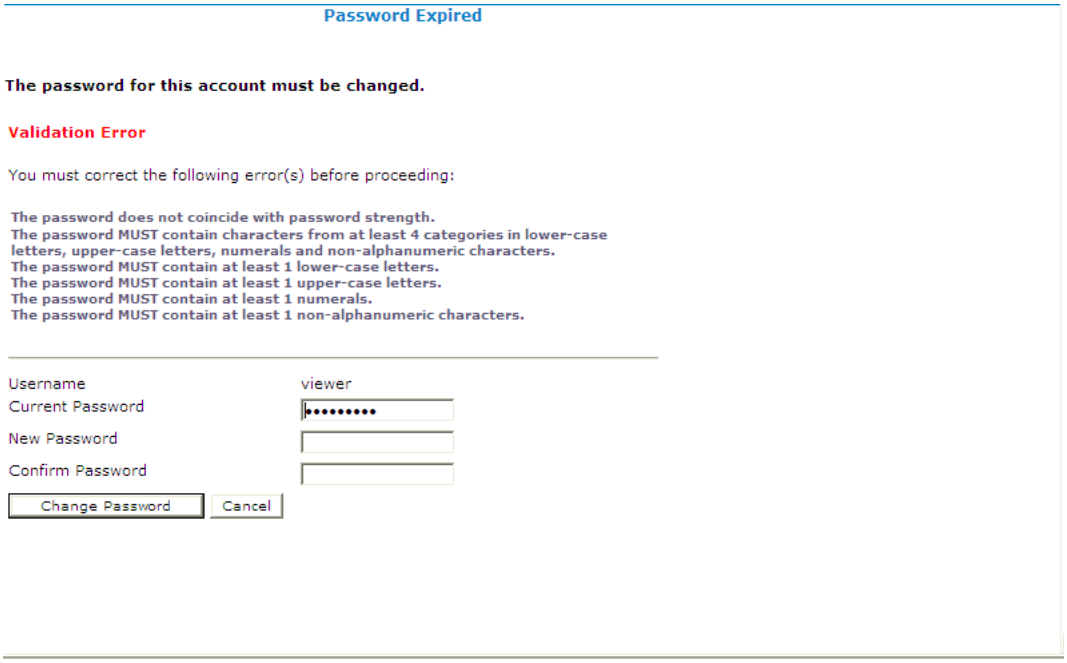
To change your password:

1. From the **System Administration** section of the navigation pane, select **Change Password**.
   The **Change Password** page opens. If your account is set up with a password expiration period, the expiration date is displayed.
2. Enter the following information:
   a) **Current Password** — The present value of the password.
   b) **New Password** — The value of the new password.

      This value is case sensitive and must conform to the password strength rules. The password cannot contain the user name.

   c) **Confirm Password** — Retype the new password.

      If your new password does not conform to the password strength rules, a validation error message appears; for example:



Enter and confirm another password that conforms to the rules.

3. When you finish, click **Change Password**.

Your password is changed.

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: 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 44: 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 41: 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 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
- **Manager is NW-CMP**— Enable Network mode in a tiered CMP system. See *The Oracle Communications Policy Management Network Configuration Management Platform* for more information.
- **Manager is S-CMP**— Enable System mode in a tiered CMP system. See *The Oracle Communications Policy Management Network Configuration Management Platform* for more information.

