Policy Management

Configuration Management Platform Wireless User's Guide

Release 12.6.1
E45402-02
April 2022

Policy Management Configuration Management Platform Wireless User's Guide, Release 12.6.1

E45402-02

Contents

About This Guide

1 Oracle Communications Policy Management System

4 Configuring Protocol Routing

5 Configuring Advanced Device Settings

6 Configuring Debug Logs

7 Managing Network Elements

11 Mapping Serving Gateways to MCCs/MNCs

12 Managing a Subscriber Profile Repository

A CMP Modes

B Generated Statistics

About This Guide

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 variables that can be used in policy rules. These variables provide information about the device, subscriber, or quota for which a policy rule is being executed.

How This Guide is Organized

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

- About This Guide provides general information about the organization of this guide, related documentation, and how to get technical assistance.
- Oracle Communications Policy Management System provides an overview of the Multimedia Policy Engine (MPE) device, which manages multiple network-based client sessions; the network in which the MPE device operates; policies; and the Configuration Management Platform (CMP) system, which controls MPE devices and associated applications.
- Configuring the Policy Management Topology describes how to set the topology configuration.
- Managing Multimedia Policy Engine Devices describes how to use the CMP system to configure and manage the MPE devices in a network.
- Configuring Protocol Routing describes how to configure protocol routing.
- Configuring Advanced Device Settings describes how to specify advanced settings for MPE or MRA devices.
- Configuring Debug Logs describes how to configure device- and system-level settings for troubleshooting system operations using logs.
- Managing Network Elements describes how to manage network elements.
- 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 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.
- System-Wide Reports describes the reports available on the function of Policy Management systems in your network.
- Upgrade Functions describes the purpose of the Upgrade Manager GUI page and the elements found on that page.
- Global Configuration describes how to configure global settings in the CMP system.
- System Administration describes functions reserved for CMP system administrators.
- The appendix CMP Modes lists the functions available in the CMP system, as determined by the operating modes and sub-modes selected when the software is installed.
- The appendix Generated Statistics lists available statistics for generated scheduled tasks.

Scope and Audience

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

- Application administrators, who install and upgrade Policy Management applications and perform advanced system administration
- Operators, who monitor Policy Management systems daily and perform adjustments
- System administrators, who control access to the CMP system
- System architects, who design carrier network system architectures, including planning for Policy Management systems
- Network administrators, who manage carrier networks

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

Policy and Protocol Specifications

The following specifications provide information on protocols:

- Internet Engineering Task Force (IETF) specifications:
  - RADIUS RFCs:
    - RFC 2865: RADIUS
    - RFC 2866: RADIUS Accounting
    - RFC 3576: Dynamic Authorization Extensions to RADIUS
  - Diameter RFCs:
    - RFC 3539: Authentication, Authorization and Accounting (AAA) Transport Profile
    - RFC 3588: Diameter Base Protocol
  - TACACS+ RFC 1492: An Access Control Protocol, Sometimes Called TACACS

- RFC 3164: The BSD syslog Protocol

- 3rd Generation Partnership Project (3GPP) technical specifications:
  - 3GPP TS 23.003: Numbering, addressing and identification (Release 12)
  - 3GPP TS 23.203: Policy and charging control architecture (Release 13.2)
  - 3GPP TS 26.114: IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction (Release 13.1.0)
  - 3GPP TS 26.445: Codec for Enhanced Voice Services (EVS); Detailed algorithmic description (Release 13.0.0)
  - 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses (Release 13)
  - 3GPP TS 29.208: End-to-end Quality of Service (QoS) signalling flows (Release 6)
  - 3GPP TS 29.209: Policy control over Gq interface (Release 6)
  - 3GPP TS 29.211: Rx Interface and Rx/Gx signalling flows (Release 6)
  - 3GPP TS 29.212: Policy and Charging Control over Gx/Sd reference point (Release 13.0)
  - 3GPP TS 29.213: Policy and Charging Control signalling flows and QoS parameter mapping (Release 12.x6)
  - 3GPP TS 29.214: Policy ad Charging Control over Rx reference point (Release 13.0)
  - 3GPP TS 29.219: Policy and Charging Control: Spending limit reporting over Sy reference point (Release 11.3)
  - 3GPP TS 29.229: Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 8)
  - 3GPP TS 29.273: Evolved Packet System (EPS); 3GPP EPS AAA interfaces (Release 12.6)
  - 3GPP TS 32.240: Charging architecture and principles (Release 8)
  - 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging applications (Release 8)
- 3rd Generation Partnership Project 2 (3GPP2) technical specifications:
  - 3GPP2 X.S0013-012-0: Service Based Bearer Control—Stage 2
  - 3GPP2 X.S0013-013-0: Service Based Bearer Control—Tx Interface Stage 3
  - 3GPP2 X.S0013-014-0: Service Based Bearer Control—Ty Interface Stage 3

Locate Product Documentation on the Oracle Help Center Site

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

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

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

4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support

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

Call the Customer Access Support 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:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support 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 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.

List of Figures

List of Tables

1 Oracle Communications Policy Management System

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

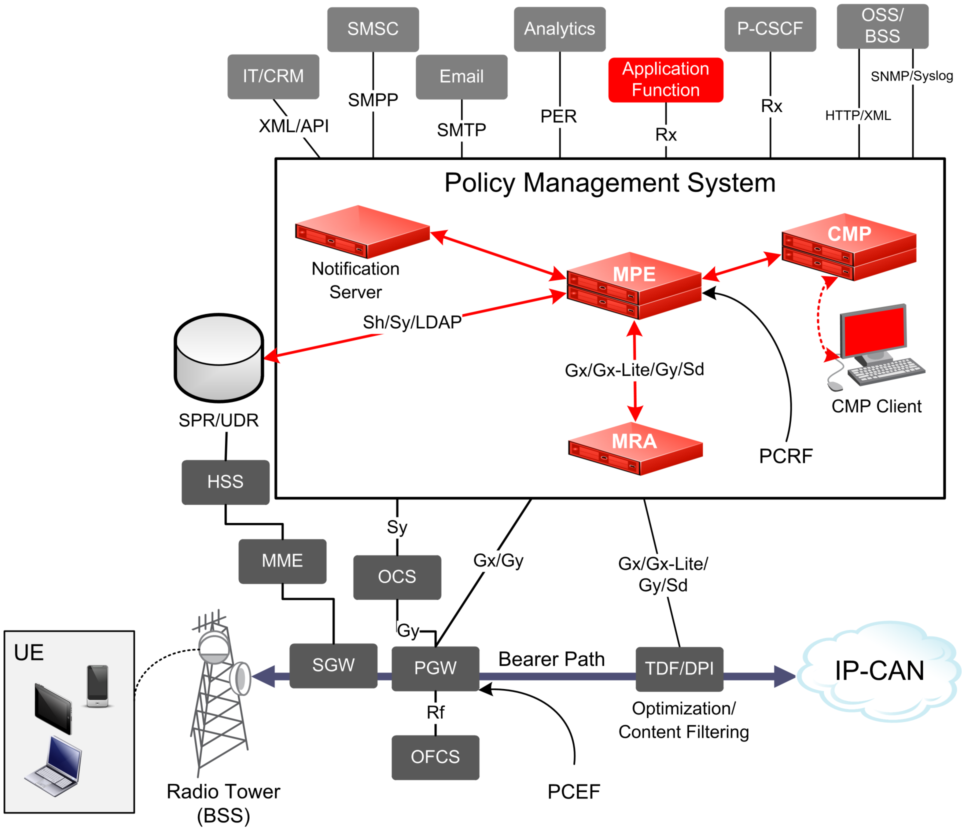
- The Oracle Communications Policy Management Configuration Management Platform (CMP) system controls MPE devices and associated applications.
- The Multimedia Policy Engine (MPE) device manages multiple network-based client sessions.
- The Multi-Protocol Routing Agent (MRA) device maintains bindings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

Introduction to Policy Management

Oracle Communications Policy Management system provides the mechanism that allows communications service providers (carriers) to control and charge for subscribers' access to network resources. The central component of Policy Management is the Multimedia Policy Engine (MPE) device. The MPE device functions as a dynamic policy and charging rules function (PCRF).

Figure 1-1 shows how the Policy Management system fits into and interacts with other elements of a wireless network.

Figure 1-1 Policy Management System and its Components



About Policy Management Service Flows

The MPE device establishes service flows between subscribers and the application servers that provide multimedia services.

A service flow is activated only after the contents of its QoS request are examined and approved by the MPE device. If approved, the request is forwarded to the intended destination network node.

As illustrated in Figure 1-1, when a subscriber wishes to make a 3G-LTE wireless call, the following actions occur:

1. Subscriber powers on the user equipment (UE) for example, a cell phone.
2. The UE radio pings for the nearest cell tower to which it can connect.
3. The UE identifies itself to the network and attaches to the network.
4. The subscriber calls a phone number.
5. The radio tower's base station (BS) equipment (node B for 3G networks) [part of the base station subsystem (BSS) that handles telecommunication traffic] receives the signal and routes it to the mobile switching center (MSC) for validation of the subscriber account.
6. The MSC routes the phone call and connects to the Mobility Management Entity (MME) for the public switched telephone network (PSTN).
7. The MME authenticates the UE/subscriber to the Home Subscriber Server (HSS).

8. The MME chooses a Serving Gateway (SGW) or Packet Data Network Gateway (PGW) for session binding.
9. The PGW authorizes the UE to access the Public Land Mobile Network (PLMN) via an Access Point Name (APN) and enforces UE roaming restrictions (if any).
10. Using the Gx interface, the PGW connects with Policy Management:
    a. The PGW connects with either its associated MPE device or MRA device (if present).
    b. The MPE device examines the QoS request before it gets to the network element and processes the request against the policy rules within its policy repository.
    c. The MPE device then makes a decision based on the defined policy rules to accept or reject the request.
    d. Depending on the decision made, the MPE device performs one of the following actions:
        - Accepts the QoS request and forwards it to the network element, where the required network resources are provisioned, allowing the service flow for IP-streaming to be admitted and activated.
        - Rejects the QoS request, in which case an error message is sent back to the application and no service flow is established.

> **Note:**
>
> When provisioned resources are no longer required and deleted, the network resources are recovered for use elsewhere.

Major Components of Policy Management

The Oracle Communications Policy Management system (see Figure 1-1) provides the capability to:

- Create dynamic Quality of Service (QoS) service flows between subscribers and application servers that provide multimedia services
- Manage network resources more efficiently and flexibly
- Manage policies

The major components of the Oracle Communications Policy Management system include:

- Configuration Management Platform Server
- Multimedia Policy Engine Device
- Multi-Protocol Routing Agent Device
- Subscriber Profile Repository
- Notification Server

Configuration Management Platform Server

The CMP server provides the following functionality:

- Provides the policy console for managing the following:
    – Policy objects like MPE and MRA devices

  - Policies
  - Configuration templates
  - Network elements
  - System topology
- Contains a centralized database of policy rules, policy objects, and network objects
- Communicates Policy Management network management information with network management systems (NMSs) using Simple Network Management Protocol (SNMP)

See Figure 1-1 for more information.

Multimedia Policy Engine Device

MPE devices perform the following actions:

- Provides policy and charging rules function (PCRF) for controlling policy decisions and flow-based charging

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

- Obtains subscriber information, evaluates the applicable policies, and directs the PCEF network element to handle the session based on policy rules when the MPE device receives a request for a policy decision for a subscriber session
- Communicates with clients using Diameter application interfaces (for example, Gx and Rx) and can communicate with an online charging system (OCS) directly using an Sy interface See Figure 1-1 for a representation of the various Diameter interfaces used by Policy Management system.
- Sends Short Message Service (SMS) or Simple Mail Transfer Protocol (SMTP) notifications to subscribers, if enabled
- Sends analytics data stream (ADS) information, as a series of policy event records (PERs), to third-party systems for analysis

> **Note:**
>
> You can increase the capacity of the Policy Management network by adding additional MPE devices.

See Multimedia Policy Engine Devices for detailed information.

Multi-Protocol Routing Agent Device

MRA devices, also known as Oracle Communications Policy Management Policy Front End devices, perform the following functions:

- In a large Policy Management network implementation, MRA devices, operating either statelessly (statically) or statefully (dynamically), distribute and load-balance sessions between pools of MPE devices.

> **Note:**
>
> You can increase the capacity of the Policy Management network by adding additional MRA and MPE devices.

- Oracle Communications Diameter Signaling Router (DSR) systems are multi-application Diameter routing agents that can support segmented Policy Management networks.

See Multi-Protocol Routing Agent Devices for more information. Refer to *Policy Front End Wireless User's Guide* for detailed information.

Subscriber Profile Repository

A subscriber profile repository (SPR) database contains subscriber or subscription information. Examples are:

- Oracle Communications Subscriber Database Management (SDM) database
- Oracle Communications User Data Repository (UDR) database
- Oracle Communications Enhanced Subscriber Profile Repository (ESPR) product

> **Note:**
>
> The **ESPR** product supports a RESTful application programming interface (API) to provisioning and OCS systems.

- A third-party SPR system

MPE devices can use Sh, Sy, Lightweight Directory Access Protocol (LDAP),and Dynamic Host Configuration Protocol (DHCP) communication protocols to communicate with an SPR database.

See Subscriber Profile Repository for more information. See Managing a Subscriber Profile Repository for detailed information.

Notification Server

Notifications are generated by a policy action. The destination, content and attributes of the notification are configurable by the operator and allow for flexible notifications within an HTTP request message.

> **Note:**
>
> Notification servers are only available when SMPP, XML, or Wireless-C (with CMPP) mode is enabled. See CMP Modes for details.

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

Hardware System Requirements

The various Policy Management applications (for example, MPE and MRA devices) run on a variety of hardware platforms:

- Hewlett-Packard (HP) Enterprise ProLiant DL360/Gen8 RMS
- HP Enterprise ProLiant BL460c Gen8 blade server

> **Note:**
>
> Depending on the hardware and the selected enclosure type, the system also requires the appropriate switches and connectors.

In addition to the selected enclosure and hardware for the Policy Management system, a separate network management server on an HP ProLiant DL380, provides tools and utilities to manage multiple c-Class enclosures and blade software, as well as networking equipment (enclosure switches) for the c-Class environment.

On all the hardware platforms Policy Management applications can execute as virtual machines within a network functions virtualization (NFV) infrastructure.

Maintaining and Managing the System

Oracle Communications Policy Management uses external utilities, applications, and tools for maintaining and managing devices.

TPD and TVOE

Oracle Communications Policy Management servers use the Tekelec Platform (TPD, also known as Tekelec Platform Distribution) operating system. TPD provides tools that configure third-party hardware and platform components that make up Platform 7.5. Configurable hardware components include HP Enterprise ProLiant and Cisco switches, HP c7000 enclosures with HP blade servers, HP and Cisco switches, and HP external storage systems. Platform components include the firmware for various hardware components as well as the Platform Management & Configuration (PMAC) application to provision and manage those components when hosting feature applications.

TPD is the operating system for many Oracle Communications products including:

- Oracle Communications Policy Management
- Oracle Communications Subscriber Database Management
- Oracle Communications User Data Repository
- Oracle Communications Enhanced Subscriber Profile Repository
- Oracle Communications Diameter Signaling Router

In addition to TPD, TVOE (Tekelec Virtual Operating Environment) platform application provides tools to manage virtual machines (VMs).

Refer to Oracle Communications Tekelec Platform documentation: *Configuration Guide* and *TPD Initial Product Manufacture* for more information.

Refer to Oracle Communications Policy Management documentation: *Bare Metal Installation Guide* and *Platform Configuration User's Guide* for information specific to installing and configuring the Policy Management system.

PMAC

A network management server with TPD and TOE installed acts as a Virtual Host environment and hosts the Product Management and Configuration (PMAC, also known as PM&C) application.

The PMAC application, configured on Policy Management devices during initial system installation, provides system-level management functions at specific sites. The PMAC application supports platform-related maintenance, software installation, provisioning, and upgrade activities. PMAC uses an internal control network (IntCtrl) with internal, non-routable addresses. The PMAC application is independent of the Oracle Communications Policy Management system.

See the Oracle Communications Tekelec Platform PMAC documents *PM&C Incremental Upgrade* and *PM&C Disaster Recovery* for additional information.

See the Oracle Communications Policy Management documents *Bare Metal Installation Guide* and *Platform Configuration User's Guide* for additional information specific to Policy Management.

iLO

In addition to signaling interfaces and networks, the Policy Management system allows for hardware platform management through out-of-band remote access to individual devices, hardware enclosure onboard administrators (OA), and enclosure switches.

The Hewlett Packard (HP) Enterprise hardware platform management tool is called Integrated Lights-out (iLO) management. This application operates independently of the Policy Management applications running on individual devices. The iLO network allows for access across devices restarts, which is needed for maintenance activities such as installations and upgrades.

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

Refer to the end-user documentation for your specific hardware platform for detailed information on using these management applications.

About Specialized Communications Protocols

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

About RADIUS Protocol

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

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

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

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

About Diameter Protocol

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

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

The Policy Management system uses Diameter interfaces (for example, Gx and Rx) to connect to many of its components and with components outside of the system. See Figure 1-2 for the Diameter-specific interfaces.

See #unique_59 for a list of supported IETF Diameter specifications.

More About Policy Management Components

Oracle Communications Policy Management supports a variety of components that perform a wide range of functions.

Multimedia Policy Engine Devices

The Multimedia Policy Engine (MPE) device provides a policy and charging rules function (PCRF) as defined in the 3rd Generation Partnership Project (3GPP) technical specification “Policy and charging control architecture” (TS 23.203). It fully supports 3GPP Releases, 7 through 11, policy and charging control (PCC) interfaces. The MPE device includes a simple, powerful, and flexible policy rules engine. The policy rules engine operates on triggers from any interface or from internal timers; evaluates conditions; and then performs appropriate actions. Through the use of policy rules, you can modify the behavior of an MPE device dynamically as it processes protocol messages.

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

- How network resources are allocated and used
- How applications and subscribers are treated

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

Figure 1-2 shows the various interfaces to external devices and functions supported by an MPE device. These interfaces include the following:

- A Policy and Charging Enforcement Function (PCEF) receives and processes requests to start new sessions for subscribers. Examples of PCEFs include a Gateway GPRS Support

Node (GGSN), a Packet Data Network Gateway (PGW), and a High-Speed Gateway (HSGW). MPE devices act as servers for PCEFs, using the Diameter Gx and Gxx interfaces to:

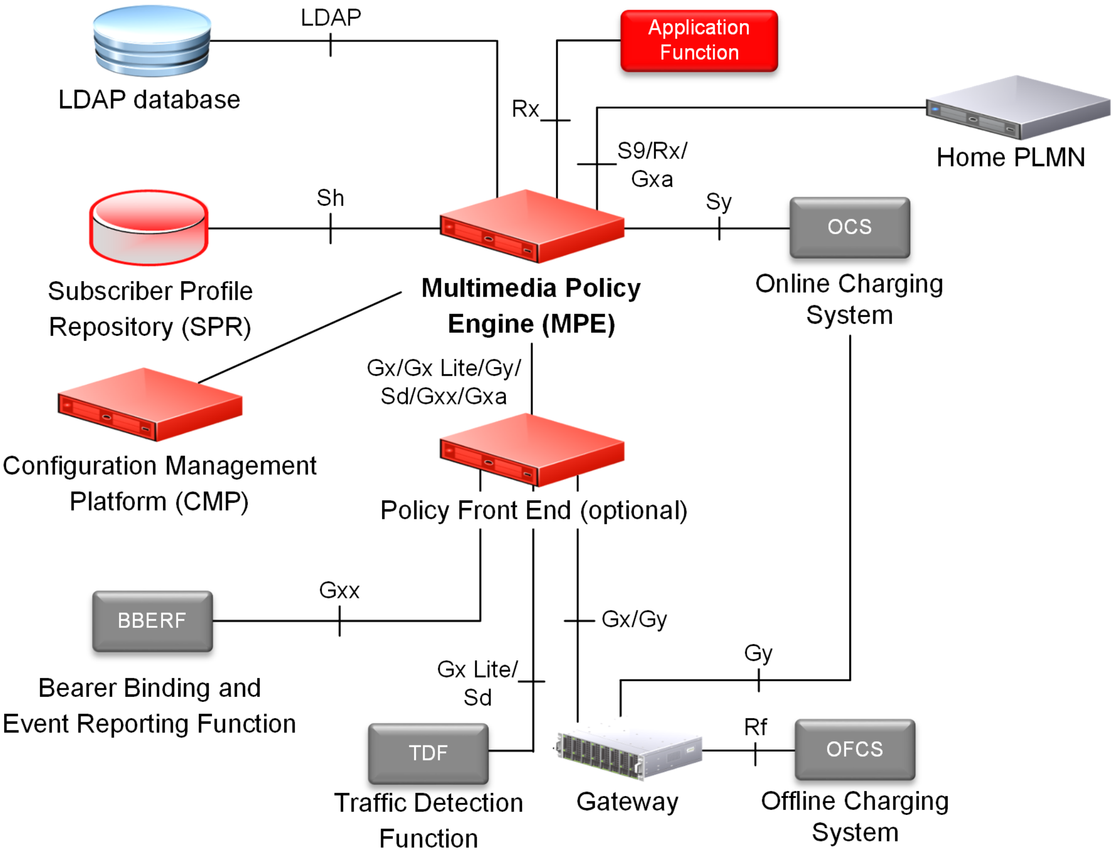
  - Receive requests for policy decisions
  - Send those policy decisions, as PCC rules, to PCEFs for implementation
  - Remove PCC rules from PCEFs
  - Receive traffic plane events from PCEFs

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

- An Application Function (AF) is a network element offering applications that require dynamic policy or charging control over the IP Connectivity Access Network (IP-CAN) user plane. An example of an AF is a Proxy Call Session Control Function (P-CSCF) device. MPE devices act as servers for AFs, using the Diameter Rx interface, to obtain dynamic session information and to send IP-CAN specific information and notifications about bearer-level events. When an AF initiates an Rx session, it is correlated to the same MPE device that hosts the Gx session for that subscriber based on the IP address, which must be globally unique and routable. (If a correlated Gx session cannot be found, the request is rejected with an error code.)
- A Traffic Detection Function (TDF) permits, gates, shapes, or redirects service traffic. An example of a TDF is a deep packet inspection (DPI) device. MPE devices act as servers for TDFs, using the Diameter Sd or Gx Lite interfaces, to receive requests for policy decisions; to send those policy decisions, as PCC rules, to TDFs for implementation; to remove PCC rules from TDFs; and to receive traffic plane events from TDFs. When a TDF initiates an Sd or Gx Lite session, it is correlated to the same MPE device that hosts the Gx session for that subscriber based on the IP address. (If a correlated Gx session cannot be found, the request is rejected with an error code.)
- A Bearer Binding and Event Reporting Function (BBERF) maps a PCC rule to an IP-CAN bearer. Examples of BBERFs are serving gateways (SGW) and HSGWs. MPE devices act as servers for BBERFs, using the Diameter Gxx interface, to receive requests for policy decisions; to send those policy decisions, as PCC rules, to BBERFs for implementation; to remove PCC rules from BBERFs; and to receive traffic plane events from BBERFs. When a BBERF initiates a Gxx session, it is correlated to the same MPE device that hosts the Gx session for that subscriber based on the IMSI. If a correlated Gxa session cannot be found, an MPE device is assigned for the session and the request is processed.
- A Subscriber Profile Repository (SPR) contains subscriber or subscription information. MPE devices act as clients for SPRs, using the Diameter Sh interface, to retrieve subscriber profiles and to register for notification of changes to a subscriber's profile. MPE devices support the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application.
- A directory services database provides distributed directory information, such as user account IDs, email and equipment addresses, and phone numbers, over an IP network. MPE devices communicate with directory servers using the Lightweight Directory Access Protocol (LDAP).
- In support of voice roaming, the S9 Diameter application installs PCC rules generated in a home public land mobile network (HPLMN) into a visited PLMN (VPLMN) and report the events that may occur in the VPLMN to the HPLMN. When an AF is in the VPLMN, The Diameter Rx protocol is used over the S9 interface to exchange service session information from the visited PCRF to the home PCRF.

- An Online Charging System (OCS) calculates charges against a prepaid account for an event and returns information on how long the subscriber can use the service; this can affect, in real time, the service rendered. MPE devices communicate with OCSes using the Diameter Sy interface. (By contrast, an Offline Charging System (OFCS) calculates charges for a service to an account, and does not affect, in real time, the service rendered.) MPE devices act as clients for OCSes, using the Diameter Sy interface, to retrieve subscriber policy counters and policy counter statuses and to register for notification of changes to a subscriber's policy counters.
- The Multi-Protocol Routing Agent (MRA) (also referred to as the Policy Front End) is an optional product deployed in a large Policy Management network that maintains bindings between subscribers and MPE devices. MPE devices communicate with MRAs as proxy Diameter Routing Agents, so they exchange Diameter messages. For more information on the MRA product, refer to *Policy Front End Wireless User's Guide*.
- The CMP system is required to configure, manage, and provision MPE devices. MPE and CMP devices communicate using a proprietary protocol.

Figure 1-2 Diameter Interfaces to the MPE Device


LDAP
LDAP database
Application Function
Rx
Home PLMN
S9/Rx/ Gxa
Sh
Sy
OCS
Subscriber Profile Repository (SPR)
Multimedia Policy Engine (MPE)
Online Charging System
Gx/Gx Lite/Gy/ Sd/Gxx/Gxa
Configuration Management Platform (CMP)
Policy Front End (optional)
Gxx
BBERF
Gx/Gy
Bearer Binding and Event Reporting Function
Gy
Gx Lite/ Sd
Rf
TDF
OFCS
Traffic Detection Function
Gateway
Offline Charging System

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

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

Multi-Protocol Routing Agent Devices

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

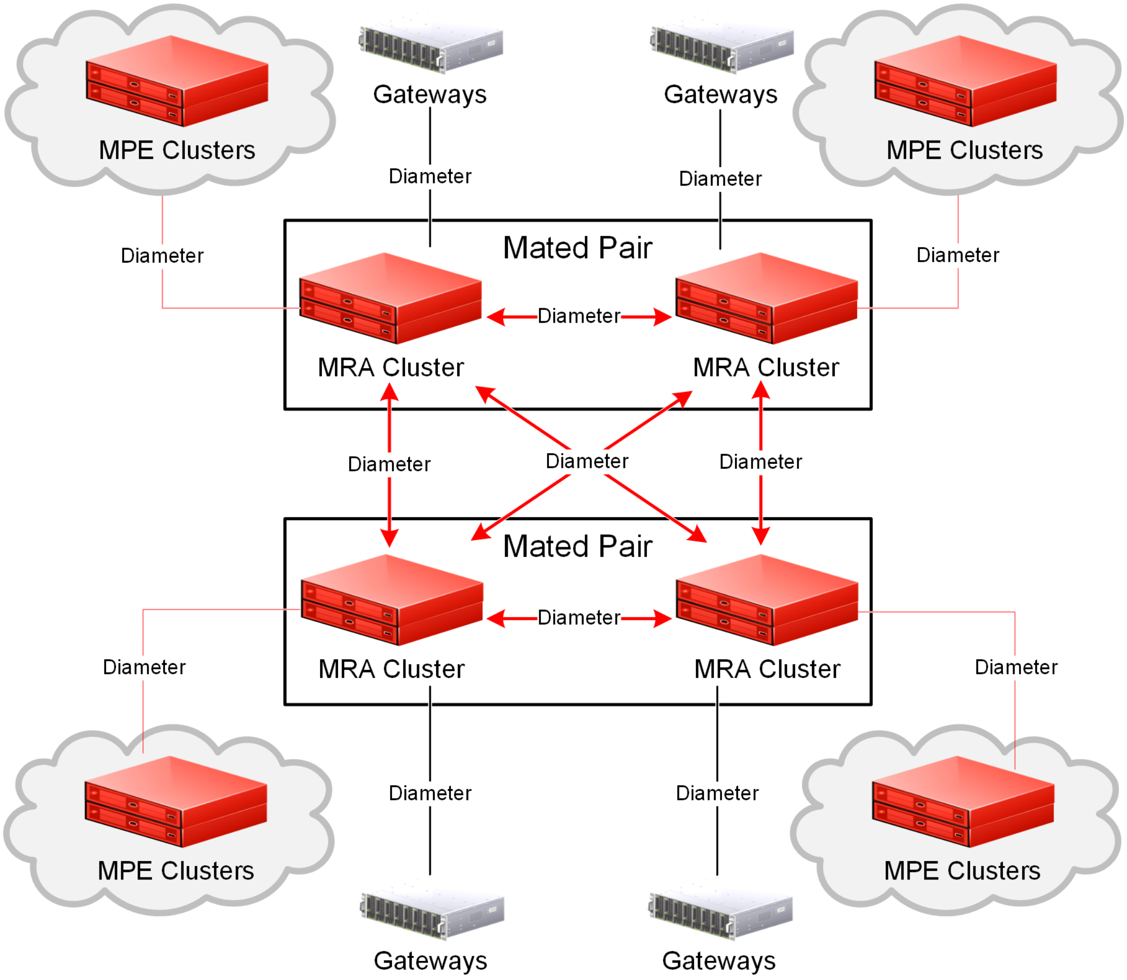
An MRA server correlates traffic between different sessions for a subscriber ensuring that all reference points reach the same MPE server when multiple and separately addressable MPE clusters are deployed.

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

When an MRA server 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 servers in the Policy Management network for a binding using the proprietary Distributed Routing and Management Application (DRMA) protocol. If another MRA server has the binding, the MRA server routes the request to it. If no other MRA server has a binding, the MRA server that received the request creates one.

An MRA server 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 1-3 Typical MRA Network



Subscriber Profile Repository

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

Policy Management supports the following SPR systems:

- Oracle Communications User Data Repository (UDR) database
- Third-party SPR system

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

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

Notification Servers

Within the Policy Management system, an MPE device configured for generic notifications connects to a notification server over HTTP. See Configuring MPE Protocol Options.

The notification server processes event notifications in response to policy actions for HTTP messages. These policy actions include the ability to:

- Send notifications using a dynamic URL
- Send notifications using a static URL

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

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

Configuration Management Platform Server

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

- Configuration and management of MPE devices
- Configuration and management of MRA devices
- Configuration of connections to subscriber profile repository (SPR) servers, including Oracle Communications User Data Repository (UDR) and Oracle Communications Enhanced Subscriber Profile Repository (ESPR) systems
- Definition of network elements
- Management and deployment of policy rules
- Management of objects that can be included in policy rules
- Monitoring of individual product subsystem status
- Administration and management of CMP users
- Upgrading the software on Policy Management devices

Specifications for Using the CMP Server

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

Web Browsers for Wireless and Cable modes

- Mozilla Firefox® release 81.0 or later
- Google Chrome version 86.0 or later

Monitor

- Resolution of 1024 x 768 or greater

Logging in to the CMP System

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

> **Note:**
>
> - If you are using the CMP system for the first time, Oracle recommends that you change the default password for your user name. See Changing a Password for details.
> - It is recommended to not open multiple CMP GUI windows where a modification is made to the config, even if the policy is modified on one window. The other windows can query the state and lead to a inconsistent data.

Before logging in, you need to know the following:

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

> **Note:**
>
> The profile `admin` has full access privileges and is the assumed profile used in all procedures described in this document. You cannot delete this user profile.

To log in to the CMP system:

1. Open a web browser and enter the IP address for the CMP system.

   > **Note:**
   >
   > You can configure the title and text that appear on the login page. For information on changing this page, see Configuring System Settings.

2. Enter your **Username** and **Password**.

   > **Note:**
   >
   > See your System Administrator if you experience problems logging in.

3. Click **Login**.

   The CMP main page opens.

You are logged in.

Logging In to a Standby or Secondary-Site CMP System

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

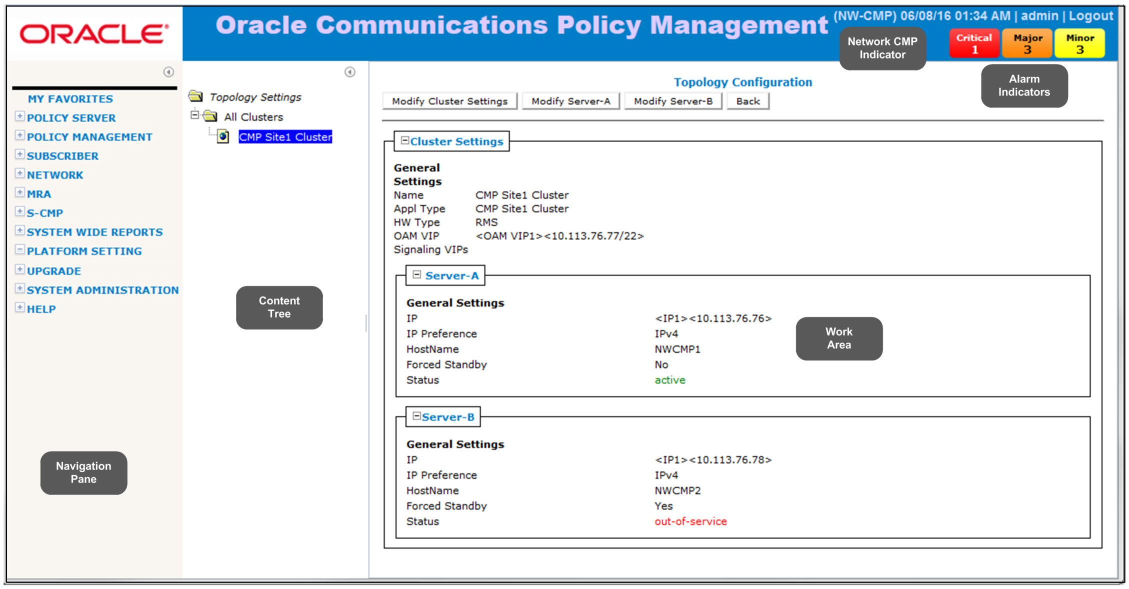
- If you log in to the standby server of a primary CMP cluster, the work area displays a message indicating that you are signed into the Primary Standby server.
- If you log in to the active server of a secondary CMP cluster, the work area displays a message indicating that you are signed in is the Secondary Active server.
- If you log in to the standby server of a secondary CMP cluster, the work area displays a message indicating that you are signed in is the Secondary Standby server.

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

GUI Overview

You interact with the CMP system through an intuitive and portable graphical user interface (GUI) supporting industry-standard web technologies (the SSL family of secure communication protocols, HTTP, HTTPS, IPv4, IPv6, and XML). Figure 1-4 shows the layout of the CMP GUI.

Figure 1-4 Layout of the CMP Window—Wireless Mode



General Settings

Name	CMP Site1 Cluster
Appl Type	CMP Site1 Cluster
HW Type	RMS
OAM VIP	<OAM VIP1><10.113.76.77/22>
Signaling VIPs	

Server-A General Settings

IP	<IP1><10.113.76.76>
IP Preference	IPv4
HostName	NWCMP1
Forced Standby	No
Status	active

Server-B General Settings

IP	<IP1><10.113.76.78>
IP Preference	IPv4
HostName	NWCMP2
Forced Standby	Yes
Status	out-of-service

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

Navigation Pane
Provides access to the various available options configured within the CMP system.
You can bookmark options in the navigation pane by right-clicking the option and selecting **Add to Favorite**. Access the bookmarks by clicking the **My Favorites** folder at the top of the

navigation pane. Within the **My Favorites** folder, you can arrange or delete options by right-clicking the option and selecting **Move Up**, **Move Down**, or **Delete from Favorite**.
You can collapse the navigation pane to make more room by clicking the button in the top right corner of the pane (◀). Click the button again to expand the pane.

Content Tree
Contains an expandable/collapsible listing of all the defined items for a given selection. For content trees that contain a group labeled **ALL**, you can create customized groups that display in the tree.

> **Note:**
>
> The content tree section is not visible with all navigation selections.

You can collapse the content tree to make more room by clicking the button in the top right corner of the pane (◀). Click the button again to expand the tree. You can also resize the content tree relative to the work area.

Work Area
Contains information that relates to choices in both the navigation pane and the content tree. This is the area where you perform all work.

Alarm Indicators
Provides visual indicators that show the number of active alarms.

Network CMP Indicator
Indicates the current CMP mode. If no mode is indicated, the mode is **CMP**.

CMP Icons

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

Add
Use this icon to add an item to a list.

Calendar
Use this icon to select a date and, in some cases, a time.

Clone
Use this icon to duplicate a selection in a list.

⊗ **Critical error**
Displays in reports to indicate a critical error during the server replication process.

🗑 **or** ✕ **Delete**
When visible in the work area, selecting the Delete icon deletes an item, removing it from the device.

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

Details
This binoculars icon displays when there is more details for an item.

Edit
Use this icon to modify a selection in a list.

External Connection
When visible in the work area, indicates which server currently has the external connection (the active server).

Gear
Displays when a policy references another policy or policy group.

Hide
When visible in the work area, selecting this 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 server.

L **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 server replication process.

⚠ **Minor error**
Displays in reports to indicate a minor error during the server replication process.

⇧⇩ **or** ▲▼ **Up/Down**
These arrow icons are displayed when you can change the sequential order of items in a list.

<-- --> **Left/Right**
These arrow icons are displayed when it is possible to move an item from one list to another.

✓ **OK status**
Displays in reports to indicate a that the blade replication process completed without error.

Remove
Removes an item from the group. The item is still listed in the **ALL** group and any other group that has an association with the item. For example, if you remove the device PS_1 from group PS_Group2, PS_1 still displays in the **ALL** group.

● **Selection**
This icon occurs in the Policy Wizard. The icon is used to select conditions and actions to add to a policy rule.

Synch broken
When visible in the Upgrade Manager, indicates that the CMP server does not have current information on a server.

Template
Displays when a field is configured by template. Hover over this icon to see the name of the template. Click the icon to view the template.

Virtual Machine
Displays when a Policy Management application is running on a virtual machine (VM).

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

Overview of Main Tasks

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

Unless otherwise specified, all procedures in this document begin with you logged in to the active CMP system.

Configuration Tasks for Setting Up the System

The system configuration tasks are a series of required steps necessary for setting up the Policy Management system. These tasks must be completed in the following order:

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

Definition Tasks for Setting Up the Network

The network element and profile definition tasks you need to perform depend on what external systems exist in your network. These tasks can be done in any order at any time. The set of tasks are as follows:

- Create network element profiles, including protocol options, for each network element with which Policy Management devices interact. This task is described in Managing Network Elements.

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

Administration Tasks for Managing the System

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

- View reports on the function of the Policy Management systems in your network. This task is described in System-Wide 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 Functions.

2 Configuring the Policy Management Topology

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

About the Policy Management Topology

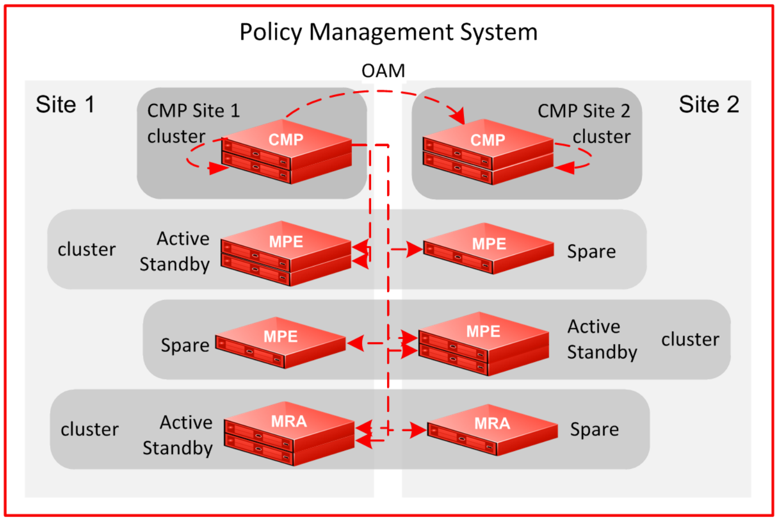
Topology determines the following:

- How component devices and clusters communicate with each other
- Which sites are primary and which are secondary
- How configuration data is replicated
- How incidents (events and alarms) get reported to the CMP system or external network management systems.

The Policy Management topology is composed of CMP, MPE, and MRA devices.

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

Figure 2-1 Example Policy Management Topology



As the figure shows:

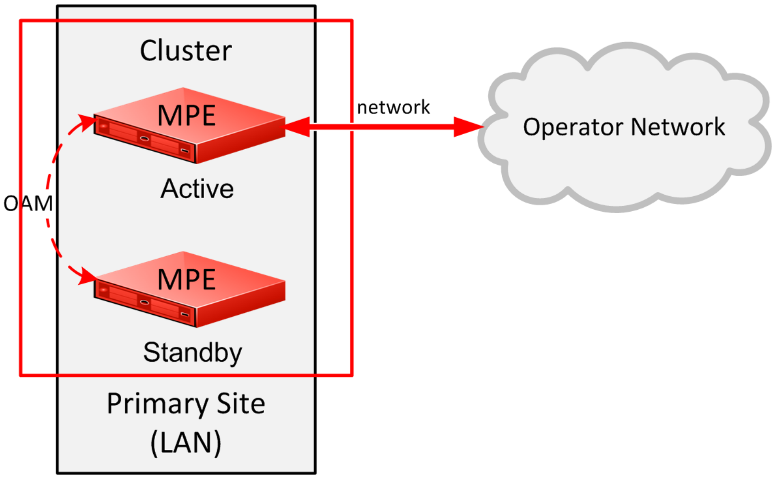
- The active CMP Site 1 server replicates its data to its standby CMP server and the active CMP server at CMP Site 2.
- In turn, the active CMP Site 2 server replicates its data to its standby CMP server.

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

High Availability

Policy Management provides High Availability (HA) to all Policy Management cluster configurations. Policy Management accomplishes HA by using two servers per cluster, an active server and a standby server. For georedundancy, a third, spare server provides additional backup support. Servers are continually monitored by the in-memory database. As shown in Figure 2-2, the active server processes network traffic and is accessible and connected to external devices, clients, gateways, and so forth. Only one server in a cluster can be the active server.

Figure 2-2 High Availability



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

1. The active and standby servers communicate using a TCP connection over the Operation, Administration, and Management (OAM) network to replicate current state data, monitor server heartbeats, and merge trace logs and alarms.

   > **Note:**
   >
   > For georedundancy, a third, spare server is part of the cluster and receives replication data and heartbeats.

2. The servers share a virtual IP (VIP) cluster address to support automatic failover. The active server controls the VIP address.
3. The standby server does not receive any live traffic load, but holds an up-to-date copy of the active session state data at all times, replicated by High Availability. (This is sometimes called a warm standby.)
4. The HA database runtime processes on each server constantly monitor server status using heartbeat signals.

5. If the active server fails, indicated by missing a succession of three heartbeats:
   a. The standby server queries the active server. If the active server fails to respond, the standby server assumes the active state and takes over the VIP address and connections.
   b. Because it continually receives session state and data updates through replication, the standby server can assume processing of ongoing sessions, so the failover is automatic and transparent to other components.

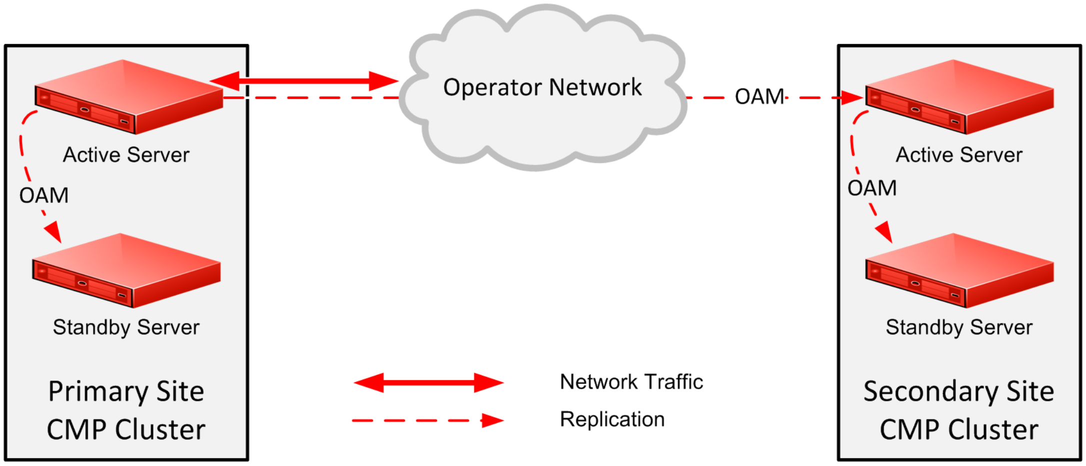
The terms active and standby denote roles, or states, that the servers assume, and these roles can change based on decisions made by the underlying HA database, automatically and at any time. If necessary, the standby server assumes control and becomes the active server. (For example, this would occur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

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

CMP Georedundancy

As shown in Figure 2-3, georedundancy is implemented for CMP clusters by pairing a primary site CMP cluster with a secondary site cluster. The active server from the Site 1 CMP cluster will continuously replicate configuration, provisioning, and policy data, using HA, to the active server of the Site 2 cluster.

Figure 2-3 CMP Georedundancy



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

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

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

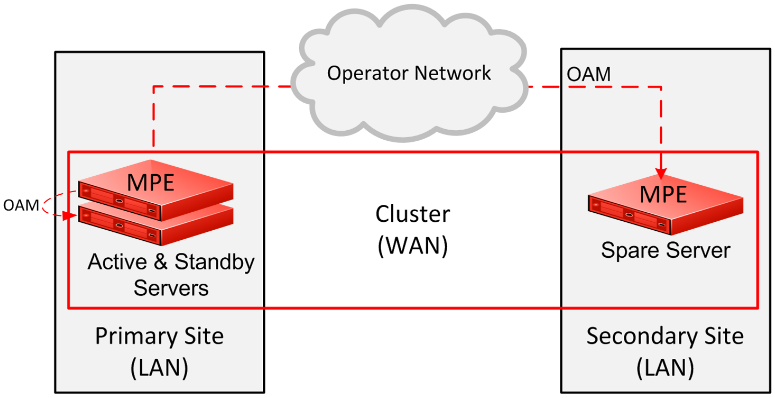
> **Note:**
>
> CMP servers do not use the replication (REP) network or Differentiated Service Code Point (DSCP) marking.

Georedundancy for Non-CMP Servers

Georedundancy is an optional configuration provided for non-CMP clusters in which the spare server can be located in a separate geographical location, as shown in Figure 2-4. The active server replicates state data to the standby and spare servers. If the two servers at one site become unavailable, the third server, located at the other site, automatically becomes the active server and continues to provide service. You can designate sites as primary and secondary.

Georedundancy supports both session-stateful (at the MPE device level) and binding-stateful (at the MRA device level) 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 2-4 Non-CMP Georedundant Configuration for Wireless



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

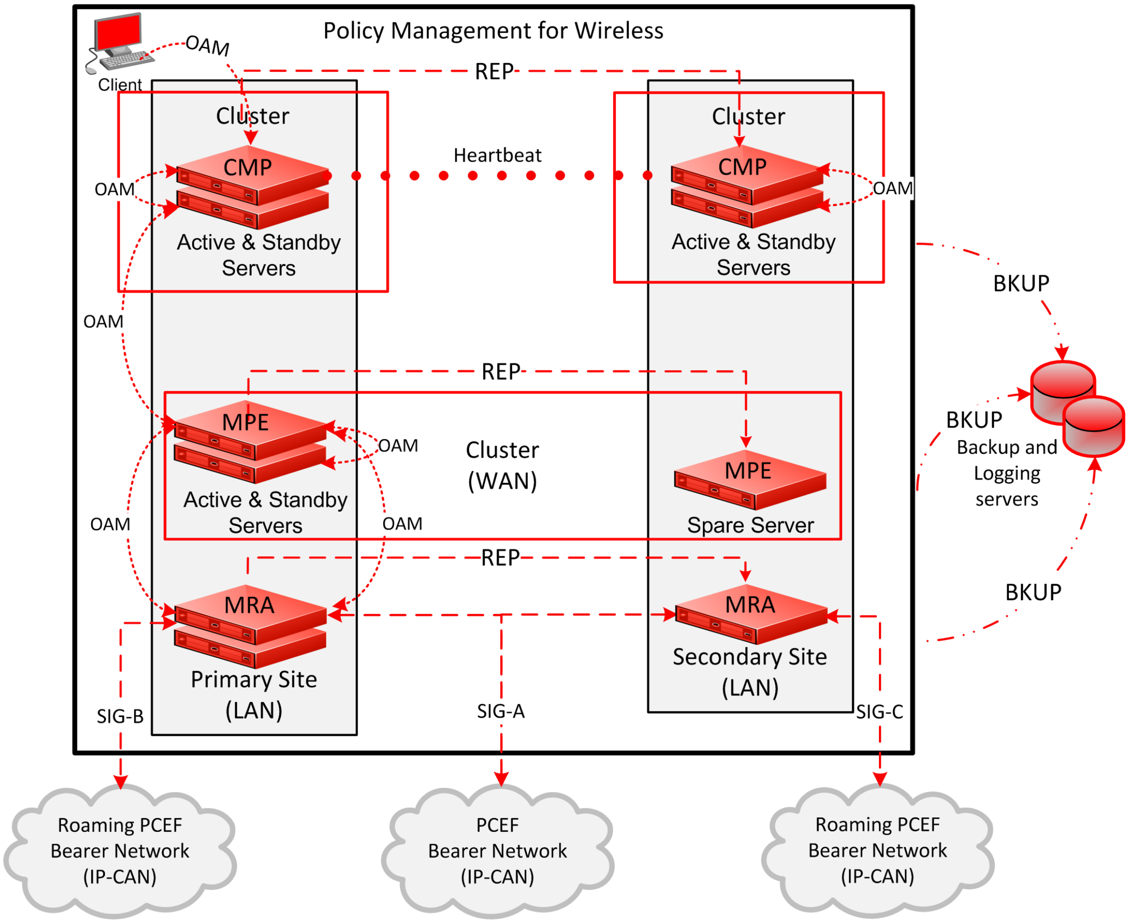
- Gateways, content filters, application servers, and other clients are connected to active MRA devices. Each client has a primary connection to the active MRA device at one site and a secondary connection to the active MRA device at the other site. (This is no different than the client connections in a non-georedundant topology.)

- Active MPE devices establish Sh connections, either directly or through Diameter Routing Agents (DRA), to SPRs. The active MPE device at the primary site establishes an Sh connection with a primary IP address, and the spare MPE device at the secondary site establishes an Sh connection with a secondary IP address for use if the spare is promoted to an active role.
- The active MPE devices establish Sy connections, either directly or through DRAs, to online charging servers (OCSs). The active MPE device at the primary site establishes an Sy connection with a primary IP address, and the spare MPE device at the secondary site establishes an Sy connection with a secondary IP address for use if the spare is promoted to an active role.

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

Within a georedundant cluster, the active and standby servers are connected through a local area network (LAN), that uses a single TCP/IP socket connection or stream. The active and spare servers, located at separate sites, are connected through a wide area network (WAN) Figure 2-5. 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.

Figure 2-5   Wireless Georedundant System with Spare CMP Cluster



Diameter Signaling

Diameter signaling traffic is carried on a virtual LAN (VLAN) Signaling A (SIG-A) network, a SIG-B, or SIG-C network. Database replication and high-availability (HA) heartbeat traffic within a site (that is, between the active and standby servers) is sent on an Operation, Administration, and Management (OAM) VLAN network. You can configure the Policy Management topology to send replication and HA heartbeat data between sites (that is, between the active and spare servers) using different VLANs. Replication data can be sent between sites on the OAM (default), SIG-A, SIG-B, SIG-C, 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, servers (with a 1x4 mezzanine card) can communicate with logging and backup servers over a dedicated backup (BKUP) network. However, for Policy Management applications, only backup of CMP systems is typical.

Replication (REP) 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

Drop Probability	Class 1	Class 2	Class 3	Class 4
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, SIG-C, 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.

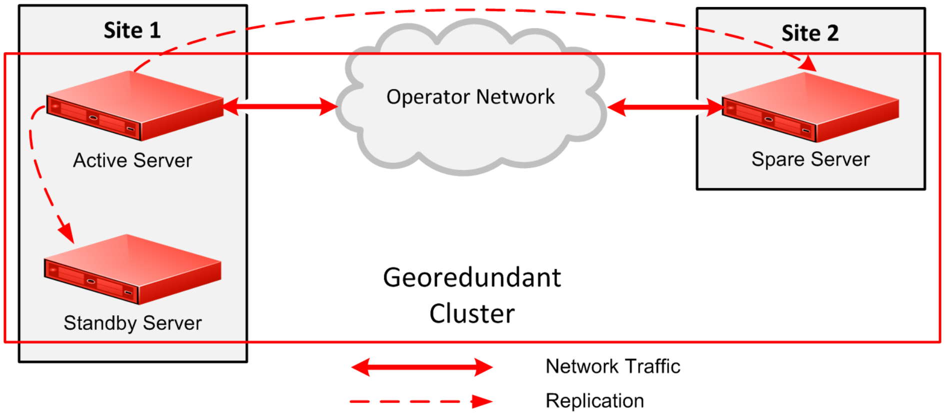
The primary HA heartbeat path is the same as the replication path. The default primary HA heartbeat and replication path is the OAM network. If you configure a different network to carry replication traffic, then that network is also used as the primary HA heartbeat network. In this case, the OAM network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

Georedundant Spare Servers

As shown in Figure 2-6, an MPE or MRA cluster can contain an additional georedundant server, called a spare server. The active server will replicate its database to the standby server as well as the spare server. In this configuration, the standby server is first in line to take over from the active server and the spare is second in line.

Figure 2-6 Clusters with Active, Standby, and Spare Servers



Active, standby, and spare servers interoperate as follows:

1. The servers communicate using WAN TCP streams to perform replication, monitor heartbeats, and merge events.
2. The active and standby servers share a common virtual IP (VIP) cluster address to support automatic failover.
3. The spare server has a unique VIP cluster address.

4. The HA database runtime process constantly monitors the status of all servers.
5. If the standby server does not receive three consecutive heartbeats, it attempts to communicate with the active server. If the standby server receives no response from the active server, it assumes the active role.
6. When HA misses the three heartbeats to the spare server, it instructs the spare server to assume the standby role.

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

Primary and Secondary Sites

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

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

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

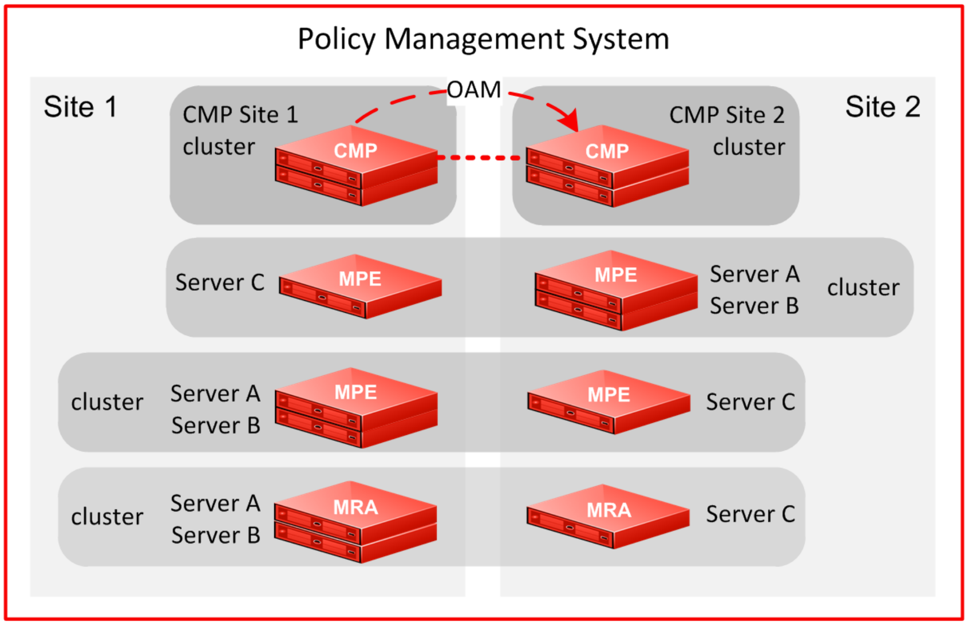
If and only if no servers are available at an MPE or MRA primary site, the cluster fails over to the secondary site, and a spare server takes over as the active server in the cluster and provides service. When one of the servers at the primary site is able to provide service, then the active status reverts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

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

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

It is not meaningful to describe a site as primary except in the context of where the active server of a cluster is located. For example, as shown in Figure 2-7, you could establish a topology with two sites and two MPE clusters, with the spare server of each cluster located at the other site. In this topology, the primary site of Cluster 1 is also the secondary site of Cluster 2, and vice versa.

Figure 2-7 Example of Primary and Secondary Sites



Georedundant Site Preferences

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

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

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

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

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

Server Status

You can view the status of a server in the **Cluster Information Report** (see Cluster Information Report).

> **Note:**
>
> The display refreshes every 10 seconds. Click **Pause** to freeze the page.

The status of a server can be thought of as its current role. The status describes what function the server is currently performing, or performing in a 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.

> **Note:**
>
> Two servers in the same cluster with the same status is an error condition.

The server status values are as follows:

Active
An active server is externally connected. In a cluster, the active server is the only server that is handling connections and servicing messages and requests. Only an 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 at the primary site is available to provide service.

Standby
A standby server is the server in a cluster 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. When the previously active server has recovered, it reverts to its former status of standby server.

Spare
A spare server is the server in an MPE or MRA cluster 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 demotes itself and reverts to its 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 its status is out of service. A server is reported as out of service in two scenarios:

- The CMP system can reach the server, but the software service on the server is down.
- The CMP system cannot reach the server.

No Data
The CMP system cannot reach the server. This status value provides backward compatibility with earlier Policy Management releases. It is seen during the upgrade process.

About Virtualization

The Policy Management system can operate as a standard virtualized hardware system with virtual machines loaded onto qualified hardware elements or as an ETSI-defined Network Functions Virtualization (NFV) Management and Organization (MANO) system where orchestrator software (such as, OpenStack) handles the network-wide orchestration and management of the NFV (infrastructure and software) resources and the NFV service topology on the NFV infrastructure. See NF Agent for VNF Management for more information.