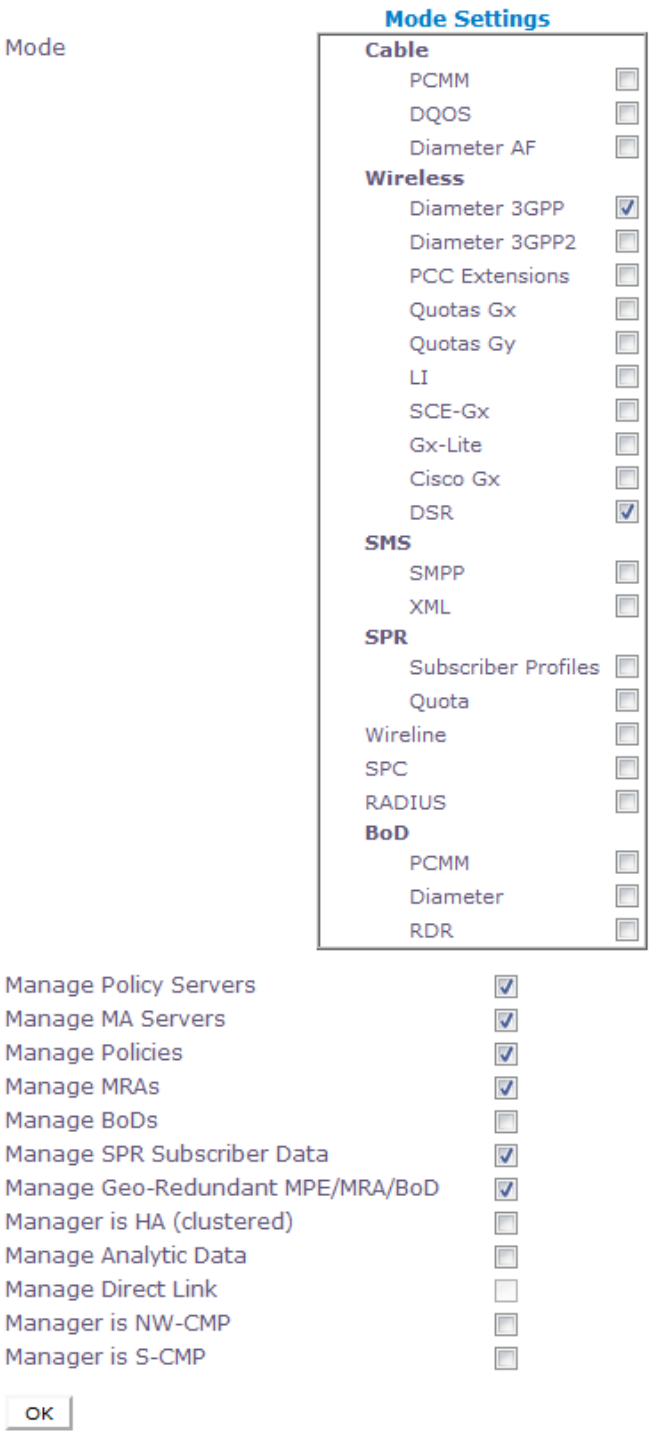


Figure 44: Mode Settings Page

Table 41: 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.
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.
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*.	
	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)

Mode	Sub-Mode	Description
		devices transmitting Raw Data Records (RDRs).

Glossary

#

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

CMP	Configuration Management Platform A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.
COMCOL	Communications Core Object Library A suite of re-usable C++ libraries, as well as processes and procedures available for use in Tekelec products. Many of its features are focused toward the communications area of software developments, although it purpose is not intended to restrict its functionality to any particular area
CPU	Central Processing Unit

D

Diameter	Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty. Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for

D

	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.
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 Service Code Point 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

D

	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.
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.
FQDN	Fully qualified domain name The complete domain name for a specific computer on the Internet (for example, www.oracle.com).

F

	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 provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.
Gx	The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.

H

HA	High Availability High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.
HTTP	Hypertext Transfer Protocol

I

IMSI	International Mobile Subscriber Identity

I

	A unique internal network ID identifying a mobile subscriber. International Mobile Station Identity
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
IPv6	Internet Protocol version 6

L

LDAP	Lightweight Directory Access Protocol A protocol for providing and receiving directory information in a TCP/IP network.
Lightweight Directory Access Protocol	See LDAP.

M

MCC	Mobile Country Code A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies

M

	a particular subscriber. See also MNC, IMSI.
MNC	Mobile Network Code A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.
MPE	Multimedia Policy Engine A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization.
MRA	Multi-Protocol Routing Agent Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.
Multimedia Policy Engine	See MPE.

N

NAI	Network Access Identifier The user identity submitted by the client during network authentication.

N

network topology	A map of physical equipment or logical entities in a network.

O

OCS	Online Charging Server
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
PCEF	Policy and Charging Enforcement 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.
PCRF	Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network

P

	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.
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.
policy and charging rules function	See PCRF.

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.

R

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 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.

S

session	A Diameter session between the MPE and an external device (e.g., a Gx, Gxa, Gx-Lite or Rx session). Subscribers can maintain multiple sessions at any given time.
SGSN	Serving GPRS Support Node
Short Message Service	See SMS.
SMPP	Short Message Peer-to-Peer Protocol An open, industry standard protocol that provides a flexible data communications interface for transfer of short message data.
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
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, etc. The

S

PCRF and SPR functionality is provided through an ecosystem of partnerships.

SSO

Single sign-on

Subscriber Profile Repository

See SPR.

U

UE

User Equipment

V

VIP

Virtual IP Address

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

X

XML

eXtensible Markup Language

A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.