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

The qualified hardware configurations includes:

- HP Enterprise DL360/DL380 Gen8

The qualified VM manager/hypervisor software includes:

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

Kernel-based Virtual Machine (KVM)
With or without OpenStack

VMware ESXi
VMware vSphere

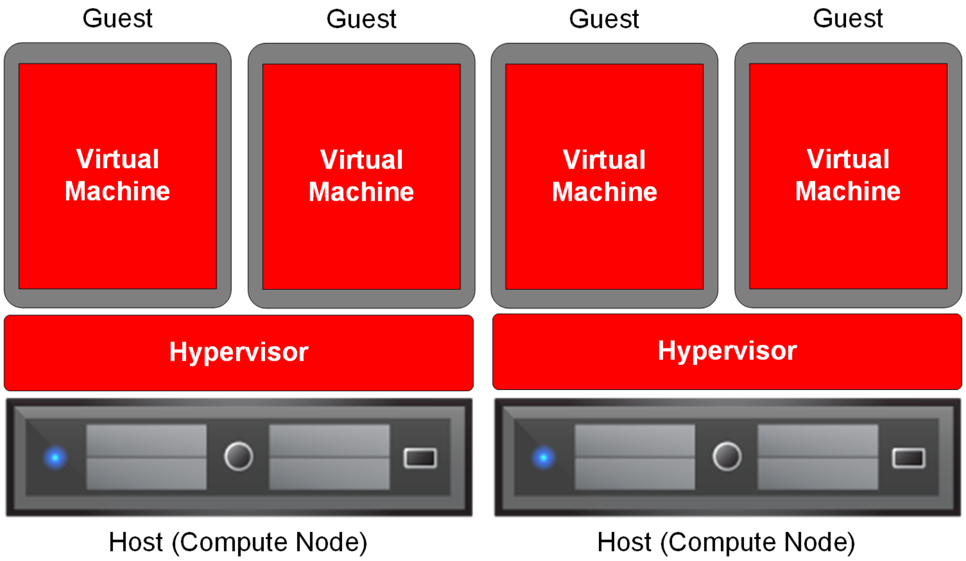
Kernel-based Virtual Machine (KVM)
No VM Manager (for server configuration)

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

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

Figure 2-8 illustrates the virtualization architecture.

Figure 2-8 Virtualization Architecture



The virtualized environment supports the multiple network interface connections (OAM, SIG A, SIG B, SIG C, REP, and BKUP) used by Policy Management applications by mapping virtual Ethernet devices as if they were separate physical devices. The virtualized environment supports HA by defining affinity, so that the hypervisor maintains a standby VM on a different host system from the active VM. The virtualized environment calculates key performance indicators (KPI) such as performance, capacity, and load factor by dynamically obtaining the current resources, and the **KPI Dashboard** indicates if a server is running as a virtual machine (see KPI Dashboard).

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

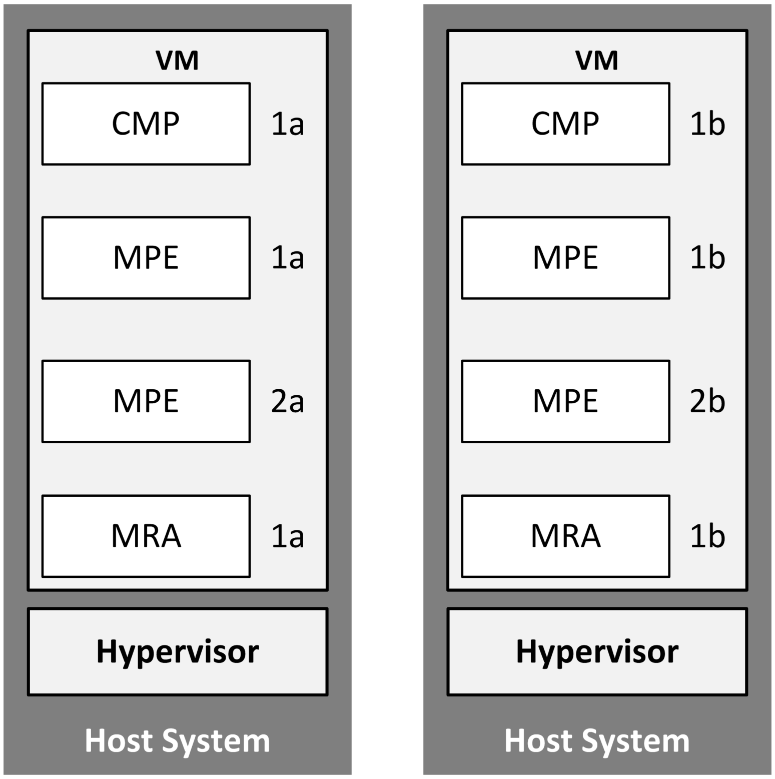
An alternate supported configuration is to include all the Policy Management VMs on a pair of HP Enterprise DL360/DL380 Gen8 blade host-based systems, running Oracle Enterprise Linux (OEL) with either the KVM, OVM-M, or VMware ESXi hypervisor, as a fully functional, high-availability, entry-level, minimal-footprint solution consisting of the following:

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

Figure 2-9 shows this minimum Policy Management virtualized topology.

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

Figure 2-9   Policy Management Minimum Virtualized Topology



Refer to *Virtual Installation Guide* for detailed information on creating Virtual Network Function Components (VNFCs) (for example, CMP, MPE, and MRA devices) on a host system.

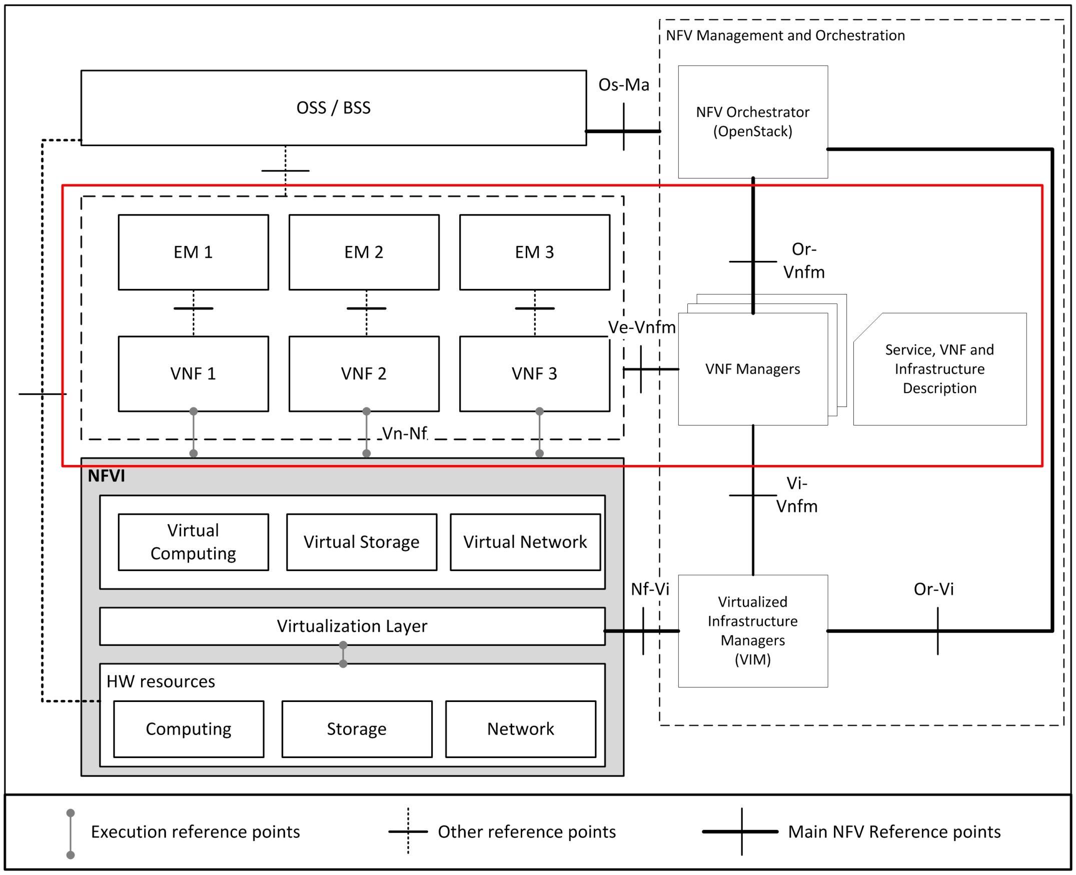
Once a virtualized host system is implemented, adding VNFCs to the Policy Management system is as simple as adding a server. See About Setting Up the Topology for details.

About VNF Management

Policy Management NF Agent implements support for VNF management functionality within the MPE. The NF Agent provides VNF management services as well as act as a point of integration with orchestrator software (for example, OpenStack) and VIM APIs that manage our VNF/VM lifecycle's. The NF Agent provides the logical interface and mappings between virtual deployments and internal Policy objects and logic. VIM connections work with the OpenStack API, the OpenStack HEAT API, and VMWare vCloud..

Figure 2-10 illustrates the NFV management and orchestration (MANO) interfaces. VNF Managers are logical objects that interface with VNF instances (VNF 1, VNF 2, and VNF 3), the Orchestrator function and the VIMs (see red rectangle). For this release, Policy Management provides a policy application service that will allow the MPE to support virtual deployment within an NFVI (Ve-Vnfm and Vi-Vnfm interfaces). The intent is to support an environment where the MPE is asked to provide its own VNF-M capabilities for deployment and horizontal scaling. Having VNF application-specific logic is important for proper VNF Descriptor (VNFD) calculations and orchestration.

Figure 2-10 ETSI VNF MANO Interfaces



NF Agent for VNF Management

The Network Function Agent (NF Agent) provides VNF (Virtual Network Function) management services as well as acting as a point of integration with Orchestrator software (like OpenStack) and VIMs (Virtual Infrastructure Managers) APIs that manage the VNF/VM lifecycles. The NF Agent provides the logical interface and mappings between virtual deployments and internal Policy objects and logic. The NF Agent has the responsibility of handling specific network functions that run on one or more virtual machines (MPE servers or MRA servers).

VNF management provides a set of services and functionality that allow for a virtual instance of an application (that is, VNF) to be instantiated, managed, and destroyed.

The NF Agent is a web service hosted on the same server that hosts the CMP server. As an independent service, the NF Agent encapsulates virtual operations and VIM and Orchestrator interfaces. The NF Agent keeps mappings between logical MPE and MRA devices as well as VNF, VM, VNFD (Virtual Network Function Descriptor) instances. The NF Agent provides support for the following VIM connection types:

- OpenStack API
- OpenStack HEAT API
- VMWare vCloud

The NF Agent functions as a service with a northbound RESTful API and multiple southbound client interfaces for various VIMs. The architecture provides sufficient flexibility for the easy implementation of additional VIM clients. The NF Agent expects the following VM profile and deployment information to the VIM so it can instantiate instances of the described VNF:

- Required vCPUs
- Required vNICs
- Required Networks and IP addressing
- Memory size
- Storage size
- Anti-affinity/Affinity requirements

Orchestration cases are manually implemented through the **Topology Settings** command. The user specifies operations on a new VNF.

Before Setting Up the Topology

Prior to setting up the topology, the server hardware must have been set up and configured as described in *TPD Initial Product Manufacture Software Installation Procedure*. This includes installing TPD, TVOE, and PMAC software, setting up the enclosure and network connections, and installing Policy Management application software (for CMP, MPE and MRA devices).

About Planning the Topology

Before beginning to set up your topology, you will need to gather the information needed to input into the servers' set up forms.

The Platform Configuration (`platcfg`) utility is used to set up and configure the hardware as well as install the proper Policy Management application software (that is, MPE, CMP, MRA).

> **Tip:**
>
> This information can be collected at any time before beginning the topology set-up procedure without interrupting service.

For more information, refer to *Platform Configuration User's Guide*.

Topology planning information includes the following:

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

Information entered using the Platform Configuration utility includes the following:

- Initial provisioning information for servers:
  - A host name
  - For CMP server access, an OAM Real IP address and subnet mask (IPv4 or IPv6)
  - An OAM IPv4/IPv6 default route (default gateway)
  - A list of network time protocol (NTP) server IP addresses
  - A list of domain name system (DNS) server IP addresses
  - Bond interface for the OAM device
  - Backplane bond interface of the OAM device
  - VLAN IDs for OAM, REP, SIG-A, SIG-B, and SIG-C 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
- 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
  - Verify that firewall rules are correctly provisioned

About Setting Up the Topology

Setting up the topology consists of configuring Policy Management sites and clusters, including their IP addresses and hierarchy. You can add MPE and MRA clusters to the topology before configuring the individual server profiles. You can set up all the servers in a cluster in the same operation.

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

1. Add a CMP Site 1 cluster as described in Setting Up a CMP Cluster.

   > **Note:**
   >
   > The primary CMP cluster cannot be deleted from the Policy Management topology.

2. (Optional) Add a Site 2 CMP cluster.
   See Setting Up a CMP Cluster for details.

   > **Note:**
   >
   > A Site 2 CMP cluster can provide georedundancy.

3. Add non-CMP (MPE and MRA) clusters.
   See Setting Up a Non-CMP Cluster for details.
4. (Optional) For georedundancy, configure sites and additional MPE and MRA clusters.
   See Setting Up a Georedundant Site and Setting Up a Georedundant Non-CMP Cluster for details.
5. After setting up the topology, the topology settings are replicated as follows:
   a. The active CMP server replicates the topology configuration, including the cluster settings, to active, standby, and (if present) spare servers over the OAM network. These servers form an MPE or MRA cluster based on the topology configuration. The servers have the following communication restrictions:
      - 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.
      - Active and standby servers share a virtual IP (VIP) address to support automatic failover.
      - If present, the spare server has a unique VIP address.
   b. The HA database runtime process constantly monitors the status of the servers in each cluster and, in the event of a server or servers failure, triggers the following actions:
      - If an active server in a cluster fails, the standby server takes over and becomes the active server.
      - In a georedundant topology, if both the active and standby servers in a cluster fail, HA instructs the spare server to take over and become the active server.
6. After you set up the topology, view the **System** tab of each server and determine if there are any configuration mismatches. See About Reapplying a Configuration for more information.

About Setting Up a CMP Cluster

You must set up at least one CMP cluster before proceeding with setting up the topology. The first CMP cluster you set up is called the CMP Site1 (or Primary) cluster. You can optionally set up a CMP Site2 (or Secondary) cluster.

Before defining the CMP Site1 cluster, ensure the following:

- The CMP application 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.

Setting Up a CMP Cluster

To set up a CMP cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

If a CMP Site1 cluster is not yet defined, a message appears asking you to add CMP Site 1 cluster.

2. Click **Add CMP Site1 Cluster**.

   The Topology Configuration page opens.

   > **Note:**
   >
   > The **Name** and **Appl Type** fields are fixed.

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

   Available options are:

   - **C-Class** (default)—HP Enterprise ProLiant BL460 Gen8 server
   - **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment)—HP Enterprise ProLiant BL460 Gen8
   - **RMS**
   - **VM**—virtual machine

4. If you selected **C-Class** or **C-Class(Segregated Traffic)**, enter the **General Network - VLAN IDs**.

   Enter the **OAM**, **SIG-A**, and (optionally) **SIG-B** virtual LAN (VLAN) IDs.

   VLAN IDs are in the range 1 to 4095. The default values are:

   - **OAM**—3
   - **SIG-A**—5
   - **SIG-B**—6

5. Click **Add New VIP**.

   The New OAM VIP dialog box appears:

   a. Enter the OAM VIP and the mask.

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

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

   b. Click **Save**.

      The OAM VIP and mask are saved.

   c. Repeat this step for a second OAM VIP, if needed.

6. (Optional) To enter up to four signaling VIPs, click **Add New VIP**.

   The New Signaling VIP dialog box appears:

a. Enter the signaling VIP and the mask.

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

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

b. From the **Interface** list, select one of the following:
   - **SIG-A**
   - **SIG-B**

c. Click **Save**.

   The signaling VIP and mask are saved.

d. Repeat this step for up to three additional signaling VIPs.

7. Configure the active server by doing the following:

   a. Click **Add New IP**.

      The New IP dialog box appears.

   b. Enter the IP address for the server.

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

   c. Select the preferred IP address format.

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

      > **Note:**
      >
      > The following restrictions apply:
      >
      > - If neither an IPv6 OAM IP nor a static IP address is defined, IPv6 is not available.
      > - If neither an IPv4 OAM IP nor a static IP address is defined, IPv4 is not available.

   d. Click **Save**.

      The IP address for the active server is saved as Server A.

8. (Optional) To enter a second **IP** address, repeat the previous step.

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

9. Enter the host name for the server.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This name must exactly match the host name for this server (that is, the output of the Linux command `uname -n`).

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

10. Select **Forced Standby**, which forces the server into standby mode.

    > **Note:**
    >
    > The state is set automatically when a new server is added to a cluster or if a server setting is modified and another server already exists in the cluster.

11. Click **Save**.

    A confirmation message appears.

12. Click **OK**.

    A restart message appears.

13. Click **OK**.

    The active server restarts.

14. Log back in to the CMP server.

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

    The Cluster Configuration page opens; the initial group is **All Clusters**.

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

    The Topology Configuration page opens.

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

18. Click **Save**.

The CMP cluster topology is defined.

After you define the topology, use the **System** tab of each server to determine if there are any topology mismatches. See About Reapplying a Configuration for more information.
After you define the primary CMP cluster, you can repeat this procedure to define a georedundant secondary CMP cluster. See Setting Up a Georedundant Site before adding a secondary CMP cluster.

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

About Setting Up a Non-CMP Cluster

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

- MRA

> **Note:**
>
> The list of available server types depends on the CMP modes configured. See CMP Modes for more information.

> **Note:**
>
> If you are creating a cluster in a georedundant system, see Setting Up a Georedundant Non-CMP Cluster.

Setting Up a Non-CMP Cluster

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

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

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

   The **Cluster Configuration** page opens; the initial group is **All Clusters**.

2. From the work area, select **Add MPE/MRA**.

   > **Note:**
   >
   > The list of available cluster types to add to the topology depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

   The Topology Configuration page opens.

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

   a. (Required) Enter the **Name** for the cluster.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.

   b. Select the **Appl Type** from the list.

      Available options are:

      - MPE (default)
      - MRA

      > **Note:**
      >
      > The list of available application types depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

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

      Available options are:

- **C-Class** (default)—HP ProLiant BL460 Gen8 server
- **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 Gen8
- **RMS** (rack-mounted server)—HP ProLiant DL380 Gen8 server
- **VM** (virtual machine)
- **VM(Automated)** (VM managed by NF Agent)
  See Setting Up a VM (Automated) Non-CMP Cluster for details on adding a VM (Automated) cluster.

d. If needed, repeat the process for the second OAM VIP.

e. (Optional) To enter up to six **Signaling VIPs** addresses (up to two each for each of SIG-A, SIG-B, and SIG-C), click **Add New VIP**.

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

   The New Signaling VIP dialog appears.

   i. Enter the **Signaling VIP** address and the **Mask**.
      This is the IP address the CMP server uses to communicate with an external signaling network.

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

   ii. Select the **Interface** from the list.
      Available options are:
      - SIG-A
      - SIG-B
      - SIG-C

   iii. Click **Save**.
      The **Signaling VIP** address and **Mask** are saved.

f. Repeat the process for any remaining Signaling VIPs.

g. If the hardware type is **C-Class**, **C-Class(Segregated Traffic)**, configure the **General Network** settings:

   i. Enter the **OAM VLAN ID**.
      The default value is `3`.

   ii. Enter the **SIG-A VLAN ID**.
      The default value is `5`.

   iii. (Optional) Enter the **SIG-B VLAN ID**.
      The default value is `6`.

   iv. (Optional) Enter the **SIG-C VLAN ID**.
      The default value is `7`.

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

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

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

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

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

      The Add New IP dialog box appears.

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

      ii. Select the **IP Preference**.
         Either **IPv4** or **IPV6**. If **IPv6** is selected, the server will preferentially use the IPv6 address for communication.

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

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

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

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

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

5. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster.

   Server-B is defined for the cluster.

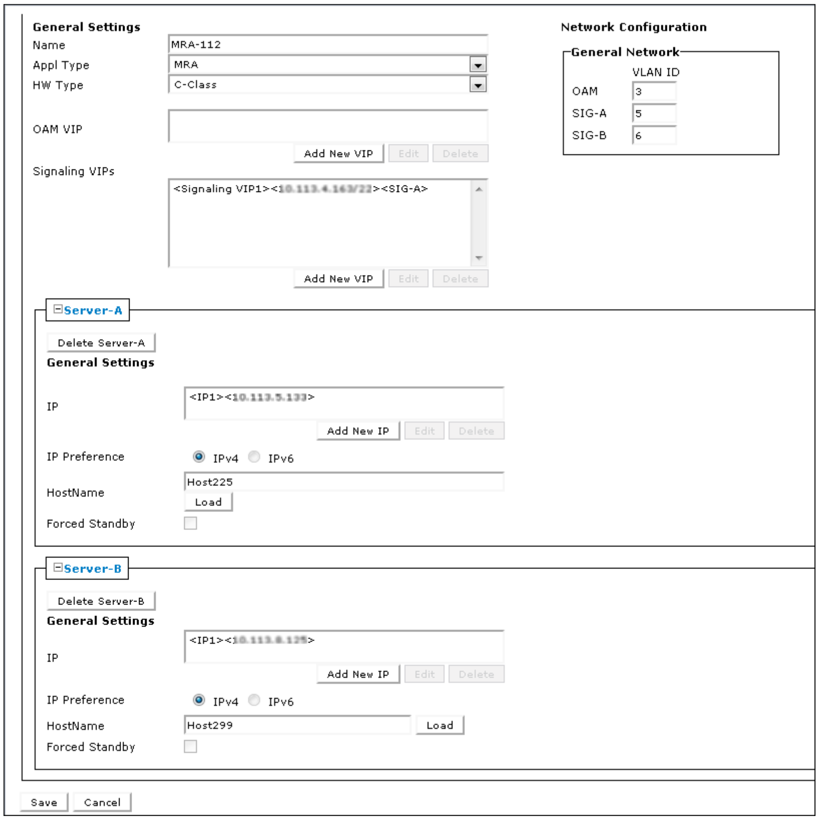
6. Click **Save**.

   A confirmation message appears.

7. Click **OK**.

Figure 2-11 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 2-11 Sample Cluster Topology Configuration



General Settings

Name: MRA-112

Appl Type: MRA

HW Type: C-Class

OAM VIP:

Signaling VIPs: <Signaling VIP1><[redacted]><SIG-A>

Network Configuration

General Network

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

Server-A

General Settings

IP: <IP1><[redacted]>

IP Preference: ● IPv4 ○ IPv6

HostName: Host225

Forced Standby: □

Server-B

General Settings

IP: <IP1><[redacted]>

IP Preference: ● IPv4 ○ IPv6

HostName: Host299

Forced Standby: □

Setting Up a VM (Automated) Non-CMP Cluster

Before defining a VM (Automated) non-CMP cluster, ensure the system is configured for virtualization and VIM Connections are defined.

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. If you do not see the Cluster Configuration page, click **All Clusters**.
3. From the work area, select **Add MPE/MRA**.

   > **Note:**
   >
   > The list of available cluster types to add to the topology depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

   The Topology Configuration page opens.

4. In the **Cluster Settings** section of the page:
   a. (Required) Enter the **Name** for the cluster.

      Enter up to 250 characters, excluding quotation marks (") and commas (,).

   b. Select the **Appl Type** from the list.

      Available options are:

- **MPE** (default)
- **MRA** (Wireless Mode)

> **Note:**
>
> The list of available application types depends on the CMP modes configured. See the *CMP Wireless User's Guide* for more information.

c. Select **VM(Automated)** from the **HW Type** list.

d. If needed, repeat the process for the second OAM VIP.

e. (Optional) Click **Add New VIP**.You can enter up to six **Signaling VIPs** addresses (up to two for each SIG-A, SIG-B, and SIG-C).

   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, SIG-B, or SIG-C for carriers who use redundant signaling channels.

   The New Signaling VIP dialog box appears.

   i. Enter the **Signaling VIP** address and the **Mask**.
      This is the IP address the CMP server uses to communicate with an external signaling network.

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

   ii. Select the **Interface** from the list.
      Available options are:

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

   iii. Click **Save**.
      The **Signaling VIP** address and **Mask** are saved.

f. Repeat the process for any remaining Signaling VIPs.

5. Configure Server-A using VM (Automated). In the **Server-A** section of the page:

   a. Select the **VIM Connection** from the list.

      If the list is empty or your connection is not listed, it may need to be created. See Creating a VIM Connection for details about creating connections.

   b. Verify that the VIM Connection Type is correct.

      You cannot change this field. If the connection is not correct, select another VIM connection, or create a new one. See Creating a VIM Connection for details about creating a new connection.

   c. If the server type is VMWare vCloud, configure the following fields:

        i. Select the **Virtual Data Center** from the list of network ports or networks.

        ii. Select the **Catalog** from the list.

        iii. Select a **VM** (Virtual Machine) from the list.

        iv. Enter a **vApp Name** site name is default, or it can be manually entered.
        The vApp Name indicates what vApp to associate with the current Virtual Machine.

        v. Enter the **NTP Server**.

    d. If the server type is OpenStack API or OpenStack Heat, configure the following fields:

        i. Select the **Image** from the list.

        ii. Select the**Flavor** from the list.

        iii. Select an **Availability Zone** from the list.

        iv. Verify the Config Drive.
        You cannot change this field.

        v. Enter the **NTP Server**.

        vi. Click **Add New** to add a DNS server.

        vii. Click **Add New** to add a DNS search.

        viii. Click **Manage** to add Security Groups.

    e. Click **Add New IP** to add an **IP** address.

    f. Select the **IP Preference** as either **IPv4** or **IPv6**.

    g. Click **Add New IP** to add an **IP** address.

    This is a fixed IP address for the VM device.

    h. Enter the **HostName**.

    i. Select to have the server in **Forced Standby**, see Changing Server Status to Forced Standby.

    j. Click **Add New** to add a new **Static IP** address.

6. (Optional) Click **Add Server-B** and enter the information for the standby server of the cluster.

    Server-B is defined for the cluster.

7. Click **Save**.

    A confirmation message appears.

8. Click **OK**.

About Setting Up a Georedundant Cluster

Before setting up georedundant clusters, you must create one or more georedundant sites. You can only create georedundant sites when **Manage Geo-Redundant** mode is enabled (see CMP Modes). See Setting Up a Georedundant Site for detailed information.

> **Note:**
>
> Before setting up sites, you should plan your Policy Management topology to determine site naming conventions.

Georedundant sites can contain one or more of the following clusters:

- MPE
- MRA

> **Note:**
>
> A site name is required when configuring georedundant non-CMP devices.

Setting Up a Georedundant Site

> **Note:**
>
> Sites may only be created when **Manage Geo-Redundant** mode is enabled. See CMP Modes for details.

To set up a georedundant site:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. From the content tree, select **All Sites**.

   The Site Configuration page opens.

3. Click **Create Site**.

   The New Site page opens.

4. (Required) Enter the **Name** for the site.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 35 characters.

5. Enter the number for **Max Primary Site Failure Threshold**.

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

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

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

   The available options are:

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

- **VM (Automated)** for a VM managed by NF Agent

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

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

   a. Enter the **OAM VLAN ID**.

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

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

   d. (Optional) Enter the **SIG-C VLAN ID**.

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

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

9. Click **Save**.

The CMP database saves the site configuration.
To define multiple sites, repeat the procedure starting at step 3.

Setting Up a Georedundant Non-CMP Cluster

> **Note:**
>
> Georedundancy requires that you configure the CMP system with **Manage Geo-Redundant** enabled. See the *CMP Wireless User's Guide* for more information.

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

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

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

- MRA

> **Note:**
>
> The list of available server types depends on the CMP modes configured.

> **Note:**
>
> If your system is not set up for georedundancy, see Setting Up a Non-CMP Cluster.

To set up a georedundant non-CMP cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. From the work area, select **Add MPE/MRA**.

The Topology Configuration page opens.

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

   a. (Required) Enter the **Name** for the site.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 35 characters.

   b. Select an **Appl Type**.

      > **Note:**
      >
      > The list of available cluster types to add to the topology depends on the CMP modes configured.

   c. Select the **Site Preference**.

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

   d. Select the **Replication Stream Count**.

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

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

      This field only is visible if the system supports georedundancy:

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

      > **Note:**
      >
      > When saving a configuration using **SIG-C**, a confirmation appears. Click **OK**. The **RMS** option for **HW Type** is removed until all configured Signaling C VIPs or **SIG-C** interfaces in static IP are removed.

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

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

      > **Note:**
      >
      > When saving a configuration using **SIG-C**, a confirmation message appears. Click **OK**. The **RMS** option for **HW Type** is removed until all configured Signaling C VIPs or **SIG-C** interfaces in static IP are removed.

> **Note:**
>
> This field only is visible if the system supports georedundancy.

Available options are:

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

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

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

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

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

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

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

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

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

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

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

   Available options are:

   - **C-Class** (default) – HP ProLiant BL460 Gen8 server
   - **C-Class (Segregated Traffic)** (a configuration where Signaling and other networks are separated onto physically separate equipment) – HP ProLiant BL460 G8
   - **RMS** (rack-mounted server) – HP ProLiant DL360 Gen8 or HP ProLiant DL380 Gen8 server
   - **VM** (virtual machine)

- **VM(Automated)** (VM managed by NF Agent)
  See Setting Up a VM (Automated) Non-CMP Cluster for details on adding a VM (Automated) cluster.

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

   The New OAM VIP dialog box appears.

   i. Enter the **OAM VIP** address and the **Mask**.
      This is the IP address the CMP server uses to communicate with a Policy Management cluster.

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

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

e. (Optional) To enter up to six **Signaling VIPs** addresses (up to two each for each of SIG-A, SIG-B,and SIG-C), click **Add New VIP**.

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

   The New Signaling VIP dialog box appears.

   i. Enter the **Signaling VIP** address and the **Mask**.
      This is the IP address the CMP server uses to communicate with an external signaling network.

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

   ii. Select the **Interface** from the list.
       Available options are:

       - SIG-A
       - SIG-B
       - SIG-C

   iii. Click **Save**.
        The **Signaling VIP** address and **Mask** are saved.

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

   i. Enter the **OAM VLAN ID**.

The default value is `3`.

ii. Enter the **SIG-A VLAN ID**.
The default value is `5`.

iii. (Optional) Enter the **SIG-B VLAN ID**.
The default value is `6`.

iv. (Optional) Enter the **SIG-C VLAN ID**.
The default value is `7`.

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

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

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

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

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

The Add New IP dialog box appears.

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

ii. Select the **IP Preference**: **IPv4** or **IPV6**.
The server will preferentially use the IP address in the specified format for communication.

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

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

The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

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

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

d. In the **Path Configuration section**, to add a **Static IP**, click **Add New**.

   The New Path dialog box appears.

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

   i. Enter a **Static IP** address and **Mask**.

   ii. Select the **Interface**:

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

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

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

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

      The Add New IP dialog box appears.

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

      ii. Select the **IP Preference**: **IPv4** or **IPV6**.
      The server will preferentially use the IP address of the specified format for communication.

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

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

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). This must exactly match the host name provisioned for this server (the output of the Linux command `uname -n`).

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

   c. Select **Forced Standby** to put Server-B into forced standby.

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

d. In the **Path Configuration section**, to add a **Static IP**, click **Add New**.

   The New Path dialog box appears.

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

   i. Enter a **Static IP** address and **Mask**.

   ii. Select the **Interface**:

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

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

7. Click **Save**.

   A confirmation message appears.

8. Click **OK**.

9. If you are setting up multiple clusters, repeat this procedure.

The cluster is defined.

Example: Adding Georedundancy to an Existing Topology

This example describes how to:

- Add a georedundant secondary site, Site-2, to an existing Policy Management topology
- Add a third spare server (Server-C), located at Site-2, to an existing active/standby MPE cluster located at the primary site, Site-1

> **Note:**
>
> If the primary site was to fail, the spare server would assume the active role.

The example 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 servers in the topology are using 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.

Gather required information. See About Planning the Topology for details.

After gathering the required information, you can proceed to performing your tasks. See Step 1: Setting Up Server-C for an example.

Step 1: Setting Up Server-C

Before you begin, be sure to have the required information available for reference. See About Planning the Topology.

> **Caution:**
>
> This procedure interrupts service.

To prepare Server-C for addition to a georedundant secondary site:

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

   For more information, refer to the relevant chapter of Oracle Communications Policy Management *Bare Metal Installation Guide*. If you have problems or questions, contact My Oracle Support for assistance.
2. Using the Platform Configuration (`platcfg`) utility, provision Server-C with the following configuration information:
   a. Host Name
   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

   For more information, refer to *Platform Configuration User's Guide*.
3. For Oracle X5-2 platforms, configure the following:
   a. OAM VLAN ID
   b. SIG A VLAN ID

   c. SIG B VLAN ID (optional)
   d. SIG C VLAN ID (optional)
4. Using the Platform Configuration utility, export routing configuration information from Server-A or Server-B and import it into Server-C.

Server-C is ready to be added to the secondary site.
Proceed to Step 2: Setting Up the Georedundant Sites.

Step 2: Setting Up the Georedundant Sites

Prior to performing this step you must have competed Step 1: Setting Up Server-C.

> **Caution:**
>
> This procedure interrupts service.

To create georedundant primary and secondary sites:

1. Log in to the CMP system, using its OAM VIP address.
2. If this is the first georedundant cluster in your topology, configure the CMP system to enable **Manage Geo-Redundant** mode.

   See CMP Modes.

   With georedundancy enabled, the content tree shows the **All Sites** group when you select **Topology Settings** from the **Platform Setting** section of the navigation pane.
3. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens.
4. From the content tree, select the **All Sites** group.

   The Site Configuration page opens.
5. Click **Create Site**.

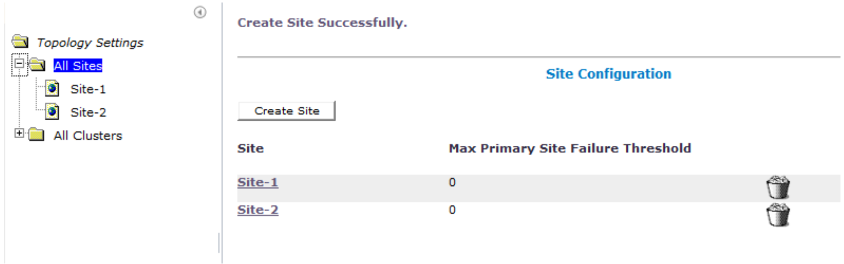
   The New Site page opens.
6. Enter the **Name** for the site name: `Site-1`.
7. Enter the number of **Max Primary Site Failure Threshold**.

   The default value is zero (0).
8. Select the **HW Type** from the list.
9. With the hardware type selected, configure the **General Network** settings:
   a. Enter the **OAM VLAN ID**.
   b. Enter the **SIG-A VLAN ID**.
   c. (Optional) Enter the **SIG-B VLAN ID**.
   d. (Optional) Enter the **SIG-C VLAN ID**.
10. Click **Save**.

    See Setting Up a Georedundant Site for more information.

    The sites become visible on the Site Configuration page.

Figure 2-12   Successful Site Creation



Create Site Successfully.

Site	Max Primary Site Failure Threshold
Site-1	0
Site-2	0

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

    The Cluster Configuration page opens, displaying the defined clusters.

12. On the Cluster Configuration page, for the MPE cluster you are expanding with Server-C, click the **View** operation.

    The Topology Configuration page opens for the selected MPE cluster.

13. Click **Modify Primary Site**.

    The fields in the **Primary Site Settings** section of the page becomes editable.

14. 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 configuration settings 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.

15. In the **Server-A** section of the page:

    a. Confirm the settings in the **General Settings** section.

    b. In the **Path Configuration** section, click **Add New**.

       The New Path dialog box appears.

       i. Enter the **Static IP** address and subnet **Mask**.

       ii. Select the **Interface** (for this example, the SIG-A network).

       iii. Click **Save**.

    c. If the **REP** network is used, repeat step 16b for the REP network.

16. Repeat step 11 for **Server-B**.

    The Primary Site Settings are defined.

17. Click **Save**.

    A restart message appears.

18. Click **OK**.

    Server-A restarts.

The two sites, primary and secondary, and the georedundant primary MPE cluster are configured.
Proceed to Step 3: Setting Up Primary Site Cluster.

Step 3: Setting Up Primary Site Cluster

Before you proceed, you must have completed Step 2: Setting Up the Georedundant Sites.

> ⚠ **Caution:**
>
> This procedure interrupts service.

To configure the primary site cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the MPE cluster you are expanding with Server-C.

   The Topology Configuration page for the selected MPE cluster opens.
4. Click **Modify Primary Site**.

   The fields in the **Primary Site Settings** section of the page becomes editable.
5. In the **Primary Site Settings** section of the page:
   a. Select the primary **Site Name** from the list: **Site-1**.
   b. Confirm the configuration settings: **HW Type**, **Network Configuration**, and **Signaling VIPs**.
   c. If the **REP** network is used, in the **User Defined Network** section, enter the **VLAN ID** for the **REP** network.
6. In the **Server-A** section of the page, confirm the settings in the **General Settings** section.
7. In the **Path Configuration** section, click **Add New**.

   The New Path dialog box appears.
   a. Enter the **Static IP** address and subnet **Mask**.
   b. Select the **Interface** (for this example, the **SIG-A** network).
   c. Click **Save**.
8. If the **REP** network is used, repeat the process for adding a **Static IP**.
9. Repeat the process for **Server-B**.
10. Click **Save**.

    A restart message appears.
11. Click **OK**.

    Server-A restarts.

The Primary Site Settings are defined.
Proceed to Step 4: Setting Up the Secondary Site with Server-C.

Step 4: Setting Up the Secondary Site with Server-C

Before you proceed, you must have completed Step 3: Setting Up Primary Site Cluster.

> **Caution:**
>
> This procedure interrupts service.

To configure the secondary site and Server-C settings:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the MPE cluster you are expanding with Server-C.

   The Topology Configuration page for the selected MPE cluster opens.
4. Click **Modify Secondary Site**.

   The fields in the **Secondary Site Settings** section of the page become editable.
5. In the **Secondary Site Settings** section of the page:
   a. Select the secondary **Site Name** from the list: **Site-2**.

   b. Confirm the configuration settings: **HW Type**, **Network Configuration**, and **Signaling VIPs**.

   c. If the **REP** network is used, in the **User Defined Network** section, enter the **VLAN ID** for the **REP** network.
6. In the **Server-C** section of the page, click **Add Server-C**.

   The Server-C section becomes editable.
7. To enter the **OAM IP** address, click **Add New VIP**.

   The New IP dialog box appears.

   a. Enter the **IP** address.

   b. Click **Save**.
8. Select the **IP Preference**: either **IPv4** or **IPv6**.

   The server will preferentially use the selected format's IP address for communication.

   > **Note:**
   >
   > If neither an IPv6 OAM IP nor a static IP address is set, IPv6 cannot be selected. If neither an IPv4 OAM IP nor a static IP address is set, IPv4 cannot be selected.
9. Enter the **HostName**.
10. Select **Forced Standby**.
11. In the **Path Configuration** section, click **Add New**.

The New Path dialog box appears.

  a. Enter the **Static IP** address and subnet **Mask**.
  b. Select the **Interface** from the list (for this example, the **SIG-A** network).
  c. Click **Save**.

12. If the **REP** network is used, in the **User Defined Network** section, enter the **VLAN ID** for the **REP** network.
13. Click **Save** (at the bottom of the page).

    A restart message appears.
14. Click **OK**.

    Server-C restarts.

    > **Note:**
    >
    > The status of Server-C is `Out of Service` and critical alarm 31283 is raised; this is expected.
15. Click the **Status** of Server-C.

    The status changes to **Spare**.
16. Click **Save**.

    The configuration is saved.

Site-2 and Server-C are defined, and Server-C is placed in Force Standby status. Proceed to Step 5: Updating the Georedundant Cluster.

Step 5: Updating the Georedundant Cluster

Before you proceed, you must have completed Step 4: Setting Up the Secondary Site with Server-C

This procedure updates the MPE cluster settings, if needed, and verifies the server is functioning properly.

> **Caution:**
>
> This procedure interrupts service.

To update the georedundant MPE cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the MPE cluster you are expanding with Server-C.

   The Topology Configuration page for the selected MPE cluster opens.
4. Click **Modify Cluster Settings**.

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

5. In the **Cluster Settings** section of the page:
   a. If DSCP marking is used, select the type of **DSCP Marking** from the list.
   b. If replication streams are used, select the number of stream from the **Replication Stream Count** list.
   c. Select the network used for the **Replication & Heartbeat** (or **None** to use the system default).
   d. If used, select the network used for the **Backup Heartbeat** (or **None** to disable the feature).
6. Click **Save**.

   The **Cluster Settings** are saved.
7. Verify the **Status** of Server-C by viewing the cluster.

   Server-C is shown as part of the cluster in **Force Standby** with replication on.
8. Use the **Alarm History Report** and filter in all alarms on the cluster name to verify that no new alarms have been raised.

   For more information, see Viewing the Alarm History Report.

   Alarm 31102 (DB Replication from a master DB failed) is in the report, but with severity of Clear.
9. Using the Platform Configuration utility on Server-C, exchange SSH keys with the other servers of the cluster.

   Refer to *Platform Configuration User's Guide* for detailed information.
10. Using the Platform Configuration utility on the CMP system, exchange SSH keys with all other CMP systems in the topology.
11. Using the CMP system, modify the cluster configuration to cancel the **Force Standby** status of Server-C.

    See #unique_113 for details.

    The status of Server-C changes to **Spare**.
12. Use the **KPI Dashboard** to verify that Server-C is reporting its status as part of the cluster.

    For more information, see KPI Dashboard.
13. (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, refer to *Policy Wizard Reference*.
14. To configure the connections on Server-C to existing data sources, use the **Data Sources** tab.

    For more information, see Connecting to Data Sources.

Step 6: Verifying Server-C Operation

Before you proceed, you must have completed Step 5: Updating the Georedundant Cluster.

> **Caution:**
>
> This procedure interrupts service.

To verify that Server-C is functioning properly within the cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the MPE cluster you are expanding with Server-C.

   The Topology Configuration page for the selected MPE cluster opens.
4. Click **Modify Primary Site**.
5. In the **Server-A** section of the page, select **Forced Standby**.
6. In the **Server-B** section of the page, select **Forced Standby**.
7. Click **Save** (at the bottom of the page).

   The system displays a message indicating that the server will restart.
8. Click **OK**.

   Server-A restarts and failover should result in Server-C becoming the active server.
9. To verify that Server-C has become the active server, from the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

   The **Server Role** for Server-C should be **Active**.
10. To verify that Sh connections are active on Server-C:
    1. From the **Policy Server** section of the navigation pane, select **Configuration**.

       The Policy Server Administration page opens; the initial group is **ALL**.
    2. Select the **Reports** tab.

       The Cluster Information Report opens.
    3. From the **Data Source Statistics** section, click **Sh Data Source Statistics**.

       The Sh Data Source Statistics page opens and the **Mode** should appear as **Active**.
11. To cancel the **Forced Standby** status on Server-A and Server-B:
    1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
    2. From the content tree, select **All Clusters**.
    3. On the Cluster Configuration page, for the MPE cluster you are expanding with Server-C, click the **View** operation.
    4. Click **Modify Server-A**.

       The Server-A section becomes editable.

e. Uncheck **Forced Standby**.

f. Click **Save**.

g. Repeat the process for Server-B.

h. Click **Save**.

   The system displays a confirmation message.

i. Click **OK**.

   Server A restarts.

Server-A and Server-B return to service.

12. To verify that Server-C has become the spare server, from the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

    The **Server Role** for Server-C should be **Spare**.

> **Note:**
>
> Either Server-A or Server-B may assume the Active status. Oracle recommends not attempting to force Server-A back into the Active status, as doing so would interrupt service.

The two sites, and the georedundant MPE cluster, are defined; 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 *Policy Front End Wireless User's Guide*.

Modifying the Topology

You can modify the topology to:

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

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

About Managing Georedundant Sites

> **Note:**
>
> Sites are only available for a system with **Manage Geo-Redundant** enabled. See CMP Modes for detailed information.

Modifying and configuring sites, hardware, VLAN IDs, and IP addresses requires Platform Configuration (`platcfg`) and PMAC (also known as PM&C) software. For detailed information, refer to the relevant Policy Management documentation:

- *Platform Configuration User's Guide*
- *Bare Metal Installation Guide*

> **Note:**
>
> The *Bare Metal Installation Guide* includes PMAC procedures for Policy Management.

For detailed information, refer to the following Tekelec Platform PMAC documentation:

- *PM&C Incremental Upgrade*
- *PM&C Disaster Recovery*

You can manage a site using the following procedures:

- Setting Up a Georedundant Site
- Modifying a Georedundant Site
- Updating Site Information
- Removing a Site from the Topology

Modifying a Georedundant Site

> **Note:**
>
> You must enable **Manage Geo-Redundant** to modify sites within the Policy Management topology. See CMP Modes for more information.

To modify a georedundant site:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Sites**.

   The Site Configuration page opens.
3. Select the site you want to modify.

The Site Configuration page displays information about the site.

4. Click **Modify**.

   The Modify Site page opens.

5. Modify site information.

   For a description of the fields contained on this page, see Setting Up a Georedundant Site.

6. Click **Save**.

Your changes to the site are saved.

Updating Site Information

You can update site information (for example, IP address, host name, or VLAN IDs) for a secondary site in a cluster. For more information on modifying a cluster, see Modifying a non-CMP Cluster.

To update the secondary site in a cluster:

1. On the CMP server, remove the secondary site from the topology.

   See Removing a Site from the Topology for more information on removing a site.

2. Using the Platform Configuration (`platcfg`) utility, re-create the configuration for the secondary site to change the IP address, host name, or VLAN ID settings.

   Refer to *Platform Configuration User's Guide* for information on configuring a site.

3. On the CMP server, from the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens; the initial group is **All Clusters**.

4. In the CMP system, add the secondary site.

   See Setting Up a Georedundant Site for more information on setting up a site.

   A confirmation message appears.

5. Click **OK**.

6. After the site has been updated, reapply the configuration for the changes to take effect.

   See About Reapplying a Configuration for more information.

The site has been updated in the cluster.

Removing a Site from the Topology

You can remove a site only if the site is not referenced by a Server C-level cluster. If you try to delete a site that is in use by a cluster, you will receive an information message indicating that the cluster cannot be removed because it is being referred to by at least one other cluster. The message also lists the referring clusters.

To remove a site from the topology:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. From the content tree, select **All Sites**.

   The Site Configuration page opens.

3. Delete the site using one of the following methods:

- From the work area, click 🗑 (Delete icon), located to the right of the site.
- From the content tree, select the site and click **Delete**.

A confirmation message appears.

4. Click **OK**.

The site is removed from the topology.

About Managing Clusters

Managing clusters, both CMP and non-CMP servers, entails the following:

- Setting Up a CMP Cluster
- Setting Up a Non-CMP Cluster
- Setting Up a Georedundant Non-CMP Cluster
- Modifying a non-CMP Cluster
- Modifying a CMP Cluster
- Removing a Cluster from the Topology
- Reversing Georedundant Cluster Preference
- Demoting a Georedundant CMP Cluster
- Promoting a Georedundant CMP Cluster
- Changing Server Status to Forced Standby
- Changing Server Status from Forced Standby

Modifying a non-CMP Cluster

To modify an non-CMP cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the cluster you want to modify.

   The Topology Configuration page opens, displaying information about the cluster.
4. Click the button for the changes you want to make:
   - To modify cluster settings, click **Modify Cluster Settings**.
   - To modify the primary server, click **Modify Server-A**.
   - To modify the secondary server, click **Modify Server-B**.
   - To delete a server configuration, click the appropriate **Modify** button and then click **Delete**.

   The appropriate section on the Topology Configuration page becomes editable.
5. Make changes as required.

   You must make changes to each section individually.
   - You can remove all servers from a cluster.

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

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

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

6. Click **Save**.

   A warning message appears.
7. Click **OK**.

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

Modifying a CMP Cluster

To modify a CMP cluster:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the CMP cluster you want to modify.

   The Topology Configuration page opens, displaying information about the CMP cluster.
4. Click the button for the changes you want to make:
   - To modify cluster settings, click **Modify Cluster Settings**.
   - To modify the primary server, click **Modify Server-A**.
   - To modify the secondary server, click **Modify Server-B**.

   The appropriate section on the Topology Configuration page becomes editable. For information on configurable settings, see Setting Up a CMP Cluster.
5. Make the changes as required.

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

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

6. Click **Save**.

   A restart message appears.

7. Click **OK**.

The changes to the CMP cluster are saved. You can determine if there is a topology mismatch by viewing the **System** tab for each policy server profile.

Removing a Cluster from the Topology

You can remove a non-CMP or secondary CMP cluster from the topology.

> **Note:**
>
> You cannot remove the 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 the cluster's servers from the CMP server. See Deleting a Policy Server Profile for details.

To remove a cluster from the topology:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.

3. In the **Cluster Settings** table, in the row listing the cluster you want to remove, click **Delete**.

   A confirmation message appears.

4. Click **OK**.

   An instructional message with further instructions appears.

The cluster is removed from the topology.
After the cluster is removed, use the Platform Configuration (PlatCfg) utility to remove cluster information. For more information, see the *Platform Configuration User's Guide*.

Reversing Georedundant Cluster Preference

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

To reverse a georedundant cluster preference:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.

2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.

3. Click **View** for the cluster you want to modify.

   The Topology Configuration page opens, displaying information about the cluster.

4. Click **Modify Cluster Settings**.
5. In the **Cluster Settings** section of the page:
   - To set the preference to reverse (where the active Site 1 becomes the inactive site and Site 2 becomes the active site), toggle to **Reverse**.
   - To set the preference to normal (where the active Site 2 becomes the inactive site and Site 1 becomes the active site), toggle to **Normal**.
6. Click **Save**.

The cluster preferences are reversed.

Demoting a Georedundant CMP Cluster

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

> **Note:**
>
> This is a manual process.

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

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

To demote a georedundant CMP cluster:

1. Log in to the currently active georedundant CMP cluster:
   a. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

      The Cluster Configuration page opens; the initial group is **All Clusters**.

   b. From the content tree, select **All Clusters**.

      The Cluster Configuration page opens.

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

You should see the operations **View** and **Demote**.

2. Open a second browser window and log in to the secondary CMP cluster.

   The page displays the a message indicating that you are signed into Secondary Active server.

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

3. Verify the status of the secondary cluster by doing the following on the secondary CMP cluster:
   1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

      The Cluster Configuration page opens; the initial group is **All Clusters**.
   2. From the content tree, select **All Clusters**.

      The Cluster Configuration page opens.

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

4. Return to the browser window showing the primary CMP cluster.

   You should still be on the Cluster Configuration page.
5. In the **Cluster Settings** table, in the row listing the primary CMP cluster, click **Demote**.

   A confirmation message displays.
6. Click **OK**.
7. Log out of the primary CMP system for the cluster you have just demoted.

The primary CMP cluster is demoted to secondary status.
After demoting a primary cluster, you must promote the secondary cluster for it to become active. See Promoting a Georedundant CMP Cluster for detailed information.

Promoting a Georedundant CMP Cluster

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

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

> **Note:**
>
> This is a manual process.

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

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

To promote a georedundant CMP cluster:

1. Log in to the secondary CMP cluster:

   The page displays a message indicating that you are signed into 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**.

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

      The Cluster Configuration page opens; the initial group is **All Clusters**.

   b. From the content tree, select **All Clusters**.

      The Cluster Configuration page opens.

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

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

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

2. If you have just demoted a primary cluster, wait 2 minutes.
3. In the **Cluster Settings** table, in the row listing the secondary CMP cluster, click **Promote**.

   A confirmation message appears.
4. Click **OK**.
5. Log out of the CMP system for the cluster you have just promoted.
6. Log in to the CMP system for the cluster you have just promoted.
7. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

   The Cluster Configuration page opens; the initial group is **All Clusters**.
8. From the content tree, select **All Clusters**.

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

   > **Note:**
   >
   > For the new primary cluster, you should see the operations **View** and **Demote**. All functions available for the primary CMP cluster should now appear and be accessible.
9. Wait 10 minutes.
10. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.

    The Cluster Configuration page opens; the initial group is **All Clusters**.
11. From the content tree, select **All Clusters**.

    The Cluster Configuration page opens.
12. Verify that both the primary and secondary CMP clusters are available and have the correct status.

The secondary CMP cluster is promoted to primary status.

Changing Server Status to Forced Standby

You can change the status of a server in a cluster to forced standby. A server placed into forced standby status cannot become active. You would do this, for example, to an active server prior to performing maintenance on it. Oracle recommends this method to switch over from an active server or to resolve issues where more than one server in a cluster is active.

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

- If the server is active, the server is demoted.
- The server will not assume the active role, regardless of its status or the roles of the other servers in the cluster.

- The server continues as part of its cluster and reports its status as Forced Standby.
- The server coordinates with the other servers in the cluster to take the role Standby or Spare.

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

To change a server to forced standby status:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the cluster you want to change.

   The Topology Configuration page opens, displaying information about the cluster.
4. Click **Modify Server-A** or **Modify Server-B** (whichever server needs the status change).
5. Select **Forced Standby**.
6. Click **Save**.

The server status is changed to forced standby.

Changing Server Status from Forced Standby

A server placed into forced standby status is not active. You can change the status of a server in a cluster from forced standby. You would do this, for example, to return a server to active status after performing maintenance on it.

When you take a server from forced standby, the server coordinates with the other servers in the cluster to take either the role **Standby** or **Spare**.

To take a server from a forced standby status:

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

   The Cluster Configuration page opens; the initial group is **All Clusters**.
2. From the content tree, select **All Clusters**.

   The Cluster Configuration page opens.
3. Click **View** for the cluster you want to change.

   The Topology Configuration page opens, displaying information about the cluster.
4. Click **Modify Server-A** or **Modify Server-B** (whichever server needs the status change).
5. Deselect **Forced Standby**.
6. Click **Save**.

The server status is changed from forced standby.

Managing VNF Components

Network Function Virtualization (NFV) uses IT virtualization-related technologies to virtualize entire classes of network node function.

NFV-Infrastructure (NFV-I) infrastructure/environment where VNFs are deployed (including managers: OpenStack, OVM-M, Cloud Director)

Virtual Network Function (VNF) responsible for handling specific network functions that run on one or more VMs (PCRF).

Virtual Infrastructure Manager (VIM) software responsible for ensuring that physical and virtual resources work smoothly together.

To manage VNF components:

1. Add **MPE/MRA Cluster** (If in Wireless-c Mode add **MPE/MRA**) .
2. Select **VM (Automated)** as the **HW Type**.
3. Select **VIM Connection**.
4. CMP requests info on VIM connection.
5. VNF Manager returns catalog data as JSON for images, flavors affinity zones, security groups and Network Ports.
6. CMP database saves the topology.
7. CMP database passes new VNF cluster topology and VIM connection to the NF Agent:
   a. The NF Agent interfaces with the VIM OpenStack to request the instantiation of the new VM.
   b. The OpenStack requests the initial configuration of the VM instance
   c. Plat Config configures the VM with the proper image files.
   d. OpenStack interfaces with NF Agent so the VNF mapping persists in HA.
8. CMP database passes new cluster topology to QP to persist in HA.

About NF Management

The NF Management function allows the creation of VIM connections for use with **VM (Automated)** devices. VIM connections work with the OpenStack API and OpenStack Heat API.

The NF Agent provides the following VM profile and deployment information to the VIM so it can instantiate instances of the described VNF:

- Required vCPUs
- Required vNICs
- Required Networks and IP addressing
- Memory size
- Storage size
- Anti-affinity/Affinity requirements

Creating a VIM Connection

To create a VIM connection:

1. From the **NF Management** section of the navigation pane, select **VIM Connections**.

   The VIM Connections page opens; the initial group is **VIM Connections**.

2. From the content tree, select the **VIM Connections** group.

   The VIM Connections page opens.

3. Click **Create VIM Connection**.

   The Create VIM Connections page opens.

4. Enter a **Name** for the VIM connection.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

   > **Note:**
   >
   > Once saved, the VIM Connection Name cannot be changed.

5. (Optional) Enter a **Description** for the VIM connection.

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

   Available options include:

   - **OpenStack API**—Indicates the connection will use the OpenStack API
   - **OpenStack Heat** —Indicates the connection will use the OpenStack Heat API
   - **VMWare vCloud**—Indicates the connection will use the vCloud API

7. Enter the **Host** name.

   Enter an IP address or the FQDN of the VIM host.

8. Enter the **Port** number.

   This is the port to connect to the VIM host. Enter a number from 1 to 65535. A typical port number is 5000.

9. (For OpenStack VIM types) Select to use a **Secure Connection**.

   If enabled, the connection will use an HTTPS connection to encrypt the connection.

10. Enter the **Username**.

11. (For VMWare) Enter the **Organization**.

12. (For OpenStack VIM types) Enter the **Tenant** name.

13. Enter the **Password**.

    Select **Show Password** to view the password in clear text.

14. Click **Save**.

The CMP server saves the VIM connection to the database.

Modifying a VIM Connection

To modify a VIM connection:

1. From the **NF Management** section of the navigation pane, select **VIM Connections**.

   The VIM Connections page opens.
2. From the content tree, select the VIM connection to modify.
3. Click **Modify**.
4. Change the values of the configuration settings as needed.
5. Click **Save**.

Deleting a VIM Connection

To delete a VIM connection:

1. From the **NF Management** section of the navigation pane, select **VIM Connections**.

   The NF Management page opens.
2. From the content tree, select the VIM connection to be deleted.
3. Click **Delete**.
4. Click **OK** to confirm the delete.

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 to up to five external systems (SNMP managers) or such that each server generates and delivers its own traps.

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

To configure SNMP settings:

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

   The SNMP Settings page opens, displaying the current settings.
2. Click **Modify**.

   The Edit SNMP Settings page opens.
3. For each SNMP manager, enter a valid host name or an IPv4/IPv6 address.

   The **Hostname/IP Address** field is required for an SNMP Manager to receive traps and send SNMP requests. The field has the following restrictions:

   - The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
   - The maximum length is 20 characters.

- The name is case insensitive (uppercase and lowercase are treated as the same).

By default, these fields are blank.

4. (Optional) You can configure a port for each SNMP manager by entering a port value between 1 and 65535 in the **Port** field. If left blank, the default value is 162.
5. From the **Enabled Versions** list, select one of the following versions:
   - **SNMPv2c**
   - **SNMPv3**
   - **SNMPv2c and SNMPv3** (default)
6. If you selected **SNMPv2c** or **SNMPv2c and SNMPv3** from the **Enabled Versions** list, configure the following:
   a. **Traps Enabled**—Specifies whether sending SNMPv2 traps is enabled. The default is enabled.

   > **Note:**
   >
   > To use the **SNMP Trap Forwarding** feature, enable this option.

   b. **Traps from individual Servers**—Specifies whether sending SNMPv2 traps from individual servers is enabled. If disabled, SNMPv2 traps are only sent from the active CMP system only. The default is disabled.

   > **Note:**
   >
   > To use the **SNMP Trap Forwarding** feature, disable this option.

   c. **SNMPv2c Community Name**—Enter the SNMP read-write community string. This field has the following restrictions:
      - The field is required if SNMPv2c is enabled.
      - The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
      - The name cannot exceed 31 characters in length.
      - The name cannot be either `private` or `public`.

      The default value is `snmppublic`.
7. If you selected **SNMPv3** or **SNMPv2c and SNMPv3** from the **Enabled Versions** list, configure the following:
   a. **SNMPv3 Engine ID**—Enter an Engine ID for SNMPv3. The Engine ID can be 10 to 64 digits long and must use only hexadecimal digits (0-9 and a-f). The default is no value (null).

   b. **SNMPv3 Security Level**—Select the level of SNMPv3 authentication and privacy from the list:
      - **No Auth No Priv**—Authenticate using the **Username**. No Privacy.
      - **Auth No Priv**—Authenticate using MD5 or SHA1 protocol.
      - **Auth Priv** (default)—Authenticate using MD5 or SHA1 protocol. Encrypt using the AES or DES protocol.

c. **SNMPv3 Authentication Type**—Select an SNMPv3 authentication protocol from the list:

   - **SHA-1**—Use Secure Hash Algorithm authentication.
   - **MD5** (default)—Use Message Digest authentication.

d. **SNMPv3 Privacy Type**—Select an SNMPv3 privacy protocol from the list:

   - **AES** (default)—Use Advanced Encryption Standard privacy.
   - **DES**—Use Data Encryption Standard privacy.

e. **SNMPv3 Username**—Enter a user name. The user name can contain 0 to 32 characters and must only contain alphanumeric characters. The default is `TekSNMPUser`.

f. **SNMPv3 Password**—Enter an authentication password. The password must contain between 8 and 64 characters and can include any character.

> **Note:**
>
> The SNMPv3 password is also used for `msgPrivacyParameters`.

8. Click **Save**.

The SNMP settings for the network are configured.

Platform Configuration Settings

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

Configuring the Upsync Log Alarm Threshold

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

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

To configure the upsync log alarm threshold:

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

   The Platform Configuration page opens.

2. Click **Modify**.
3. In the **Upsync Log Alarm Threshold** field, enter the percent of upsync log capacity at which the upsync log alarm will be triggered.

   Valid values are 50 through 90.

4. Click **Save**.

Configuring Concurrent Bulk Transfers

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

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

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

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

   The Platform Configuration page opens.
2. Click **Modify**.
3. In the **Concurrent Bulk Transfers** field, enter the allowed number of concurrent bulk transfers.

   Valid values are 1 to 8. The default is 1.
4. Click **Save**.

The number of allowed concurrent bulk transfers is set.

3 Managing Multimedia Policy Engine Devices

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

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

About Managing an MPE Device

To manage an MPE device:

1. You must first create its profile (see Managing Policy Server Profiles).
2. After creating the profile, you must configure the device:
   - Manually (see Configuring a Policy Server Profile)
   - By applying a configuration or virtual template (see Managing Configuration and Virtual Templates)

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

Managing Policy Server Profiles

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

The following sections describe how to manage policy server profiles:

- Creating a Policy Server Profile
- Configuring a Policy Server Profile
- Modifying a Policy Server Profile
- Deleting a Policy Server Profile

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

Creating a Policy Server Profile

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

To create a policy server profile:

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

   The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.

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

   The New Policy Server page opens.
4. (Required) Select the **Associated Cluster** with which to associate this MPE device.

   See Configuring the Policy Management Topology for details on adding clusters to the topology.
5. (Required) Enter the **Name** for this device.

   The default is the associated cluster name. A name is subject to the following rules:
   - The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
   - The name is case insensitive (uppercase and lowercase are treated as the same).
   - The maximum length is 255 characters.
6. (Optional) Enter the **Description / Location**.

   Information that defines the function or location of this MPE device.
7. (Optional) Select to enable **Secure Connection**.

   This setting determines whether or not to use the HTTPS protocol for secure communication between Policy Management devices. If selected, devices communicate over port 8443. See the *Platform Configuration User's Guide* for information on creating and exchanging security certificates within and between Policy Management clusters to support secure communication.
8. Select the **Type** from the list.

   This setting defines the policy server type:
   - **Oracle** (default)
     The policy server is an MPE device and can be fully managed by the CMP system.
   - **Unmanaged**
     The policy server is not an MPE device and therefore cannot be actively managed by the CMP system. This selection is useful when an MPE device is routing traffic to a third-party policy server.
9. (Optional) Select **Associate Templates**.

See Managing Configuration and Virtual Templates for information about configuration and virtual templates.

10. Click **Save**.

The server profile appears in the list of policy servers. You have defined the policy server profile.
Proceed with configuring the policy server. See Configuring a Policy Server Profile.

About Policy Server Administration

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

The Policy Server Administration page contains the following tabs:

- **System**
  Defines the system information associated with this policy server, including the name, host name or IP address in IPv4 or IPv6 format, information about the policy server, and whether or not the policy server uses a secure connection to any management system (such as the CMP system). See Creating a Policy Server Profile for details.
- **Reports** (read only)
  Displays various statistics and counters related to the physical hardware of the cluster, policy execution, and network protocol operation. Reports cannot be modified. See Policy Server Reports for details.
- **Logs**
  Displays the Trace Log, Syslog, SMS, SMTP,and HTTP log configurations. See #unique_144 for details.
- **Policy Server**
  Lets you associate applications and network elements with an MPE device and configure protocol information. See Configuring MPE Protocol Options for details.
- **Diameter Routing**
  Lets you configure the Diameter peer and route tables. See Configuring Protocol Routing for details.
- **Policies**
  Lets you manage policies that are deployed on the policy server. Refer to *Policy Wizard Reference* for details.
- **Data Sources**
  Lets you configure interfaces to LDAP (Lightweight Directory Access Protocol), Diameter Sh, or SPR (Subscriber Profile Repository) systems. See Connecting to Data Sources for details.
- **Debug**
  Lets you troubleshoot and modify component-specific level logging. The files logback-tomcat.log, logback-rc.xml, and logback-bod.xml can be modified using the CMP interface for each target Policy Management device. See Configuring Debug Logs.
- **Session Viewer** (read only)
  Displays static session and binding data for a specific subscriber from the Policy Management device that is managing the session. See Displaying Static Session and Binding Data for a Subscriber for details.

Configuring a Policy Server Profile

To configure a policy server profile:

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

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

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

   The Policy Server Administration page opens in the work area.

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

4. Edit the information:

   - **Logs**
     See Configuring Log Settings for Servers in a Cluster for details.
   - **Policy Server**
     See Configuring MPE Protocol Options for details.

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

   - **Diameter Routing**
     See Configuring Protocol Routing for details.
   - **Policies**
     Refer to *Policy Wizard Reference* for details.
   - **Data Sources**
     See Connecting to Data Sources for details.
   - **Debug**
     See Configuring Debug Logs for details.

5. Click **Save**.

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

Modifying a Policy Server Profile

To modify a policy server profile:

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

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

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

   The Policy Server Administration page opens in the work area.

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

4. Edit the information:

   - **System**
     See Creating a Policy Server Profile for details.
   - **Logs**
     See Configuring Log Settings for Servers in a Cluster for details.
   - **Policy Server**

See Configuring MPE Protocol Options for details.

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

- **Diameter Routing**
  See Configuring Protocol Routing for details.
- **Policies**
  Refer to *Policy Wizard Reference* for details.
- **Data Sources**
  See Connecting to Data Sources for details.
- **Debug**
  See Configuring Debug Logs for details.

5. Click **Save**.

Deleting a Policy Server Profile

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

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

To delete a policy server profile:

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

   The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.

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

   A confirmation message appears.
4. Click **OK** to delete the MPE device profile.

   The profile is removed from the list.

The policy server profile is deleted.

Managing Configuration and Virtual Templates

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

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

About Configuring Templates

Because an MPE or an MRA device exist independently of one another, you can create both virtual and configuration templates in two locations in the CMP interface. You can create templates either in the **MRA** or the **Policy Server** section of the navigation pane.

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

Creating a Configuration Template

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

> **Note:**
>
> SCEF pools cannot be configured in an SCEF-FE configuration template.

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

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

To create a configuration template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.

   The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates.**

2. From the content tree, select **Configuration Templates**.

   The Configuration Template Administration page opens.

3. Click **Create Template**.

   The New Configuration Template page opens.

4. Enter the **Name** of the template.

   > **Note:**
   >
   > This is an alphanumeric field that is limited to 255 characters. Single quotes, double quotes, spaces, commas, and backslash characters are not valid.

5. (Optional) To use an existing template as a base for the new template, select an existing template from the **Copy From** list.

6. (Optional) Enter a **Description / Location**.

   The text box is limited to 255 characters.

7. Click **Save**.

The new template appears in the list in the content pane.
After creating the template, proceed with configuring the template.

Modifying a Configuration Template

> **Note:**
>
> This procedure applies to both MPE and MRA servers.

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

To modify a configuration template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.

   The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates.**

2. From the content tree, select the **Configuration Template** for modification.

   The Configuration Template Administration page opens with the template configuration settings.

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

4. For an MRA server, edit the information:

   a. On the **MRA** tab, click **Modify**:

      - **Associations**
        Network Elements and/or Network Element Groups #unique_150 for details.

      - **MPE Pools**
        See #unique_151 for details.

> **Note:**
>
> SCEF pools cannot be modified in an SCEF-FE configuration template.

- **Subscriber Indexing**
  See #unique_152 for details.
- **Diameter**
  Provide the port and Realm (such as example.com), see #unique_152.
- **S9**
  If you connecting to an external MRA, see #unique_152.
- **Radius Configuration**
  If you are using a fixed mobile convergence and need Radius, see #unique_152.

b. On the **MRA** tab, click **Advanced**:

- **Expert Settings**
- **Service Overrides**
- **Load Shedding Configuration**

c. On the **Diameter Routing** tab:

- **Diameter Peers**: See #unique_153 for details.
- **Diameter Routes**: See #unique_151 for details.

5. Click **Save**.

The configuration template is modified. The modified template is applied to all associated MRA or MPE servers.

Changing the Template Priority

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

> **Note:**
>
> This procedure applies to both MPE and MRA servers.

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration**.

   The content tree displays a list of **All Policy Servers** or **MRA** devices.
2. From the content tree, select the device.

   The Administration page opens with the device configuration.
3. Select the **System** tab.

   The device's system configuration settings display on the page.
4. Click **Modify**.

   The administration page becomes enabled for editing.

5. In the **Associated Templates** section, edit the **Priority** value to change the number to a higher or lower value.
6. Click **Update Order**.

   The priority order of the **Associated Templates** is changed.

Creating a Virtual Template

Because an MPE or an MRA device can exist independently of one another, you can create both virtual and configuration templates in two locations in the CMP interface. Depending on your needs, the CMP interface enables you to create templates in the **MRA** or the **Policy Server** 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 template is created, the template has the functionality that is specific to that instance (that is, MPE or MRA). After templates are created and associated, the templates can be viewed and managed from the **System** tab of the MPE or MRA device.

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

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

Use this procedure if you have virtual template capability.

To create a virtual template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.

   The content tree displays a list of **All Templates** including **Virtual Templates** and **Configuration Templates.**
2. From the content tree, select **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, spaces, commas, and backslash characters are not valid.
5. Select a template from the **Associated Configuration Template** list.

6. (Optional) Enter a **Description**.
7. Click **Save**.

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

About Overlaps

Overlaps occur when both a template and an MPE or an MRA server 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 MPE or MRA server. The result is that when the template and MPE or MRA server are associated, the index of the user name becomes an overlapped field. When an overlap occurs, a prompt appears stating, `The server configuration has overlaps with the associated template(s).` You can take one of two actions:

- Remove the overlaps and use the settings from the template.
- Keep the overlaps and use the settings from the server.

Associating Templates with a Device

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

You would use this procedure if you had a number of devices that required the same instance.

To associate templates with an MPE or MRA device:

1. From the **MRA** or **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 device.

   The administration page opens in the work area.
3. Select the **System** tab.
4. Click **Modify**.

   The administration page becomes editable.
5. In the Associated Templates section, click **Add**.

   The Add Associated Templates dialog appears.
6. Select one or more templates from the list and click **Add**.

   The Associated Templates list updates to include the selected templates.
7. To order the **Priority** of the associated templates, change the values for each listed template.

> **Note:**
>
> Lower-numbered templates have higher priority than higher-numbered templates. This means that settings configured with a lower-value priority template can override the settings of a higher-value priority template.

8. Click **Save**.

The specified templates' configurations are applied to the specified device.

Configuring MPE Protocol Options

To configure protocol options on an MPE device:

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

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

2. From the content tree, select the MPE device.

   The Policy Server Administration page opens.

3. Select the **Policy Server** tab.

   The current configuration options are displayed.

4. Click **Modify** and define options as necessary.

   Selecting or choosing **undefined** signifies that the value comes from a configuration profile. If there is not a configuration profile, then the default value is used.
   The following sections define the available options. (The options you see vary depending on the mode configuration of your system.)

   - Associations Configuration Options
   - Subscriber Indexing Configuration Options
   - General Configuration Options
   - RADIUS-S Configuration Options
   - Diameter Configuration Options
   - S9 Configuration Options
   - User Profile Lookup Retry and Session Updates Configuration Options
   - Diameter AF Default Profiles Configuration Options
   - Default Charging Servers Configuration Options
   - Default Charging Methods Configuration Options
   - SMS Relay Configuration Options
   - #unique_169
   - SMPP Configuration Options
   - Primary SMSC Host Configuration Options
   - Secondary SMSC Host Configuration Options
   - SMTP Configuration Options
   - Generic Notification Configuration Options
   - RADIUS Configuration Options

- Analytics Configuration Options

5. Click **Save**.

You have defined the protocol options for this MPE device.

Associations Configuration Options

Applications
The application profiles associated with this MPE device. To modify this list, click **Manage**. For more information on application profiles, see *Policy Wizard Reference*.

Network Elements
The network elements associated with this MPE device. To modify this list, click **Manage**. For more information on network elements, see Managing Network Elements.

Network Element Groups
The network element groups associated with this MPE device. To modify this list, select or deselect groups. For more information on network element groups, see Managing Network Elements.

Notification Servers
The notification servers associated with this MPE device. To modify this list, click **Manage**. For more information on notification servers, see Notification Servers.

Subscriber Indexing Configuration Options

Index by IPv4
Select if the associated Subscriber Profile Repository is indexed by IPv4 address.

Index by IP-Domain-ID
Select if the associated Subscriber Profile Repository is indexed by IP domain ID. The combination of framed IPv4 address and IP domain ID ensures a globally unique binding, even if the same IPv4 address is locally assigned in multiple networks.

Index by IPv6
Select if the associated Subscriber Profile Repository is indexed by IPv6 address.

Index by Username
Select if the associated Subscriber Profile Repository is indexed by account ID.

Index by NAI
Select if the associated Subscriber Profile Repository is indexed by network access ID.

Index by E.164 (MSISDN)
Select if the associated Subscriber Profile Repository is indexed by E.164 phone number.

Index by IMSI
Select if the associated Subscriber Profile Repository is indexed by International Mobile Subscriber Identity (IMSI) number.

Overrides by APN
Select to configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN).

1. In the Overrides by APN section, click **Add**.

2. Enter the APN name.

> **Note:**
>
> APN names are alphanumeric and have the following restrictions:
>
> - A 255 character limit
> - No spaces or special characters such as asterisks
> - Can contain hyphens (-) and periods (.) but must not begin or end with a hyphen or period
>
> Example name: pdn1.examplecorp.com

3. Select one or more of the following:
   - **Index by IPv4**
   - **Index by IP-Domain-Id**
   - **Index by IPv6**
   - **Index by Username**
   - **Index by NAI**
   - **Index by E.164 (MSISDN)**
   - **Index by IMSI**
   - **Index by Session ID**
4. click **Save**

You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

General Configuration Options

Time of Day Triggering
Select **Enable** or **Disable** (default) from the list. If you select **Enable**, this MPE device supports time-of-day triggering when evaluating policy rules. For more information on time-of-day triggering, refer to *Policy Wizard Reference*.

Billing Day
If **true**, you can configure a global monthly billing day for subscribers who do not have a specific day configured in their profiles in a back-end database.

Billing Day of Month
If **Billing Day** is enabled, enter the day of the month on which subscriber usage counters are reset. This date is the default billing date for all subscribers handled by this MPE device; billing dates can be changed on a per-subscriber basis.

Billing Time Zone
Select the time zone used for billing cycle calculations. If this feature is configured, the user equipment time zone, even if reported, is irrelevant for billing cycle calculations.

Observe Daylight Saving Changes
If **true**, the MPE device observes Daylight Saving Time for the configured Billing Time Zone.

Default Local Time Mode
Select the time used within a session for a user from the list: **System Local Time** to use the local time of the MPE device (default) or **User Local Time** to use the local time for the user.

> **Note:**
>
> If the time zone was never provided for the user equipment, system local time is applied.

Enable Pro Rate
If **false** or **undefined**, the full monthly quota for subscribers is granted for the billing cycle following a quota reset.

If **true**, the monthly quota for subscribers is prorated, on a per-quota basis (for up to 30 quotas), for the billing cycle following a quota reset, based on the value of the **Billing Date Effective** field in the profile for the subscriber profile. This is a global setting affecting all subscribers. (If the field value is null, usage will not be prorated.)

Billing Date Effective Name
Enter the name of the custom field in subscriber profiles to use for the SPR variable *NewBillingDateEffective*. The default is null. This is a global setting affecting all subscribers.

- To specify a local time in the SPR, the field must be in the format:

  ```
  yyyy-mm-ddThh:mm:ss
  ```

- To specify a time zone (UTC offset), the field must be in the format:

  ```
  yyyy-mm-ddThh:mm:ssZ
  ```

  For example: `2011-10-30T00:00:00-5:00`

Track Usage for Unknown Users
If **true**, the MPE device tracks usage and state per subscriber ID, even if the subscriber is not registered in the SPR. If tracking was enabled and is now disabled, usage and state is no longer tracked for unknown users, but existing usage and state data is retained.

Subscribe For Unknown Users
If **Validate user** is **false** (at the MPE device), then unknown users are allowed to create sessions. In this case, if **Subscribe for Unknown Users** is **true**, then the MPE device will subscribe for those users.

> **Note:**
>
> This setting is only for the MPE device and does not have any effect on the SPR. There are settings in the SPR that must be set to allow auto-enrolling.

Use Single Lookup
If **true**, the MPE device reads multiple Sh user data blocks (subscriber, quota usage, and entity state) with a single read request. If you enable this feature, you must also configure the Sh data source with the option **Notif-Eff** (see Configuring an Sh Data Source).

If **false**, separate lookups are used.

Use Combined Writes
If **true**, the MPE device will combine the updates (PUR messages) resulting from a single user request into a single PUR update to the SPR. The PUR will contain both the quota usage and state updates for the user. This reduces the number of transactions between the MPE and SPR.

Cache Quota Usage
If **true**, the MPE device caches the quota usage objects locally for as long as the user session exists.

If **false**, objects are cached for a default of 60 seconds.

Cache Entity State
If **true**, the MPE device caches the entity state objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.

Subscribe Quota Usage
If **true**, the MPE device subscribes to receive notifications from the SPR for any changes to the quota.

Subscribe Entity State
If **true**, the MPE device subscribes to receive notifications from the SPR for any changes to the entity state.

RADIUS-S Configuration Options

RADIUS Shared Secret
Authenticates RADIUS messages received from external gateways (that is, PDSN or HA). This field must be configured with a value or the RADIUS-S protocol will not work. Also, each gateway must be configured to use this value when sending messages to the MPE device, or the messages received from that gateway will be dropped.

Untiered Plan Name
When the MPE device is set to RADIUS-S mode, this attribute indicates that a matching plan name does not participate in any tiered service plan. On a successful lookup for a given subscriber, the plan name returned by LDAP is compared to the Untiered Plan Name configured for the MPE device via the **Policy Server** tab. If they match, no default QoS values are sent to the gateway for the subscriber. If the Untiered Plan Name is null, this only matches if the subscriber has an entry in LDAP with no value for the associated attribute. The default value is null.

Default Downstream Profile / Default Upstream Profile
Define the upstream and downstream bandwidth parameters that are used when establishing a default traffic profile using RADIUS-S. You can override these parameters by configuring policy rules that apply different profiles. If a default profile is not configured, and the policy rules do not set the bandwidth parameters, a default traffic profile is sent to the Gateway to disable policing.

Index by Username
Select if the RADIUS database is indexed by subscriber account ID.

Index by NAI
Select if the RADIUS database is indexed by subscriber network address ID.

Index by Calling Station ID
Select if the RADIUS database is indexed by subscriber calling station ID.

Index by IP Address
Select if the RADIUS database is indexed by subscriber IP address.

Diameter Configuration Options

Diameter Port
The port number over which the device receives Diameter messages.

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

Diameter Identity
The fully qualified domain name (FQDN) or the valid routable domain address (formatted as described in 3GPP TS 23.003) of the MPE device (for example, `mpe3.galactel.com`).

Default Resource Id
The bearer used if a GGSN does not send any bearer information in a Credit-Control Request (CCR). Enter an alphanumeric string of up to 100 characters. The default is no resource ID (that is, no bearer).

Correlate PCEF sessions
If **true**, the primary PCEF Gx session will share information with all secondary sessions that share an IP address within the same IP-CAN session. Up to 10 different Gx sessions can be correlated to one subscriber. By default, PCEF sessions are not correlated and do not share information.

Validate user
If **true**, sessions for unknown users are rejected.

Diameter PCEF Default Profile
Select the default traffic profile from the list that will be applied during PCEF session establishment using the Gx or Ty protocols, or if no other SCE traffic profile is applied as a result of a policy being triggered. Refer to *Policy Wizard Reference* for details on creating a traffic profile.

Use Synchronous Sd
If **true**, the MPE device establishes an Sd session before sending a Gx CCA message to a traffic detection function (TDF).

Identify Duplicate sessions based on APN
If **true**, the MPE device will detect duplicate sessions. This makes it possible to remove duplicate sessions if their number becomes excessive.

Subscriber ID to detect duplicate sessions
This option is available only if **Identify Duplicate sessions based on APN** is **true**. Select the subscriber index type to use from the list:

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

Protocol Timer Profile
The timer profile to use. See Creating a Protocol Timer Profile for details.

Prevent Overlapping Rule Names
If selected, rule names that are dynamically generated on the primary and spare MPE devices in the same Gx session are unique.

Allow Multiple Rx Connections with the same Origin-host Id
When enabled, the MPE device accepts multiple Rx connections with the same Origin-Host Attribute Value Pair (AVP) and source IP address.

Timers
Rx-to-PCMM gate timers. Enter values in seconds for T1 (authorized, default 1 second), T2 (reserved, default 300 seconds), and T3 (committed, default 300 seconds).

S9 Configuration Options

Initiate S9 Requests
If **true**, the MPE device can initiate S9 requests. In addition, you must specify **Initiate Connection** when you define the Diameter peer. For more information, see Configuring Diameter Peers.

> **Note:**
>
> If an MRA device is deployed in the Policy Management network, the MPE device will not initiate S9 connections regardless of how you configure S9 options.

Accept S9 Requests
If **true**, the MPE device can accept S9 requests. If not enabled, when the MPE device receives an S9 request, an error code is generated at the device.

Primary DEA
If one or more Diameter Edge Agents is defined, you can select the primary agent from the list. For information on defining a DEA, see Configuring Diameter Peers.

Secondary DEA
If multiple Diameter Edge Agents are defined, you can select the secondary agent from the list. If you select both primary and secondary DEAs (and there is not a deployed MRA device in the Policy Management network), the MPE device establishes a connection to both DEAs. If the primary connection is down, the MPE device sends messages over the secondary connection. After the primary connection is back up, communication reverts back to the primary.

User Profile Lookup Retry and Session Updates Configuration Options

Enforcement
If **true**, enables user profile lookup retry on session updates for Gx and Gxx updates.

Application
If **true**, enables user profile lookup retry on session updates for Rx.

Diameter AF Default Profiles Configuration Options

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

Default
Define the bandwidth parameters that are used when a request from an Application Function (AF) does not contain sufficient information for the MPE device to derive QoS parameters. These profiles are defined per media type: The **Default** profile is used when a profile for a media type is not defined.

Audio
The profile for the audio.

Video
The profile for the video.

Data
The profile for data.

Application
The profile for application.

Control
The profile for control.

> **Note:**
>
> To select a profile, first create a Diameter profile in the general profile configuration.

Text
The profile for text.

Message
The profile for messages.

Other
The profile for all other media types.

Default Charging Servers Configuration Options

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.

Default Charging Methods Configuration Options

> **Note:**
>
> See #unique_180 for detailed information on managing charging servers.

Default Online Method
Controls the online charging method. The default is **N/A** which indicates that there is not an online charging method configured.

Default Offline Method
Controls the offline charging method. The default is **N/A** which indicates that there is not an online charging method configured.

SMS Relay Configuration Options

SMS Enabled
Select **true** to enable SMS messaging to subscribers.

Relay Host
Enter the FQDN or IP address of the relay server.

Relay Port
Enter the port number on which the relay server is listening for SMS messages. The default port is 8080.

Throttle Value
Enter the time interval, in milliseconds, at which SMS messages are sent from the MPE device. If set to `1000` ms, the MPE device sends one SMS message per second; if set to `500` ms, the MPE device sends two messages per second. The recommend throttle value is `0` ms which means that the device sends the SMS message as soon as it receives the message.

SMPP Configuration Options

SMPP Enabled
Select **true** to enable Short Message Peer to Peer (SMPP) messaging to subscribers. To send an SMS message to a subscriber, a Mobile Station International Subscriber Directory Number (MSISDN) must be present in the profile for the subscriber. The maximum length is 254 characters.

Validate Message Length
Select **true** to validate message length.

SMPP Long Message Support
If **true**, SMS messages longer than 160 characters are split into segments and reassembled by the receiving device. Messages of up to 1000 characters are supported.

Delivery Method for Long Message
Select the message delivery method for long messages from the list:

- **Segmentation and Reassembly (SAR)** (default)
- **Message Payload**

SMS/XML Configuration Options

> **Note:**
>
> This function is restricted. See About Mode Settings for more information.

Service Name
The name of the SMS service. For example, sendMessage.

Service URL
The URL for the service. For example, `http://192.0.2.0 /example/sms`

SMS Source Address
The address to use in the From element in the sendMessageRequest. If left empty, the From element is not included in the sendMesssageRequest.

Alert URL
The URL for message alerts. For example, `http://192.0.2.0/example/alertsms`

Primary SMSC Host Configuration Options

SMSC Host
Enter the FQDN or IP address of the primary Short Messaging Service Center (SMSC) store-and-forward server that accepts SMS messages from the relay server.

SMSC Port
Enter the port number on which the primary Short Messaging Service Center store-and-forward server is listening for SMS messages. The default port is 2775.

ESME System ID
Enter the system ID of the primary External Short Messaging Entity (ESME). Sending the ID and password values authenticates the relay server as a trusted source.

> **Note:**
>
> This value must be configured on the primary SMPP server.

ESME Password
Enter the password of the primary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source.

> **Note:**
>
> This value must be configured on the SMPP server.

Confirm ESME Password
Re-enter the primary ESME password for verification.

> **Note:**
>
> This setting is only available from the Modify page.

Secondary SMSC Host Configuration Options

SMSC Host
Enter the FQDN or IP address of the secondary Short Messaging Service Center (SMSC) store-and-forward server, which accepts SMS messages from the relay server.

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

SMSC Port
Enter the port number on which the secondary Short Messaging Service Center store-and-forward server is listening for SMS messages. The default port is 2775.

ESME System ID
Enter the system ID of the secondary External Short Messaging Entity (ESME). Sending the ID and password values authenticates the relay server as a trusted source.

> **Note:**
>
> This value must be configured on the secondary SMPP server.

ESME Password
Enter the password of the secondary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source.

> **Note:**
>
> This value must be configured on the SMPP server.

Confirm ESME Password
Re-enter the secondary ESME password for verification.

ESME Source Address
Enter the source address for a SUBMIT_SM operation in SMPP Protocol V3.4. The default is none.

ESME Source Address TON
Select the source address Type of Number (TON) from the list:

- **UNKNOWN** (default)
- **INTERNATIONAL**
- **NATIONAL**
- **NETWORK SPECIFIC**
- **SUBSCRIBER NUMBER**
- **ALPHANUMERIC**
- **ABBREVIATED**

ESME Source Address NPI
Select the source address Number Plan Indicator (NPI) from the list:

- **UNKNOWN** (default)
- **ISDN (E163/E164)**
- **DATA (X.121)**
- **TELEX (F.69)**
- **LAND MOBILE (E.212)**
- **NATIONAL**
- **PRIVATE**
- **ERMES**
- **INTERNET (IP)**
- **WAP CLIENT ID**

Character Encoding Scheme
Select the character-set encoding for SMS messages from the list:

- **SMSC Default Alphabet**
- **IA5 (CCITT T.50)/ASCII (ANSI X3.4)**
- **Latin 1 (ISO-8859-1)**
- **Cyrillic (ISO-8859-5)**
- **Latin/Hebrew (ISO-8859-8)**
- **UCS2 (ISO/IEC-10646)**
- **ISO-2022-JP (Music Codes)**
- **JIS (X 0208-1990)**
- **Extended Kanji JIS(X 212-1990)**

SMSC Default Encoding Scheme
Select the SMSC default encoding from the list: **UTF-8** or **GSM7**.

Request Delivery Receipt
Select the global default behavior when evaluating the policy action **send SMS** from the list:

- **No Delivery Receipt**
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

SMTP Configuration Options

SMTP Enabled
Select **true** to enable Simple Mail Transport Protocol (SMTP) messaging (email) to subscribers. SMTP notifications are triggered from policy action and sent through an SMS Relay (SMSR) function to an external mail transfer agent (MTA).

> **Note:**
>
> There is no delivery receipt for the SMTP messages sent from the SMSR, only confirmation that it reached the configured MTA.

MTA Host
Enter the FQDN or IP address of the Mail Transfer Agent server, which accepts SMTP messages from the SMSR function.

MTA Port
Enter the port number on which the MTA server is listening for SMTP messages. The default port is 25.

MTA Username
Enter the system ID of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source.

> **Note:**
>
> This value must be configured on the MTA.

MTA Password
Enter the password of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source.

> **Note:**
>
> This value must be configured on the MTA.

Confirm MTA Password
Re-enter the password for verification.

Note:

This is a new configuration setting for the SMTP connection.

Default From Address(es)
Enter the source address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none.

Note:

The total number of To, CC, and BCC addresses is limited to five.

SMTP Connections
The number of SMTP connections. Enter a number from 1 through 10.

Note:

SMTP connections can be increased to support a higher throughput. Contact My Oracle Support for more information.

Default Reply-To Address(es)
Enter the email address automatically inserted into the To field when a user replies to an email message. For most email messages, the From and Reply-To fields are the same, but this is not necessarily so. If no Default Reply-To is specified here, the From address is used. Optionally, enter a static email address to use for Reply-To.

The default is none.

Default CC Address(es)
Enter the copy address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none.

Note:

The total number of To, CC, and BCC addresses is limited to five.

Default BCC Address(es)
Enter the blind copy recipient address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none.

Note:

The total number of To, CC, and BCC addresses is limited to five.

Default Signature
Enter the text that should appear as the signature in an SMTP message.

The default is none.

Generic Notification Configuration Options

Notification Enabled
If SMPP, XML, or CMPP mode is enabled, select **true** to enable notifications using notification servers. For more information about notification servers, see the *Policy Wizard Reference*.

RADIUS Configuration Options

RADIUS Enabled
When selected, the MPE device processes RADIUS messages.

When not selected, RADIUS messages are ignored.

The default is enabled.

RADIUS Ports (Listening)
Enter a comma-separated list of UDP port numbers that the MPE device listens on for RADIUS messages.

The default is **1813,3799**.

Concatenate Multiply Occurring VSA's
When selected, if a string VSA appears multiple times in a RADIUS message, the values are concatenated to form one large value.

When not selected, if a string VSA appears multiple times in a RADIUS message, the value of the last TLV or VSA is used, and the earlier values are ignored. The default is disabled (earlier values are ignored).

Validate User
When selected, if an SPR lookup fails for a subscriber, the MPE device rejects the request.

When not selected, if an SPR lookup fails for a subscriber, the MPE device creates a dummy subscriber instance to store necessary information for later use. The default is disabled (requests are processed).

Default Passphrase
Enter the default passphrase (a text string). This shared secret value is used when no shared secret is defined for a specific RADIUS network element. The same shared secret is used for decrypting accounting requests and CoA responses and encoding accounting and CoA responses.

If you enter no passphrase and either of the fields in the associated network elements are not set, then the MPE device ignores RADIUS requests and responses.

The default is `radius`.

RADIUS Configuration Options

RADIUS Enabled
When selected, the MPE device processes RADIUS messages.

When not selected, RADIUS messages are ignored.

The default is enabled.

RADIUS Ports (Listening)
Enter a comma-separated list of UDP port numbers that the MPE device listens on for RADIUS messages.

The default is **1813,3799**.

Concatenate Multiply Occurring VSA's
When selected, if a string VSA appears multiple times in a RADIUS message, the values are concatenated to form one large value.

When not selected, if a string VSA appears multiple times in a RADIUS message, the value of the last TLV or VSA is used, and the earlier values are ignored. The default is disabled (earlier values are ignored).

Validate User
When selected, if an SPR lookup fails for a subscriber, the MPE device rejects the request.

When not selected, if an SPR lookup fails for a subscriber, the MPE device creates a dummy subscriber instance to store necessary information for later use. The default is disabled (requests are processed).

Default Passphrase
Enter the default passphrase (a text string). This shared secret value is used when no shared secret is defined for a specific RADIUS network element. The same shared secret is used for decrypting accounting requests and CoA responses and encoding accounting and CoA responses.

If you enter no passphrase and either of the fields in the associated network elements are not set, then the MPE device ignores RADIUS requests and responses.

The default is `radius`.

Analytics Configuration Options

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

Connecting to Data Sources

MPE devices establish connections with data sources to retrieve information about subscribers from a database. An MPE device queries a data source using a key attribute that uniquely identifies a subscriber and stores the results in its cache. A data source uses this key attribute (for example, the phone or account number of a subscriber) to index the information contained in the database.

The CMP system supports the following data sources:

- LDAP data source (such as, an external subscriber database)
- Sh data source (such as, the Oracle Communications Subscriber Database Management (SDM), the Oracle Communications User Data Repository (UDR), or Home Subscriber Server (HSS))
- Sy data source (such as, an online charging system (OCS))

You can use a single data source (that is, a redundant database) that holds all subscriber information or you can have the subscriber data distributed across multiple data sources. When using a single data source, you configure the server connection and the query format.

The following scenarios require flexible and efficient management of multiple data sources:

- Server scalability limitations require multiple servers to contain subscriber information.
- One server stores quota information while another server stores subscriber information.
- Information received from the initial subscriber query triggers a lookup for quota information from another repository.
- A network event triggers retrieval of quota information.

To support multiple data sources, the CMP system defines the following data source roles:

Primary
When the MPE device receives a subscriber query, it connects to a primary data source to retrieve information about the subscriber using key information included in the request (for example, MSISDN or IMSI). The MPE device can query primary data sources in a specified order or it can query all primary data sources and merge the results.

Secondary
The MPE device uses the information received from the primary data source as a key attribute to retrieve additional information from a secondary data source. After results are retrieved from the primary data source, the secondary search runs. For each primary data source, you can configure the order in which secondary data sources are queried. The secondary searches do not wait for the results from other primary sources before initiating their search.

On-demand
The MPE device uses policies to retrieve information on demand from data sources.

Table 3-1 details the available roles supported by each type of data source. You can create multiple data source definitions to allow access to a server in multiple ways (for example, as both a secondary and an on-demand data source).

Table 3-1 Data Source Roles

Type of Data Source	Supported Data Source Roles		
	Primary	Secondary	On-Demand
LDAP databases	Yes	Yes	No
Sh interface (to SDM, UDR, or HSS)	Yes	No	No
Sy interface (to OCS)	Yes	Yes	Yes

An MPE device initiates a data lookup to a data source in either of the following scenarios:

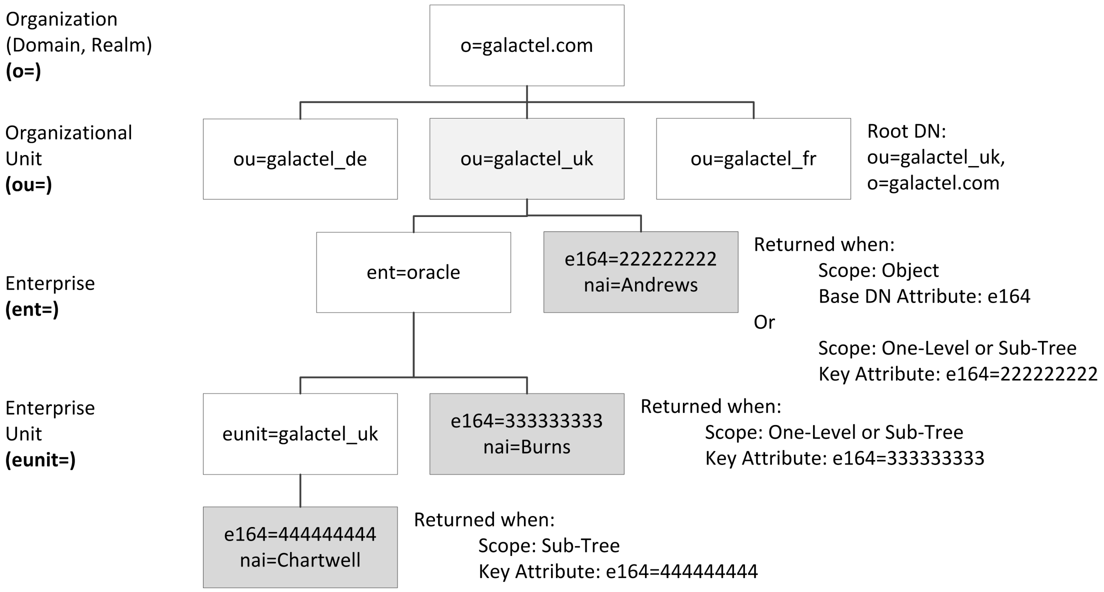
- A lookup to a primary data source occurs when the MPE device receives a CCR-I (Credit-Control-Request-Initiate) message from the PGW (PDN Gateway). Additionally, a lookup occurs when the MPE device receives a CCR-U (Credit-Control-Request-Update) message and there is no subscriber information in its cache.
- A lookup to a secondary data source occurs when the MPE device receives information from an associated primary data source. This occurs in response to a message sent by the MPE device to a primary data source or when the MPE device receives an unsolicited update from the primary data source.

About LDAP Data Sources

An LDAP data source uses a tree-like structure, called a directory information tree (DIT), for storing, organizing, and retrieving data objects (or entries) from a database. Organizing entries into a DIT makes the information faster and easier to look up which is crucial for time sensitive processing.

The database organizes the entries in a hierarchical model; for example, by group, people, or location like a state or region. A distinguished name (DN) identifies where each entry is located in the DIT.

Figure 3-1 LDAP Data Source Structure - Example



In Figure 3-1, the example database structure has a realm (or domain) of `o=galactel.com`, which encompasses all subscribers in the system. The subscribers may then be organized by organizational unit; for example, by country `ou=galactel_uk`. Within an organizational unit, the subscribers could be further subdivided into enterprises and enterprise units. A data lookup locates a subscriber's information based on the key attribute used to index the information, for example the NAI or the E.164 (MSISDN). An example of a DN for a specific subscriber's record is `e164=222222222, ent=oracle, ou=galactel_uk, o=galactel.com`.

The **Search Criteria** tab of the Edit Data Source dialog provides a method of restricting a record search to a particular section of the DIT. By specifying the **Root DN** (for example, `ou=galactel_uk,o=galactel.com`) and the **Scope**, you can either broaden or narrow the LDAP database search. See Defining LDAP Search Criteria for more information.

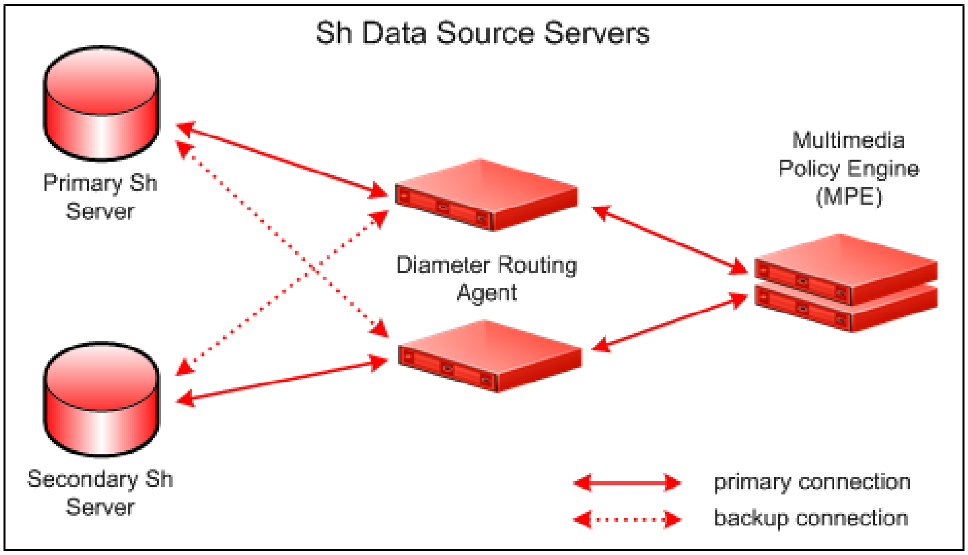
See Configuring an LDAP Data Source for details on configuring an LDAP data source.

About Sh Data Sources

The MPE device looks up subscriber profile information from an Sh data source. Examples of Sh data sources include the User Data Repository (UDR), the Subscriber Database Management (SDM), and the Home Subscriber Server (HSS). The Sh interface enables the downloading and updating of user data (including quota and entity state information), as well as the requesting of notification on changes to user data.

To protect the system from network issues, the primary and secondary servers typically back up each other using primary and backup connections (see figure).

Figure 3-2 Sh Data Sources Connections



MPE devices send queries to the Sh data source servers in the following order:

1. By Primary connection:
   a. Primary server
   b. Secondary server

   > **Note:**
   >
   > The MPE device processes incoming messages from either primary connection.

2. By Backup connection
   a. Primary server
   b. Secondary server

The MPE device connects with the Sh data source using the following process:

1. The MPE device establishes an Sh Diameter session when it sends a UDR (User-Data-Request) message to the Sh data source. This message requests user profile, quota (optional), and entity state (optional) information. The Sh data source responds with a UDA

(User-Data-Answer) message that includes the requested subscriber information. The MPE device caches the profile information until the session for the subscriber is terminated.

2. The MPE device may also send an SNR (Subscribe-Notifications-Request) message to the Sh data source to request notifications of changes in user information in the data source. The Sh data source responds with an SNA (Subscribe-Notifications-Answer) message.

   > **Note:**
   >
   > The CMP system provides the configuration option to combine the UDR message with an SNR message. See Configuring Sh Settings for details.

3. The MPE device may also send a PUR (Profile-Update-Request) message to the Sh data source to update the user data in the data source. The Sh data source responds with a PUA (Profile-Update-Answer) message indicating the results of the request.
4. The Sh data source can send a PNR (Push-Notification-Request) to the MPE device to notify the device of data source changes in the user information. The MPE device updates the cached profile and re-evaluates the policies for all sessions using the updated profile and responds to the Sh data source with a PNA (Push-Notification-Answer) message indicating the results of the request.

> **Note:**
>
> If an Sh request fails, the MPE device receives an error code ands compares it with a set of error codes and, if the code matches, the MPE retries the request once. See Configuring Advanced Device Settings for details on configuring Sh retry options.

See Configuring an Sh Data Source for details on configuring an Sh data source.

About Sy Data Sources

MPE devices use the Sy interface to connect to the Online Charging System (OCS). This Sy data source provides spending information (using policy counters and statuses) for a specific subscriber. After the device receives the information from the OCS, it uses this data to drive policy decisions for the subscriber.

For an Sy data source, you can define primary, secondary, and tertiary servers. The MPE device sends an SLR (Spending-Limit-Request) message to the primary server first. If it receives no response, it attempts to establish a session with the secondary server. If it receives no response, it then queries the tertiary server. The MPE device queries the data source servers in order, always defaulting to the highest server available. As soon as a higher server becomes available, requests resume to that server.

The MPE device connects with the Sy data source using the following process:

1. The MPE device establishes the Sy Diameter session when it sends an SLR message to the OCS. This session remains active until the session is terminated or the Sy session is lost. The OCS responds with an SLA (Spending-Limit-Answer) message with policy counters and information about the specific subscriber.
2. If the MPE device receives an SNR (Spending-Status-Notification-Request) message from the OCS updating the quota information for the subscriber, the device updates the cached policy counters and re-evaluates any policies. The device responds to the OCS request

with an SNA (Spending-Status-Notification-Answer) message indicating the results of the request.

> **Note:**
>
> See Configuring Sy Settings for details on configuring the Sy data source to use policies to send re-authorization messages.

3. When the MPE device determines that policy decisions for a subscriber no longer require policy counter information for which it has requested notifications of status changes, the device sends a STR (Session-Terminate-Request) message to the OCS to unsubscribe from updates to policy counter status changes. The OCS removes any policy counter subscriptions associated with the Sy session and responds with an STA (Session-Termination-Answer) message to close the session.

See Configuring an Sy Data Source for details on configuring an Sy data source.

About Configuring Data Sources

Configuring a data source in the CMP server includes the sections of parameters listed in Table 3-2.

Table 3-2 Parameter Requirements

Parameter Specifications	Data Source Type		
	LDAP	Sh	Sy
Server info	Required	Required	Required
Search Criteria	Required	Not Required	Not Required
Search Filters	Required for reading	Not Required	Not Required
Associated Data Sources	Optional	Optional	Optional
External Fields	Required for writing	Not Applicable	Not Applicable

Many system deployments require minimal configuration. Most carriers require a single (typically Sh) primary data source. Larger carriers may also have an OCS as a secondary or on-demand data source. Depending on your data source requirements, you must define a data source using the following specifications:

- To define a primary data source, you must configure the **Server Info** tab and set the **Role** as **Primary**.
- To define a secondary data source, you must configure the **Server Info** tab and set the **Role** as **Secondary**. You must also configure the **Associated Data Source** for the primary data source to include the secondary data source.
- To read from an LDAP data source, you must enable **Read Enabled** and configure a **Search Filter**.
- To write to an LDAP data source, you must enable **Write Enabled** and configure one or more **External Fields**.
- To access a data source using policies, you must configure the **Role** as **On-demand**. You can use the policy action, `enable subscription for notification of user profile changes`, where needed.

About Server Info

> **Note:**
>
> You must configure the information on the **Server Info** tab for every data source.

The information configured on the **Server Info** tab defines the various data servers associated with this data source, including the sequence in which lookup requests are sent to the servers.

About Search Criteria

> **Note:**
>
> You must configure the information on the **Search Criteria** tab for LDAP data sources. For Sh or Sy data sources **Search Criteria** configuration is optional.

The **Search Criteria** tab defines the data format of the information that is sent to the data source as part of a query. When accessing LDAP data sources, the criteria identify the location of the target information in the LDAP hierarchy. Additionally, you can modify the format of the key attribute before sending it to any data source. Use industry-standard regular expressions (also known as regex) to define patterns for matching and modifying strings.

Example 3-1 Examples Search Criteria

- Always add a plus sign to the beginning of the MSISDN fora subscriber before sending to the data source:

  Key Type: E.164 (MSISDN)
  Transform Pattern: \+?(.*)
  Replace Pattern: +$1

- Replace the first 5 digits of an IMSI with `11111` before sending to the data source:

  Key Type: IMSI
  Transform Pattern: ([0-9]{5})(.)
  Replace Pattern: 11111$2

About Search Filters

> **Note:**
>
> To read an LDAP data source, you must configure the parameters on the **Search Filters** tab. For Sh and Sy data sources, **Search Filters** are optional.

Search filters allow you to select whether an incoming request results in sending a query to a data source. If no search filters are defined, all received subscriber requests result in a query for each type of defined search criteria being sent to this data source.

> **Note:**
>
> A data source may support multiple search filters.

Example 3-2 Example Search Filters

This example applies to a scenario where subscriber information is distributed across three data sources based on the last two digits of the E.164 (MSISDN) key attribute. Using search filters, you can direct a query to the appropriate data source.

- **Data Source #1**: Define a search filter that performs lookups only for subscribers ending with 00 through 33:

  Key Type: E.164 (MSISDN)
  Expression: `(.)*(0[0-9] | 1[0-9] | 2[0-9] | 3[0-3])`

- **Data Source #2**: Define a search filter that performs lookups only for subscribers ending with 34 through 66:

  Key Type: E.164 (MSISDN)
  Expression: `(.)*(3[4-9] | 4[0-9] | 5[0-9] | 6[0-6])`

- **Data Source #3**: Define a search filter that performs lookups only for subscribers ending with 67 through 99:

  Key Type: E.164 (MSISDN)
  Expression: `(.)*(6[7-9] | 7[0-9] | 8[0-9] | 9[0-9])`

About External Fields

> **Note:**
>
> To write data to an LDAP data source, you must define external fields on the **External Fields** tab.

External fields simplify writing data to an LDAP data source. External fields define short names and map them to specific LDAP data source attributes and distinguished names (DNs). Then you can use the same external field name when writing a policy that will be deployed across multiple MPE devices. The policy assigns a value and writes it to an LDAP server. The policy actions that use external fields include:

- `set` *`external field`* `to` *`'value'`*
- `set` *`external field`* `to #` `percent of` *`select type`* `for` *`selected`* `quota`

Refer to the *Policy Wizard Reference* for details on creating and managing policies.

About Associated Data Sources

> **Note:**
>
> The information configured on the **Associated Data Sources** tab applies to primary data sources only.

The **Associated Data Sources** tab lists all possible secondary data sources that can be queried when a response is received from the primary data source. The secondary data sources are listed in priority order, that is, the first data source will be queried first then the second, and so forth.

Viewing Data Sources

To view a list of data sources defined in 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.
3. Select the **Data Sources** tab.

   The page lists the current data sources, including the following configuration information:
   - Administrative State (Enabled or Disabled)
   - Name
   - Role (Primary or Secondary)
   - Subscription State (Enabled or Disabled)
   - Type (Sh, Sy or LDAP)
   - Primary host (FQDN)
   - Secondary host (optional)
   - Tertiary host (optional)
   - Transport Type (TCP or SCTP)
   - Transport Info (number of TCP or SCTP connections)
   - Protocol Timer Profile
   - General Settings
   - Sh Settings
   - Sy Settings

Adding a Data Source

Before the MPE device can communicate with any data sources, you must first configure the data source and its connections.

After the data sources are configured, configure other relevant MPE parameters (for example, subscriber indexing options, lookup retry options) using the **Policy Server** tab for each MPE device (see Configuring MPE Protocol Options). You can also configure Sh retry options (see Configuring Advanced Device Settings for details).

To add a data source:

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 page lists the current data sources.

4. To add a data source, click **Modify**.

   The Modify Data Sources page opens.

5. To add a data source using the settings for an existing data source:

   a. From the data source listing, select the data source to copy.

   b. Click **Clone**.

      The Clone Data Source window opens.

   c. Edit the data source configuration parameters as needed, especially the Unique Name.

   d. Click **Save** to save the data source and close the Clone Data Source window.

6. To add a new data source:

   a. Click **Add** and select the data source type from the **Add** list.

      The appropriate Add Data Source window opens.

   b. Configure the values as described in the appropriate section:

      - 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.

   c. Click **Save** to save the data source and close the Add Data Source window.

7. Click **Save** to save your changes and close the Modify Data Sources page for editing.

Configuring an LDAP Data Source

You can configure connections to up to three LDAP servers. To add an LDAP data source:

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 page lists the current data sources defined in the specified device.

4. To modify the list of data sources, click **Modify**.

   The Modify Data Sources page opens.

5. Click **Add** () and select **LDAP**.

   The Add Data Source window appears.

6. Select each tab and enter the information as described in the following sections:

   - Configuring LDAP Server Information
   - Defining LDAP Search Criteria
   - Defining LDAP Subscription ID Filters
   - Selecting LDAP Associated Data Sources

- Defining LDAP External Fields

Configuring LDAP Server Information

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

1. Select the **Role** from the list:
   - **Primary**
     Indicates the data source that performs the initial lookup operation.
   - **Secondary**
     Indicates a dependency on the results of the initial lookup operation to the primary data source.

   > **Note:**
   >
   > You must configure the secondary data source as an **Associated Data Source** in the primary data source configuration.

2. Enter an **Unique Name**.

   Identifies the data source.
3. Select to enable the **Admin State** (that is, enable this data source).

   The default value is enabled. If disabled, the server receives no primary or secondary queries.
4. Select **Read Enabled**.

   Enables read access to this data source. The default value is enabled.
5. If you specified the **Role** as **Primary**, select **Write Enabled**.

   Enables write access to this data source. The default value is disabled.
6. Enter the **Primary Host**.

   Specifies the FQDN or IP address (in IPv4 or IPv6 format) of the primary LDAP server.
7. Enter the **Primary Port** number.

   The default value is 389.
8. Enter the **Secondary Host**.

   Specifies the FQDN or IP address (in IPv4 or IPv6 format) of the secondary LDAP server.
9. Enter the **Secondary Port** number.

   The default value is 389.
10. Enter the **Tertiary Host**.

    Specifies the FQDN or IP address (in IPv4 or IPv6 format) of the tertiary LDAP server.
11. Enter the **Tertiary Port** number.

    The default value is 389.
12. Enter the **Authentication DN**.

    Specifies the Distinguished Name (DN) used for binding (that is, establishing a connection) to the LDAP database. 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
- `o`
  Domain name

For example, `cn=PolicyServer,ou=galactel,o=example.com`. See About LDAP Data Sources for more information.

13. Enter the **LDAP Password**.

    This parameter is required for read-only access the LDAP directory. The MPE device must bind to the LDAP server with the **Authentication DN** and the **LDAP Password** to access the database.

14. If you specified the **Role** as **Secondary**, select the number of **Read Connections** from the list.

    You can select up to 10 connections. The default value is one.

15. If you specified the **Role** as **Primary**, select the number of **Write Connections** from the list.

    You can select up to 10 connections. The default value is one.

16. If you specified the **Role** as **Secondary**, proceed with Defining LDAP Search Criteria; otherwise, click **Save**.

Defining LDAP Search Criteria

> **Note:**
>
> **Search Criteria** only applies to secondary data sources. LDAP data sources require **Search Criteria**.

Use the **Search Criteria** tab to define the data format for each type of subscriber index key that will be used with this data source. On the **Search Criteria** tab, enter the following:

- From the left pane, select how the LDAP database is indexed:
  1. **Alternate Key**—See Data Source Indexed by Alternate Key for details.
  2. For details on configuring criteria for any of the following indexes:
     - **Username**
     - **NAI**
     - **E.164 (MSISDN)**
     - **IMSI**

     See Data Source Indexed by Username, NAI, MSISDN, or IMSI.

Data Source Indexed by Alternate Key

If you selected **Alternate Key** as the indexing method on the **Search Criteria** tab, enter the following:

1. Enter the **Alternative Key Name** for the **Search Key**.

   Enables you to use a non-standard entity as the search key.

2. To define the **Key Transformation**:

   a. Enter the **Key Transform Pattern**.

      Specifies a regular expression (regex) pattern used for transforming the search key.

   b. Enter the **Key Replace Pattern**.

      Specifies a replacement string used to transform the search key.

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

3. To define the **Search DN**:

   a. Enter the **Root DN**.

      Specifies the location in the data source directory where the search starts.

   b. Enter the **Base DN Attribute**.

      If the **Scope** is **Object**, the MPE device prepends this value to the Root DN when building the DN for a search.

4. Select the **Search Scope** from the list:

   - **One-Level**
     Extends the scope of the LDAP data search to one level under the given Root DN.

   - **Sub-Tree** (default)
     Extends the scope of the LDAP search to the whole sub-tree under the given Root DN.

   - **Object**
     Restricts the scope of the LDAP search to the specified object.

5. Enter the **LDAP Attribute Name**.

   Specifies the attribute whose value is checked to match the key value. The attribute is used to construct a search filter in the form `KeyAttribute=KeyValue`.

6. Enter an **Extra Filter**.

   Specifies free-form text that the MPE device appends to the search filter defined by the **Key Attribute**.

7. Enter the **Retrieved Attributes**.

8. Proceed with Defining LDAP Subscription ID Filters.

Data Source Indexed by Username, NAI, MSISDN, or IMSI

If you selected **Username** (account ID), **NAI** (Network Access Identifier), **E.164 (MSISDN)** (phone number), or **IMSI** (International Mobile Subscriber Identity) as the indexing method on the **Search Criteria** tab, set the following parameters:

1. Enter the **Root DN**.

   Specifies the location in the data source directory where the search starts.

   For example, `ou=galactel_uk,o=galactel.com`.

2. Select the **Scope** of the search from the list:
   - **One-Level**
     Extends the scope of the LDAP data search to one level under the given Root DN.
   - **Sub-Tree** (default)
     Extends the scope of the LDAP search to the whole sub-tree under the given Root DN.
   - **Object**
     Restricts the scope of the LDAP search to the specified object.
3. Enter the **Key Attribute**.

   This parameter identifies the attribute whose value is checked to match the key value of the query. Enter the attribute using the format `KeyAttribute=KeyValue`. If the **Scope** is **One-Level** or **Sub-Tree**, the attribute specifies the match criteria for the search.
4. Enter an **Extra Filter**.

   Specifies free-form text that the MPE device appends to the search filter defined by the **Key Attribute**.
5. Enter the **Base DN Attribute**.

   If the **Scope** is **Object**, the MPE device prepends this value to the Root DN when building the DN for a search.
6. Enter the **Key Transform Pattern**.

   Specifies a regular expression (regex) pattern used to transform the key.
7. Enter the **Key Replace Pattern**.

   Specifies a replacement string used 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. Enter the **Attributes**.

   Specifies a comma-separated list of entries defining which objects will be returned from the LDAP data source search. The default value is null, meaning that all values returned. Otherwise, each entry should use one or more of the following formats:
   - `attr`
     The name of the attribute that is returned by this search, for example `nai`. You can use attribute names to define policies.
   - `field=attr`
     Each specified attribute (`attr`) is stored in a Policy Content Property (PCP) named {`field`}. For example, `name=nai`. You can use the PCP `name` to define policies

     .
   - `field=attr[from:to]`
     The specified subset of the attribute (`attr`) is stored in a Policy Content Property (PCP) named {`field`}. The `from` and `to` values define the starting and ending points in the string. For example, if the NAI for the retrieved record is `Chartwell`, then `name=nai[1:3]` stores the string `Cha` in a PCP named `name`. You can use the PCP `name` to define policies.

     > **Note:**
     >
     > A value of `0` in `from` indicates the beginning of the value. A value of `0` in `to` indicates the end of the value.

9. Proceed with Defining LDAP Subscription ID Filters.

Defining LDAP Subscription ID Filters

You can configure multiple search filters per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters.

> **Note:**
>
> Best practice recommends to priority order filtered data sources higher than unfiltered ones. See Ordering Data Source Priority for details on re-ordering data sources.

The APN search filter supports regular expressions and uses these patterns:

- Wild Card: Pattern.*
- Equal to: Pattern
- Not Equal to: ^(?!.*Pattern).*$

These rules are followed when using the search filters:

- If only subscription ID filters exist, if at least one subscription ID filter is matched, the result is matched.
- If only APN filters exist, if at least one APN filter is matched, the result is matched.
- If APN filters and subscription ID filters exist, if at least one subscription ID filter and one APN filter are matched, the result is matched.

To define LDAP Subscription ID search filters:

1. Click **Search Filters** tab.
2. In the Subscription ID section, select the **Key Type** from the list:
   - **User Name** (default)
     User name (account ID)
   - **NAI**
     Network address ID
   - **E.164 (MSISDN)**
     E.164 phone number
   - **IMSI**
     International Mobile Subscriber Identity
   - **IP Address**
     IP address
3. Enter a regular expression to use to filter the search results.

   For example:
   - `508.*`
     Matches numbers beginning with `508`
   - `".*@example.com"`
     Matches strings ending with `@example.com`
   - `.*`
     Matches any input string

4. Click **Add**.

   The expression appears in the list of search filters.

5. Click **Save** or proceed with Selecting LDAP Associated Data Sources.

Defining LDAP APN Filters

Define the APN name to filter the data source. You can configure multiple search filters per data source.
The APN search filter supports regular expressions and uses these patterns:

- Wild Card: Pattern.*
- Equal to: Pattern
- Not Equal to: ^(?!.*Pattern).*$

These rules are followed when using the search filters:

- If only subscription ID filters exist, if at least one subscription ID filter is matched, the result is matched.
- If only APN filters exist, if at least one APN filter is matched, the result is matched.
- If APN filters and subscription ID filters exist, if at least one subscription ID filter and one APN filter are matched, the result is matched.

To define LDAP APN filters:

1. Click **Search Filters** tab.
2. In the APN Filters section, enter a regular **Expression** to use to filter the search results.

   For example:

   - `508.*`
     Matches numbers beginning with `508`
   - `".*@example.com"`
     Matches strings ending with `@example.com`
   - `.*`
     Matches any input string
3. Click **Add**.

   The expression appears in the list of search filters.
4. Click **Save** or proceed with Selecting LDAP Associated Data Sources.

Deleting LDAP Subscription ID Filters

You can delete search filters per data source.
To delete LDAP Subscription ID filters:

1. Click **Search Filters** tab.
2. In the Subscription ID section of the window, select an expression in the list.
3. Click **Delete**.

   The selected expression is removed from the list.
4. Click **Save** or proceed with Selecting LDAP Associated Data Sources.

Deleting LDAP APN Filters

You can delete APN search filters per data source.
To delete LDAP APN filters:

1. Click **Search Filters** tab.
2. Select it and click **Delete**.

   The selected expression is removed from the list.
3. In the APN filters section of the window, select the expression in the list.
4. Click **Delete**.

   > **Note:**
   >
   > The filter is deleted without a conformation. However the deletion is not final until you click save. If you want to reverse the deletion, click **Cancel** on the **Search Filters** tab.
5. Click **Save** or proceed with Selecting LDAP Associated Data Sources.

Selecting LDAP Associated Data Sources

> **Note:**
>
> The Associated Data Sources information applies only to primary data sources.

On the **Associated Data Sources** tab:

1. From the **Associated Data Sources** list, select any secondary data sources that can be used with the primary data source.

   The list is displayed in the priority order listing of the secondary data sources on the Modify Data Sources page.
2. To change the priority order, see Ordering Data Source Priority.
3. Select **Deselect All** if you do not want to send a lookup to any secondary server.
4. Click **Save** to save your changes or proceed to Defining LDAP External Fields.

Defining LDAP External Fields

The **External Fields** tab lets you define external fields and map them to specific LDAP data source attributes and distinguished names (DNs). A policy uses a defined External Field to write data to an LDAP data source. You can define up to 50 attributes per data source.
To define an External Field:

1. To define a new external field:
   a. Click **Add**.

      The Add External Field window opens.
   b. Enter the **External Field Name**.

    This value specifies the variable name used in the policy for write actions to the LDAP database

   c. Enter the **LDAP Attribute Name**.

      This value specifies the database attribute entity.

   d. Enter the **DN** (distinguished name).

      This value specifies the location in the directory.

   e. Click **Save**.

2. (Optional) To clone, modify, or delete an existing external field use the following functions:

   - Cloning an entry in the table

     a. Select an entry in the table.

     b. Click **Clone**. The Clone window opens with the information for the entry.

     c. Make changes as required.

     d. Click **Save**. The entry is added to the table.

   - Editing an entry in the table

     a. Select the entry in the table.

     b. Click **Edit**. The Edit Response window opens, displaying the information for the entry.

     c. Make changes as required.

     d. Click **Save**. The entry is updated in the table.

   - Deleting a value from the table

     a. Select the entry in the table.

     b. Click ✕ **Delete**. A confirmation message displays.

     c. Click **Delete** to remove the entry. The entry is removed from the table.

Configuring an Sh Data Source

You can configure connections to up to two active primary servers and two standby backup servers. To add an Sh data source:

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 page lists the current data sources.

4. To modify the list of data sources, click **Modify**.

   The Modify Data Sources page opens.

5. Click **Add** () and select **Sh**.

   The Add Data Source window appears.

6. Select each tab and enter the information as described in the following sections:

- Configuring Sh Server Information (required)
- Defining Sh Search Criteria (optional)
- Defining Sh Subscription ID Filters (optional)
- Selecting Sh Associated Data Sources (optional)

7. After configuring the Sh data source, proceed to Configuring Sh Settings.

Configuring Sh Server Information

On the Server Info tab:

1. Select to enable the **Admin State**.

   The default value is enabled. If disabled, the server receives no primary or secondary queries.

2. Enter the server's **Realm**.

   For example, `example.com`.

3. Select to **Enable Subscription**.

   If enabled, the MPE device subscribes to receive updates to data source records which have previously been sent to the device.

   > **Note:**
   >
   > If **Enable Subscription** for the Sh data source is selected, enabling **Combine Lookup And Subscription** (see Configuring Sh Settings) allows the system to combine user profile changes within the SNR/SNA requests for all users. If **Enable Subscription** is not selected, the system sends UDR/UDA requests but no SNR/SNA requests.

4. Enter a **Unique Name** to identify the data source.

   Use alphanumeric and special characters.

5. Select to **Use Notif-Eff**.

   If enabled, the Sh data source reads multiple user data blocks in a single message. Enable this option only if the Sh data source supports this functionality.

6. Select the **Sh Profile** from the list:

   - **ProfileV1** (default)
     Select for generic Sh data repositories.
   - **ProfileV2**
     Select for SPR release 7.5 and earlier. This release supports user, quota and state service indications for individual subscribers.
   - **ProfileV3**
     Select for SPR release 8.0 and higher. This release supports pools, pooled quotas, and pool states.
   - **ProfileV4**
     Select for Oracle Communications User Data Repository (UDR) release 10.0 and higher. This release supports dynamic quotas for both individual users and pools.

7. Select the **Protocol Timer Profile**.

See Managing Protocol Timer Profiles for more information.

8. Select the **Transport** protocol:
   - **TCP**
     Indicates the MPE device will communicate with this data source using Transmission Control Protocol.
     - Select the number of **Connections** (up to a maximum of 8) from the list.
   - **SCTP**
     Indicates the MPE device will communicate with this data source using Stream Control Transmission Protocol.
     - Select the number of **Max Incoming Streams** (up to a maximum of 8) from the list.
     - Select the number of **Max Outcoming Streams** (up to a maximum of 8) from the list.
9. Enter the information for the **Primary Server**:
   a. Enter the **Primary Identity**.

      Specifies the host name (Diameter identity) or FQDN of the primary server.

   b. Enter the **Primary Address**.

      Specified the IP address of the primary server. If omitted, the **Primary Identity** of the primary server is used to look up the server address.

   c. Enter the **Primary Port**.

      The default value is 3868.

   d. Enter the **OAM IP**.

      Specifies the IP address the Oracle Access Management (that is, the CMP server) uses when communicating to the Sh data source when using RESTful APIs.

   e. Enter the **Secondary Identity**.

      Specifies the host name (Diameter identity) or FQDN of the secondary server.

   f. Enter the **Secondary Address**.

      Specifies the IP address of the secondary server. If omitted, the secondary identity of the secondary server is used to look up the server address.

   g. Enter the **Secondary Port**.

      The default value is 3868.
10. Enter the information for the **Backup Server**:
   a. Enter the **Primary Identity**.

      Specifies the host name (Diameter identity) or FQDN of the primary server.

   b. Enter the **Primary Address**.

      Specified the IP address of the primary server. If omitted, the **Primary Identity** of the primary server is used to look up the server address.

   c. Enter the **Primary Port**.

      The default value is 3868.

   d. Enter the **OAM IP**.

      Specifies the IP address the Oracle Access Management (that is, the CMP server) uses when communicating to the Sh data source when using RESTful APIs.

e. Enter the **Secondary Identity**.

   Specifies the host name (Diameter identity) or FQDN of the secondary server.

f. Enter the **Secondary Address**.

   Specifies the IP address of the secondary server. If omitted, the secondary identity of the secondary server is used to look up the server address.

g. Enter the **Secondary Port**.

   The default value is 3868.

11. Click **Save** to save your changes or proceed with Defining Sh Search Criteria (optional).

Defining Sh Search Criteria

> **Note:**
>
> **Search Criteria** only applies to secondary data sources. Sh data sources do not require **Search Criteria**.

Use the **Search Criteria** tab to define the key format for each type of subscriber index that will be used with this data source.

On the **Search Criteria** tab:

1. From the left pane, select how the Sh database is indexed:
   - **NAI**
     Network address ID
   - **E.164 (MSISDN)**
     Phone number
   - **IMSI**
     International Mobile Subscriber Identity
2. **Key Transform Pattern**.

   Specifies a regular expression (regex) pattern used to transform the key.
3. **Key Replace Pattern**.

   Specifies a replacement string to use to transform the key.

   For example, `17$2` means the new string starts with `17` and is followed by the group 2 (`$2`) pattern.
4. Click **Save** to save your changes or proceed with Defining Sh Subscription ID Filters (optional).

Defining Sh Subscription ID Filters

You can configure multiple search filters per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters.

> **Note:**
>
> Best practice recommends to priority order filtered data sources higher than unfiltered ones. See Ordering Data Source Priority for details on re-ordering data sources.

The APN search filter supports regular expressions and uses these patterns:

- Wild Card: Pattern.*
- Equal to: Pattern
- Not Equal to: ^(?!.*Pattern).*$

These rules are followed when using the search filters:

- If only subscription ID filters exist, if at least one subscription ID filter is matched, the result is matched.
- If only APN filters exist, if at least one APN filter is matched, the result is matched.
- If APN filters and subscription ID filters exist, if at least one subscription ID filter and one APN filter are matched, the result is matched.

To define search filters:

1. Click the **Search Filters** tab.
2. Select the **Key Type** from the list:
   - **NAI** (network address ID)
   - **E.164 (MSISDN)** (phone number)
   - **IMSI** (International Mobile Subscriber Identity)
3. Enter a regular expression.

   For example:
   - `508.*`
     Matches numbers beginning with `508`
   - `".*@example.com"`
     Matches strings ending with `@example.com`
   - `.*`
     Matches any input string
4. Click **Save**.

   The expression appears in the list of **Search Filters**.
5. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Defining Sh APN Filters

Define the APN name to filter the data source. You can configure multiple search filters per data source.
The APN search filter supports regular expressions and uses these patterns:

- Wild Card: Pattern.*
- Equal to: Pattern
- Not Equal to: ^(?!.*Pattern).*$

These rules are followed when using the search filters:

- If only subscription ID filters exist, if at least one subscription ID filter is matched, the result is matched.
- If only APN filters exist, if at least one APN filter is matched, the result is matched.
- If APN filters and subscription ID filters exist, if at least one subscription ID filter and one APN filter are matched, the result is matched.

To define Sh APN filters:

1. Click the **Search Filters** tab.
2. In the APN Filters, enter a regular **Expression**.

   For example:

   - `508.*`
     Matches numbers beginning with `508`
   - `".*@example.com"`
     Matches strings ending with `@example.com`
   - `.*`
     Matches any input string
3. Click **Save**.

   The expression appears in the list of **Search Filters**.
4. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Deleting Sh Subscriber ID Filters

You delete search filters per data source.
To delete search filters:

1. Click the **Search Filters** tab.
2. In the Subscriber ID Filters section of the window, select the expression in the list.
3. Click **Delete**.

   > **Note:**
   >
   > The filter is deleted without a conformation. However the deletion is not final until you click save. If you want to reverse the deletion, click **Cancel** on the **Search Filters** tab.
4. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Deleting Sh APN Filters

You can delete APN filters per data source.
To delete search filters:

1. Click the **Search Filters** tab.
2. In the APN filters section of the window, select the expression in the list.

3. Click **Delete**.

> **Note:**
>
> The filter is deleted without a conformation. However the deletion is not final until you click save. If you want to reverse the deletion, click **Cancel** on the **Search Filters** tab.

4. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Selecting Sh Associated Data Sources

> **Note:**
>
> The Associated Data Sources information applies only to primary data sources.

On the **Associated Data Sources** tab:

1. From the **Associated Data Sources** list, select any secondary data sources that can be used with the primary data source.

   The list is displayed in the priority order listing of the secondary data sources on the Modify Data Sources page.
2. To change the priority order, see Ordering Data Source Priority.
3. If you do not want to send a lookup request to any secondary server, click **Deselect All**.
4. Click **Save** to save your changes.

Configuring an Sy Data Source

To add an Sy data source:

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 page lists the current data sources.
4. To modify the list of data sources, click **Modify**.

   The Modify Data Sources page opens.
5. Click **Add** (+) and select **Sy**.

   The Add Data Source window opens.
6. Proceed to Configuring Sy Server Information.
7. After configuring the Sy data source, proceed to Configuring Sy Settings.

Configuring Sy Server Information

To configure the server information for an Sy data source:

1. Select the **Server Info** tab.
2. Select to enable the **Admin State**.

   Enabled is the default state. If disabled, the server receives no primary or secondary queries.
3. To specify the **Role** (that is, how and when the data source is used to look up information in the database):
   - If the MPE device automatically queries the data source, select **Automatic** and select one of the following roles from the list:
     - Select **Primary** (default) if the MPE device directly queries this data source when data is needed.
     - Select **Secondary** if this data source will be queried only after a successful query to a primary data source.
   - If the MPE device uses a policy to access a data source, select **On Demand**.
4. Enter the **Realm** to define the Diameter realm of the primary and optional secondary servers.

   For example, `galactel.com`.
5. Enter a **Unique Name** to identify this data source.

   Use alphanumeric and special characters.
6. Select a **Protocol Timer Profile** from the list.

   See Managing Protocol Timer Profiles for more information.
7. Select the **Transport** protocol:
   - **TCP**
     Indicates the MPE device will communicate with this data source using the Transmission Control Protocol.
     - Select the number of **Connections** (up to a maximum of 8) from the list.
   - **SCTP**
     Indicates the MPE device will communicate with this data source using the Stream Control Transmission Protocol.
     - Select the number of **Max Incoming Streams** (up to a maximum of 8) from the list.
     - Select the number of **Max Outgoing Streams** (up to a maximum of 8) from the list.
8. Enter the information for the **Primary Servers**:
   a. Enter the **Identity**.

      Specifies the host name (Diameter identity) or FQDN of the primary server.

   b. Enter the **Primary Address**

      Specifies the IP address of the primary server. If omitted, the **Identity** of the primary server is used to look up the server address.

   c. Enter the **Primary Port**.

The default value is 3868.

9. (Optional) Enter the information for the **Secondary Server**:
   1. Enter the **Identity**.

      Specifies the host name (Diameter identity) or FQDN of the secondary server.
   2. Enter the **Secondary Address**.

      Specifies the IP address of the secondary server. If omitted, the **Identity** of the secondary server is used to look up the server address.
   3. Enter the **Secondary Port**.

      The default value is 3868.
10. (Optional) Enter the information for the **Tertiary Server**:
    1. Enter the **Identity**.

       Specifies the host name (Diameter identity) or FQDN of the tertiary server.
    2. Enter the **Tertiary Address**.

       Specifies the IP address of the tertiary server. If omitted, the **Identity** of the tertiary server is used to look up the server address.
    3. Enter the **Tertiary Port**.

       The default value is 3868.
11. Click **Save** to save your changes or proceed with Defining Sy Search Criteria (optional).

Defining Sy Search Criteria

> **Note:**
>
> **Search Criteria** only applies to secondary data sources. Sy data sources do not require **Search Criteria**.

Use the **Search Criteria** tab to define the key format for each type of subscriber index that will be used with this data source.
On the **Search Criteria** tab:

1. Select the **Search Criteria** tab.
2. From the left pane, select how the Sy database is indexed:
   - If the **Role** is **Secondary**, select **Alternate Key** to use a non-standard entity as the search key.
   - **NAI** (network address ID)
   - **E.164 (MSISDN)** (phone number)
   - **IMSI** (International Mobile Subscriber Identity)
3. If you selected **Alternate Key**, enter the **Alternative Key Name** for the **Search Key**.
4. Enter the **Key Transform Pattern** to transform the search key.
5. Enter the **Key Replace Pattern** as a replacement string to transform the key.

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

6. Click **Save** to save your changes or proceed with Defining Sy Subscription ID Search Filters (optional).

Defining Sy Subscription ID Search Filters

You can configure multiple search filters per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters.

> **Note:**
>
> Best practice recommends to priority order filtered data sources higher than unfiltered ones. See Ordering Data Source Priority for details on re-ordering data sources.

The APN search filter supports regular expressions and uses these patterns:

- Wild Card: Pattern.*
- Equal to: Pattern
- Not Equal to: ^(?!.*Pattern).*$

These rules are followed when using the search filters:

- If only subscription ID filters exist, if at least one subscription ID filter is matched, the result is matched.
- If only APN filters exist, if at least one APN filter is matched, the result is matched.
- If APN filters and subscription ID filters exist, if at least one subscription ID filter and one APN filter are matched, the result is matched.

To define search filters:

1. Click the **Search Filters** tab.
2. In the Subscription ID filters section of the window, click **Add**.

   The Add Search Key Value window opens.
3. Select the **Key Type** from the list:
   - **NAI**
     Network address ID
   - **E.164 (MSISDN)**
     Phone number
   - **IMSI**
     International Mobile Subscriber Identity
   - **Alternate Filter**
     If the Sy data source is a secondary data source, the **Alternate Filter** specifies a subscriber profile attribute retrieved from the primary data source lookup process. For example, if the primary data source returned a subscriber profile attribute named `PaymentPlan` with a value of either `Prepaid` or `Postpaid`, you could configure an alternate filter, `PaymentPlan`, to direct Sy lookup procedures for `Prepaid` subscribers to one data source and `Postpaid` subscribers to a different data source.
4. Enter a regular **Expression**.

   For example:
   - `508.*`

Matches numbers beginning with `508`

- `".*@example.com"`
  Matches strings ending with `@example.com`
- `.*`
  Matches any input string

5. Click **Save**.

   The expression displays in the list of **Filters** in the Subscription ID filters section of the window.

6. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Defining Sy APN Filters

Define the APN name to filter the data source. You can configure multiple search filters per data source.
The APN search filter supports regular expressions and uses these patterns:

- Wild Card: Pattern.*
- Equal to: Pattern
- Not Equal to: ^(?!.*Pattern).*$

These rules are followed when using the search filters:

- If only subscription ID filters exist, if at least one subscription ID filter is matched, the result is matched.
- If only APN filters exist, if at least one APN filter is matched, the result is matched.
- If APN filters and subscription ID filters exist, if at least one subscription ID filter and one APN filter are matched, the result is matched.

To define Sy APN filters:

1. Click the **Search Filters** tab.
2. In the APN Filters section of the window, enter a regular expression.

   For example:

   - `508.*`
     Matches numbers beginning with `508`
   - `".*@example.com"`
     Matches strings ending with `@example.com`
   - `.*`
     Matches any input string

3. Click **Add**.

   The expression displays in the list of **Filters** in the APN Filters section of the window.

4. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Modifying Sy Subscription ID Filters

You can modify search filters for a data source.

> **Note:**
>
> Best practice recommends to priority order filtered data sources higher than unfiltered ones. See Ordering Data Source Priority for details on re-ordering data sources.

To modify search filters:

1. Click the **Search Filters** tab.

   The Add Search Key Value window appears.
2. In the Subscription ID filters section of the window, select the expression in the list.
3. Click **Edit**.
4. Modify the filter.
5. Click **Save**.
6. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Deleting Sy Subscription ID Filters

You can delete search filters per data source.
To delete search filters:

1. Click the **Search Filters** tab.
2. In the Subscription ID filters section of the window, select the expression in the list.
3. Click **Delete**.

   > **Note:**
   >
   > The filter is deleted without a conformation. However the deletion is not final until you click save. If you want to reverse the deletion, click **Cancel** on the **Search Filters** tab.
4. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Deleting Sy APN Filters

You can delete APN search filters per data source.
To delete APN search filters:

1. Click the **Search Filters** tab.
2. In the APN filters section of the window, select the expression in the list.
3. Click **Delete**.

> **Note:**
>
> The filter is deleted without a conformation. However the deletion is not final until you click save. If you want to reverse the deletion, click **Cancel** on the **Search Filters** tab.

4. Click **Save** to save your changes or proceed with Selecting Sy Associated Data Sources (optional).

Selecting Sy Associated Data Sources

> **Note:**
>
> The Associated Data Sources information applies only to primary data sources.

The **Associated Data Sources** tab displays a list of all possible secondary data sources that can be used with this primary data source, listed in priority order.

To selecting the Sy associated data source:

1. From the **Associated Data Sources** list, select any secondary data sources that can be used with the primary data source.

   The list is displayed in the priority order listing of the secondary data sources on the Modify Data Sources page.
2. To change the priority order, see Ordering Data Source Priority.
3. Select **Deselect All** if you do not want to send a lookup to any secondary server.
4. Click **Save** to save your changes.

Modifying a Data Source

To modify a data source:

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 page lists the current data sources.
4. Click **Modify**.

   The Modify Data Sources page opens.
5. Select the data source from the list.
6. Click **Edit**.

   The Edit Data Source window opens.
7. See the following sections for data type-specific settings:
   - 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.

8. Click **Save**.
9. Click **Save** to close the Modify Data Sources page.

   The CMP system saves your changes.

Ordering Data Source Priority

To order the priority of data sources:

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 page lists the current data sources.
4. To modify the list of data sources, click **Modify**.

   The Modify Data Sources page opens.
5. To set the priority order for listed data sources:
   a. To move a data source to a higher priority, select the data source and click ⬆ Up.
   b. To move a data source to a lower priority, select the data source and click ⬇ Down.
   c. Repeat as needed until the data sources are correctly ordered.
6. Click **Save** to close the Modify Data Sources page.

   The CMP system saves your changes.

Deleting a Data Source

To delete a data source:

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 page lists the current data sources.
4. Click **Modify**.

   The Modify Data Sources page opens.
5. Select the data source from the listing.
6. Click ✕ **Delete**.

   A message displays asking you to confirm the deletion of the data source.
7. Click **Delete** to proceed.

8. Click **Save**.

The CMP system saves your changes.

Configuring General Settings for an MPE device

To configure the general settings for 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.
3. Select the **Data Sources** tab.

   The page lists the current data sources.
4. Click **Modify**.

   The Modify Data Sources page opens.
5. The following general settings are available:
   - **Merge Search Results**
     If this option is set to **False** and you have defined multiple data sources and a search returns results from more than one source, the results are displayed in source order.

     To display search results in one sorted list, set this option to **True**. If enabled,, multiple primary data sources are searched asynchronously. Secondary searches are dependent on the results of the primary data sources 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.
   - **Subscription Enabled Via Policy Only**
     If this option is set to **True**, the MPE device will only send SNR (Subscription-Notifications-Requests) messages to data sources when a policy is executed that includes the policy action `enable subscription for notification of user profile changes`. If the option is set to **False**, you can enable subscriptions by setting the appropriate Subscribe options (see Configuring MPE Protocol Options).
6. Click **Save**.

Configuring Sh Settings

To configure Sh settings:

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 page lists the current data sources.
4. Click **Modify**.

   The Modify Data Sources page opens.
5. The following Sh settings are available:

- **Notification Re-auth Via Policy**
  If this option is enabled (that is, set to **True**), the MPE device processes every notification to determine whether it should generate a re-authorization request. If this setting is not enabled (default), the MPE device only re-evaluates policies after it receives a PNR (Push-Notification-Request) message related to provisioning (such as, user profile, pool profile, dynamic quota, or pool dynamic quota notifications).

  If you enable this option, you must define policy rules to specifically generate the re-authorization messages. See *Policy Wizard Reference* for more information on policy rules.
- **Combine Lookup And Subscription**
  If set to **True**, lookup and subscription requests are combined in one message.

  > **Note:**
  >
  > If **Enable Subscription** for the Sh data source is selected, enabling this option allows the system to combine user profile changes within the SNR/SNA requests for all users. If **Enable Subscription** is not selected, the system sends UDR/UDA requests but no SNR/SNA requests.

6. Click **Save**.

Configuring Sy Settings

To configure Sy settings:

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 page lists the current data sources.
4. Click **Modify**.

   The Modify Data Sources page opens.
5. Click **Save**.

Connecting to Multiple Data Sources

When multiple data sources being set in a system, there should not be an assumption that a subscriber that is not found in one data source will be available in the next one. Each data source is expected to have a different set of subscribers (or keys) and filters on the MPE that are used to direct queries to a specific data source. The only scenario is were the provisioned subscriber base is expected to be replicated among the servers within a data source. If you have multiple data sources, the following are the functionality scenarios supported.

1. Primary and Secondary role data sources
   Primary and Secondary roles are used to designate a data source to target with the first query. A key retrieved from the first server (Primary) is used to query the Secondary server. If the Primary server query times out, the Secondary server is not queried because of the dependency.

2. Primary Data sources configured for Merge Results functionality
The Primary Data sources are queried simultaneously to retrieve different sets of data about a subscriber which is then merged for a complete profile. There is not a question of timeout and the try next data source as dependency does not exist as in scenario 1.
3. Multiple Primary data sources with different provisioned subscriber base
Filters are used to direct queries to specific Data Sources. There is not an automatic query of the next data source after timeout because filters for each data source are different. the MPE can still query across the data source boundary using the priority order in the GUI data source table.

> **Important:**
>
> There must be an explicit UNKNOWN SUBSCRIBER response from the first data queried for this to occur. A timeout or no response from first data query will not trigger the lookup of next data source

Policy Server Groups

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

Creating a Policy Server Group

To create a policy server group:

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

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

   The Policy Server Administration page opens in the work area.
3. Click **Create Group**.

   The Create Group page opens.
4. Enter the name of the new policy server group.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
5. Click **Save**.

You have created a policy server group.

Adding a Policy Server to a Policy Server Group

To add a policy server to a policy server group:

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

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

   The Policy Server Administration page opens in the work area displaying the contents of the selected policy server group.

3. Click **Add Policy Server**.

   The Add Policy Server page opens, displaying the policy servers not already part of the group.

4. Click the policy server you want to add; press Ctrl or Shift-Ctrl to select multiple policy servers.
5. Click **Save**.

The policy server is added to the selected group.

Creating a Policy Server Sub-group

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

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

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

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

   The Policy Server Administration page opens in the work area, displaying the contents of the selected policy server group.

3. Click **Create Sub-Group**.

   The Create Group page opens.

4. Enter the name of the new sub-group.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

5. Click **Save**.

The sub-group is added to the selected group.

Renaming a Policy Server Group or Sub-group

To rename aa policy server group or sub-group:

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

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

2. From the content tree, select the policy server group or sub-group.

   The Policy Server Administration page opens in the work area.

3. Click **Modify**.

   The Modify Group page opens.

4. Modify the name.

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

5. Click **Save**.

   The group is renamed.

Removing a Policy Server Profile from a Policy Server Group

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

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

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

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

2. From the content tree, select the policy server group or sub-group.

   The Policy Server Administration page opens in the work area, displaying the contents of the selected policy server group or sub-group.

3. Remove the policy server profile using one of the following methods:

   > **Note:**
   >
   > The profile is removed immediately, without a confirmation message.

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

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

Deleting a Policy Server Group

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

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

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

2. From the content tree, select the policy server group or sub-group.

   The Policy Server Administration page opens in the work area, displaying the contents of the selected policy server group or sub-group.

3. On the Policy Server Administration page, click **Delete**.

   A confirmation message displays.

4. Click **OK** to delete the group.

The policy group is deleted.

About Reapplying a Configuration

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

- When the servers of a cluster are replaced, the new servers come up initially with default values. Reapplying the configuration lets you redeploy the entire configuration rather than reconfiguring the server field by field. You should also use the Rediscover Cluster operation to clear the failed status in the Cluster Information Report. See Rediscovering a Cluster for more information.

- After upgrading the software on a server, it is recommended that you reapply the configuration from the CMP system to ensure that the upgraded server and the CMP system are synchronized.
- The server configuration may go out of synchronization with the CMP system (for example, when a break in the network causes communication to fail between the CMP system and the server). If such a condition occurs, the CMP system displays the server status on the **System** with a message that there is a configuration mismatch. You can click the notice to display a report comparing the server configuration with the CMP database information. Reapplying the configuration brings the server back into synchronization with the CMP database.

CMP provides the following methods for reapplying a configuration:

- Reapplying the Configuration to a Single Device
- Reapplying the Configuration to a Group of Devices

If your system is configured with **Manager is NW-CMP** enabled, to reapply a configuration, see:

- #unique_239
- #unique_240

Reapplying the Configuration to a Single Device

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

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.

   The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. From the content tree, select the device.

   The Policy Server Administration page opens to the **System** tab, displaying information for that device.
3. Click **Reapply Configuration**.

The device is synchronized with the CMP system.

Reapplying the Configuration to a Group of Devices

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

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.

   The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. From the content tree, select the group.

   The appropriate Administration page opens in the work area.
3. From the **Operations** menu, select **Reapply Config**.

   The Bulk Reapply Config dialog displays stating the number of agents affected.

4. Specify the delay time (in seconds) for applying the operation to each server in the group.

   The number of seconds is 0 to 60. 0 is the default.

5. Click **Reapply Config** to reapply the configuration.

   An in-progress message appears. After the action completes, a message stating the reapply was successful with a list of the affected devices appears.

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

Rediscovering a Cluster

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

To rediscover a cluster:

1. From the appropriate section of the navigation pane (for example, **Policy Server** or **MRA**), select **Configuration**.

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

2. From the content tree, select the server or cluster.

   The corresponding administration page opens in the work area.

3. Click the **Reports** tab.

   The **Reports** tab opens.

4. Click **Rediscover Cluster**.

   The Cluster Information Report is updated.

The cluster is rediscovered.

Resetting Counters

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

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

1. From the **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.

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

2. From the content tree, select the group that contains the servers of interest.

   The Policy Server Administration page opens in the work area.

3. From the **Operations** list, select **Reset Counters**.

   The Bulk Reset Counters dialog displays showing the number of servers affected.

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

The counters are reset.

Enabling or Disabling All Sh Connections

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

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

To manually disable or enable all Sh connections:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the group that contains the servers.

   The Policy Server Administration page opens in the work area.
3. From the **Operations** menu, select **Enable Sh** or **Disable Sh**.

   The Bulk Enable Sh or Bulk Disable Sh dialog displays stating the number of servers affected.
4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.
5. Click **Enable Sh** or **Disable Sh** to perform the action.

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

Checking the Status of an MPE Server

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

Group View
Select **ALL** from the policy server content tree to view all the defined MPE servers, or select a specific policy server group or sub-group to view just the servers associated with that group. The display in the work area includes a status column that indicates the following states:

- **On-line**

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

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

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

- **Out of Service**

  Communication to the cluster has been lost.
- **No Data**

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

  The MPE device configuration does not match the CMP database.
- **Pending Apply**

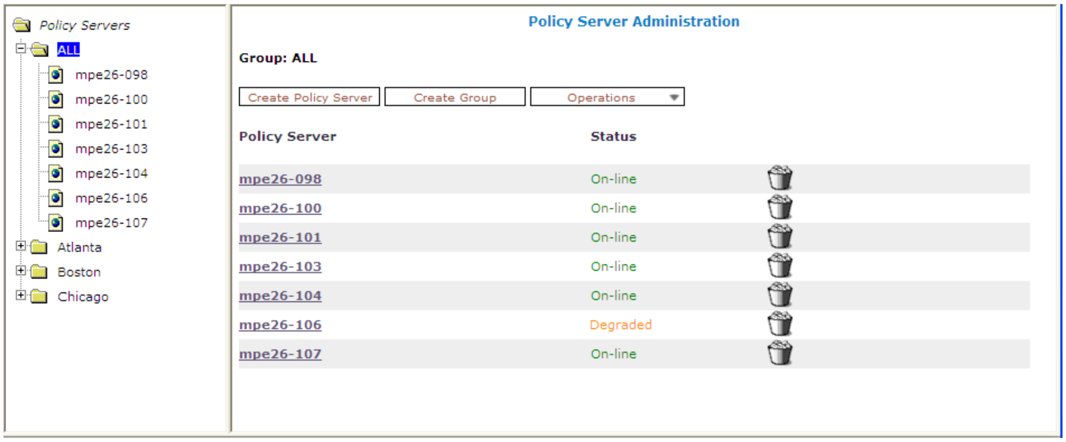
  With **Manager is NW-CMP** enabled, when the NW-CMP pushes configuration changes down to On-line MPE, MRA, or S-CMP devices, the devices have the **Pending Apply** status indicating that the devices have not received the configuration changes.
- **Applying**

  With **Manager is NW-CMP** enabled, when the NW-CMP pushes configuration changes down to On-line MPE, MRA, or S-CMP devices, the devices have the **Applying** status indicating that the devices are receiving the configuration changes.

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

Policy Server Group View
Select a group from the content tree to view the current operating status of the servers in the group.
Figure 3-3 shows an example of a Group View in which one of the servers is degraded.

Figure 3-3 Group View



Policy Server Administration

Group: ALL

Policy Server	Status
mpe26-098	On-line
mpe26-100	On-line
mpe26-101	On-line
mpe26-103	On-line
mpe26-104	On-line
mpe26-106	Degraded
mpe26-107	On-line

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

Policy Server Reports

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

Report pages provide the following information:

Mode
Shows whether data collection is currently Active or Paused, Absolute (displaying statistics since the last reset) or Delta (displaying changes in the statistics during the last 10-second refresh period).

Buttons
The buttons let you navigate between reports, or control the information displayed within the report. The following list describes the buttons; which buttons are available depends on your configuration and differ from one report page to the next:

> **Show Absolute/Show Deltas**
> Switches between absolute mode (statistics since last reset) and delta mode (statistics since last display).
>
> **Reset Counters**
> Resets counters on the current page back to initial values (except for Session count and Downstream Bandwidth in the Network Elements section).
>
> **Rediscover Cluster**
> Rediscovers the cluster, deleting any failed servers that have been removed from service or refreshing the status of the failed server after reapplying the configuration.
>
> **Pause/Resume**
> Stops or restarts automatic refreshing of displayed information. The refresh period is 10 seconds.
>
> **Cancel**
> Returns to previous page.

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

Cluster Information Report
Information about the cluster.

Blades
Information about the individual physical components in the cluster.

Time Period
Information about the current time period and transition status.

Policy Statistics
Information about the execution of policy rules.

Quota Profile Statistics
Information about quota profiles.

Traffic Profile Statistics
Information about traffic profiles.

Session Cleanup Statistics
Information about removal of stranded subscriber sessions.

Sy Reconciliation Statistics
Information about the activity of reconciling Sy sessions after a split-brain event between georedundant MPE devices.

Protocol Statistics
Information about the active network protocols.

Latency Statistics
Information about protocol latency.

Event Trigger Statistics
Information about triggered events.

Error Statistics
Information about any errors, arranged by protocol.

Data Source Statistics
Information about LDAP, Sh, Sy, and SPR activity.

KPI Interval Statistics
Information about the configured reporting interval for key performance indicator (KPI) statistics.

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

Viewing the Policy Server Report

The Policy server report shows information for a specific MPE.

To view the Policy Server report:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
2. Expand the **ALL** folder and select an MPE.
3. Click **Reports** tab.

The report page for the selected MPE is displayed.

Cluster Information Report

The Cluster Information Report section displays the following information:

- **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, and one is spare.

  - **Degraded**: One server is active, but at least one other server is not available.
  - **Out-Of-Service**: No server is active.
  - **No Data**: The CMP system cannot reach the server.
- **Site Preference**
  The preference of the cluster (Normal or Reversed). Default status is Normal.

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

- **Overall**
  Displays the current topology state (Active, Standby, Forced-Standby, or Spare), number of server (blade) failures, and total uptime (time providing active or standby policy or GUI service). For the definitions of these states, see Server Status.
- **Utilization**
  Displays the percentage utilization of disk (of the `/var/camiant` file system), average value for the CPU utilization, and memory.

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

Time Period

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

N/A
No time periods are defined, or the cluster has not yet made the transition to any time periods.

Transitioning
The cluster is updating sessions based on the transition of the time period.

Completed
The cluster has updated all affected sessions (either successfully or not) after a time period transition.

Aborted
The transition was stopped by a CMP user.

Incomplete
The transition has not completed, due to a communication failure with an enforcement device.

Cancel
Cancels a transition that is in progress.

Policy Statistics

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

The following statistics are included:

Name
Name of the policy being polled.

Evaluated
Number of times the conditions in the policy were evaluated.

Executed
Number of times policy actions were executed. This implies that the conditions in the policy evaluated to be true.

Ignored
Number of times the policy was ignored. This can happen because the policy conditions refer to data which was not applicable given the context in which it was evaluated.

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

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

Total Execution Time (ms)
The summary of all execution durations, where execution duration is measured starting at the beginning of the policy conditions evaluation until the execution completion.

Maximum Execution time (ms)
The longest execution duration of the policy.

Average Execution time (ms)
The average of all execution durations of the policy.

Processing Time Statistics
The number of policies processed per time range, in milliseconds. Ranges include:

- 0 to 20
- 20 to 40
- 40 to 60
- 60 to 80
- 80 to 100
- 100 to 150
- 150 to 200
- 200 to 250
- greater than 250

Quota Profile Statistics

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

The following statistics are included:

- **Name**
  Name of the quota profiles.
- **Activated**
  Number of times the quota profile was activated.
- **Volume Threshold Reached**

Number of times the quota profile reached its volume threshold.

- **Time Threshold Reached**
  Number of times the quota profile reached its time threshold.
- **Event Threshold Reached**
  Number of times the quota profile reached its event threshold.

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

Traffic Profile Statistics

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

The following statistics are included:

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

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

Session Cleanup Statistics

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

For information on configuring session cleanup, see Configuring Advanced Device Settings.

The following statistics are included:

- **Ready for Cleanup**
  Number of sessions that are stale.
- **Removed on unknown session id**
  Number of sessions removed because the session ID is no longer valid.
- **Reauthorized**
  Number of sessions reauthorized.

- **Reauthorization Timeout**
  Number of sessions for which the reauthorization request timed out.
- **Removed for Expiration**
  Number of sessions removed.

Sy Reconciliation Statistics

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

For information on configuring Sy Reconciliation, see Configuring Advanced Device Settings.

The following statistics are included:

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

Protocol Statistics

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

The summary protocol statistics are the following:

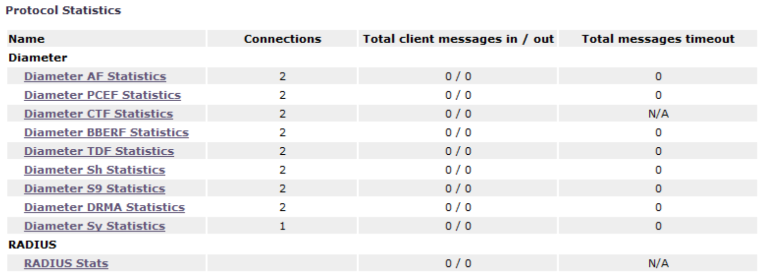
Connections
If the protocol is connection oriented, this value represents the current number of established connections using each protocol.

Total client messages in / out
The total number of incoming and outgoing messages received and sent using each protocol.

Total messages timeout
The total number of incoming and outgoing messages that timed out using each protocol.

Figure 3-4 shows a sample.

Figure 3-4   Sample Protocol Statistics



Protocol Statistics

Name	Connections	Total client messages in / out	Total messages timeout
Diameter			
Diameter AF Statistics	2	0 / 0	0
Diameter PCEF Statistics	2	0 / 0	0
Diameter CTF Statistics	2	0 / 0	N/A
Diameter BBERF Statistics	2	0 / 0	0
Diameter TDF Statistics	2	0 / 0	0
Diameter Sh Statistics	2	0 / 0	0
Diameter S9 Statistics	2	0 / 0	0
Diameter DRMA Statistics	2	0 / 0	0
Diameter Sy Statistics	1	0 / 0	0
RADIUS			
RADIUS Stats		0 / 0	N/A

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

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

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

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

For example, the DRMA statistics include the following:

RUR_SEND_COUNT
The number of RUR messages sent.

RUR_RECV_COUNT
The number of RUR messages received.

RUA_SEND_SUCCESS_COUNT
The number of RUA success messages sent.

RUA_RECV_SUCCESS_COUNT
The number of RUA success messages received.

RUA_SEND_FAILURE_COUNT
The number of RUA failure messages sent.

RUA_RECV_FAILURE_COUNT
The number of RUA failure messages received.

LNR_SEND_COUNT
The number of LNR messages sent.

LNR_RECV_COUNT
The number of LNR messages received.

LNA_SEND_SUCCESS_COUNT
The number of LNA success messages sent.

LNA_RECV_SUCCESS_COUNT
The number of LNA success messages received.

LNA_SEND_FAILURE_COUNT
The number of LNA failure messages sent.

LNA_RECV_FAILURE_COUNT
The number of LNA failure messages received.

LSR_SEND_COUNT
The number of LSR messages sent.

LSR_RECV_COUNT
The number of LSR messages received.

LSA_SEND_SUCCESS_COUNT
The number of LSA success messages sent.

LSA_RECV_SUCCESS_COUNT
The number of LSA success messages received.

LSA_SEND_FAILURE_COUNT
The number of LSA failure messages sent.

LSA_RECV_FAILURE_COUNT
The number of LSA failure messages received.

Latency Statistics

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

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

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

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

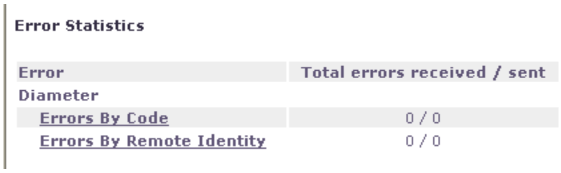
The Event Trigger Statistics section summarizes any event triggers reported by the MPE device. This is presented as a table of overall statistics for event triggers by code and event triggers by application.

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 3-5 shows a sample.

Figure 3-5 Sample Error Statistics



Error Statistics

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

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. See Errors by Code and Errors by Remote Identity for details.

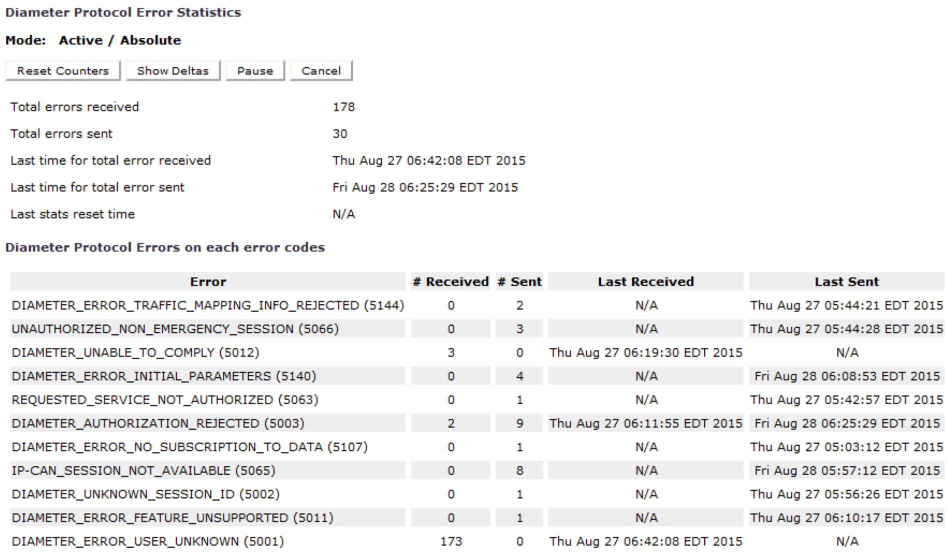
Errors by Code

The Error by Code detailed report displays the following information:

- Total errors received
- Total errors sent
- Last time for total error received (day, date, and time)
- Last time for total error sent (day, date, and time)
- Last stats reset time (day, date, and time)
- Lists Diameter Protocol Errors by error codes (error code, # received, # sent, last received, last sent)

Figure 3-6shows a sample.

Figure 3-6 Diameter Protocol Error Statistics



Diameter Protocol Error Statistics

Mode: Active / Absolute

Total errors received	178
Total errors sent	30
Last time for total error received	Thu Aug 27 06:42:08 EDT 2015
Last time for total error sent	Fri Aug 28 06:25:29 EDT 2015
Last stats reset time	N/A

Diameter Protocol Errors on each error codes

Error	# Received	# Sent	Last Received	Last Sent
DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED (5144)	0	2	N/A	Thu Aug 27 05:44:21 EDT 2015
UNAUTHORIZED_NON_EMERGENCY_SESSION (5066)	0	3	N/A	Thu Aug 27 05:44:28 EDT 2015
DIAMETER_UNABLE_TO_COMPLY (5012)	3	0	Thu Aug 27 06:19:30 EDT 2015	N/A
DIAMETER_ERROR_INITIAL_PARAMETERS (5140)	0	4	N/A	Fri Aug 28 06:08:53 EDT 2015
REQUESTED_SERVICE_NOT_AUTHORIZED (5063)	0	1	N/A	Thu Aug 27 05:42:57 EDT 2015
DIAMETER_AUTHORIZATION_REJECTED (5003)	2	9	Thu Aug 27 06:11:55 EDT 2015	Fri Aug 28 06:25:29 EDT 2015
DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107)	0	1	N/A	Thu Aug 27 05:03:12 EDT 2015
IP-CAN_SESSION_NOT_AVAILABLE (5065)	0	8	N/A	Fri Aug 28 05:57:12 EDT 2015
DIAMETER_UNKNOWN_SESSION_ID (5002)	0	1	N/A	Thu Aug 27 05:56:26 EDT 2015
DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011)	0	1	N/A	Thu Aug 27 06:10:17 EDT 2015
DIAMETER_ERROR_USER_UNKNOWN (5001)	173	0	Thu Aug 27 06:42:08 EDT 2015	N/A

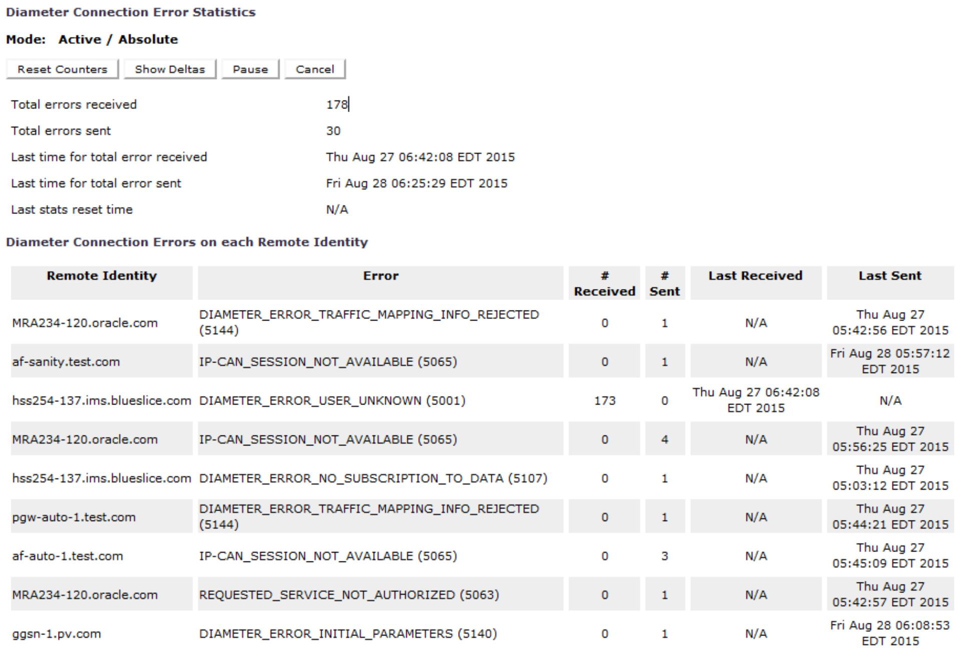
Errors by Remote Identity

The Error by Remote Identity detailed report displays the following information:

- Total errors received
- Total errors sent
- Last time for total error received (day, date, and time)
- Last time for total error sent (day, date, and time)
- Last stats reset time (day, date, and time)
- Lists Diameter Protocol Errors by each remote identity (remote identity, error code, # received, # sent, last received, last sent)

Figure 3-7 shows a sample.

Figure 3-7   Error Statistics by Remote Identity



Diameter Connection Error Statistics

Mode: Active / Absolute

Total errors received	178
Total errors sent	30
Last time for total error received	Thu Aug 27 06:42:08 EDT 2015
Last time for total error sent	Fri Aug 28 06:25:29 EDT 2015
Last stats reset time	N/A

Diameter Connection Errors on each Remote Identity

Remote Identity	Error	# Received	# Sent	Last Received	Last Sent
MRA234-120.oracle.com	DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED (5144)	0	1	N/A	Thu Aug 27 05:42:56 EDT 2015
af-sanity.test.com	IP-CAN_SESSION_NOT_AVAILABLE (5065)	0	1	N/A	Fri Aug 28 05:57:12 EDT 2015
hss254-137.ims.blueslice.com	DIAMETER_ERROR_USER_UNKNOWN (5001)	173	0	Thu Aug 27 06:42:08 EDT 2015	N/A
MRA234-120.oracle.com	IP-CAN_SESSION_NOT_AVAILABLE (5065)	0	4	N/A	Thu Aug 27 05:56:25 EDT 2015
hss254-137.ims.blueslice.com	DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA (5107)	0	1	N/A	Thu Aug 27 05:03:12 EDT 2015
pgw-auto-1.test.com	DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED (5144)	0	1	N/A	Thu Aug 27 05:44:21 EDT 2015
af-auto-1.test.com	IP-CAN_SESSION_NOT_AVAILABLE (5065)	0	3	N/A	Thu Aug 27 05:45:09 EDT 2015
MRA234-120.oracle.com	REQUESTED_SERVICE_NOT_AUTHORIZED (5063)	0	1	N/A	Thu Aug 27 05:42:57 EDT 2015
ggsn-1.pv.com	DIAMETER_ERROR_INITIAL_PARAMETERS (5140)	0	1	N/A	Fri Aug 28 06:08:53 EDT 2015

Data Source Statistics

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

LDAP Statistics

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

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

- **Average time spent on successful updates (ms)**
- **Average time spent on unsuccessful updates (ms)**

Sh Statistics

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

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

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

Sy Statistics

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

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

SPR Statistics

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

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

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

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 maximum MPE transactions per second for the previous interval.

Interval MaxSessionCount
The highest value of the counter MaxSessionCount during the previous interval.

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

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

Cancel
Returns to the previous page.

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

Viewing Policy Server Logs

The log files trace the activity of a Policy Management device. You can view and configure the logs for an individual cluster.
To view the log:

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

   The content tree displays a list of policy server groups.
2. From the content tree, select the Policy Management device.

   The Policy Server Administration page opens in the work area.
3. Select the **Logs** tab.

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

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

Viewing the Trace Log

The trace log records Policy Management application notifications, such as protocol messages, policy messages, and custom messages generated by policy actions, for individual servers. Trace logs are not replicated between servers in a cluster, but they persist after

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

To view the Trace log:

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

   The content tree displays a list of groups; the initial group is **ALL**.
2. From the content tree, select the device.

   The appropriate Administration page opens in the work area.
3. On the Administration page, select the **Logs** tab.

   Log information for the selected device is displayed.
4. Click **View Trace Log**.

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

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

- **Severity**
  Filter by severity level. Events with the selected severity and higher are displayed. For example, if the severity selected is **Warning**, the trace log displays events with the severity level `Warning` and higher.
- **Contains**
  Enter a text string to search for. For example, if you enter `connection`, all events containing the word `connection` display.

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

6. After entering the filtering information, click **Search**.

   The selected events are displayed. By default, the window displays 25 events per page.
7. To change the number of events per page, select a value from the **Display results per page** list.

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

   > **Note:**
   >
   > Events that occur after the Trace Log Viewer starts are not visible until you refresh the display.
8. To refresh the display, click any of the following:
   - **Show Most Recent**
     Applies filter settings and refreshes the display. This displays the most recent log entries that fit the filtering criteria.
   - **Next/Prev**
     When the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.
   - **First/Last**
     When the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.
9. Click **Close**.

   The trace log window closes.

Syslog Support

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

> **Note:**
>
> These logs are separate from the TPD syslogs.

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

Viewing the Trace Log

The trace log records Policy Management application notifications, such as protocol messages, policy messages, and custom messages generated by policy actions, for individual servers. Trace logs are not replicated between servers in a cluster, but they persist after failovers. You can use the trace log to debug problems by tracing through application-level messages.
The activity of the Policy Rules Engine is recorded in a trace log at eight levels: Emergency (ID 4560), Alert (ID 4561), Critical (ID 4562), Error (ID 4563), Warning (ID 4564), Notice (ID 4565) Info (ID 4566), and Debug (ID 4567). You can configure the severity level of messages that are recorded in the trace log.

To view the Trace log:

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

   The content tree displays a list of groups; the initial group is **ALL**.
2. From the content tree, select the device.

   The appropriate Administration page opens in the work area.
3. On the Administration page, select the **Logs** tab.

   Log information for the selected device is displayed.
4. Click **View Trace Log**.

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

   When the Trace Log Viewer window opens in a new browser window, all events contain the following information:
   - **Date/Time**
     Event timestamp. This time is relative to the server time.
   - **Code**
     The event code or ID number. For information about event codes and messages, see the *Troubleshooting Reference*.
   - **Severity**
     Severity level of the event. Application-level trace log entries are not logged at a higher level than Error.
   - **Message**
     The message associated with the event. If additional information is available, the event entry shows as a link. Click the link to see additional detail in the frame below.
5. Filter the events displayed using the following:

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

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

6. After entering the filtering information, click **Search**.

   The selected events are displayed. By default, the window displays 25 events per page.
7. To change the number of events per page, select a value from the **Display results per page** list.

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

   > **Note:**
   >
   > Events that occur after the Trace Log Viewer starts are not visible until you refresh the display.
8. To refresh the display, click any of the following:
   - **Show Most Recent**
     Applies filter settings and refreshes the display. This displays the most recent log entries that fit the filtering criteria.
   - **Next/Prev**
     When the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.
   - **First/Last**

When the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.

9. Click **Close**.

   The trace log window closes.

Syslog Support

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

> **Note:**
>
> These logs are separate from the TPD syslogs.

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

The SMS Log

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

The SMPP Log

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

The SMTP Log

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

The HTTP Log

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

Configuring Log Settings for Servers in a Cluster

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

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

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

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

   The Policy Server Administration page opens in the work area.

3. Select an MPE device from the list.

   The Policy Server Administration page opens in the work area and details the configuration settings of the selected device.

4. Select the **Logs** tab.

   The Policy Server Administration page opens and details the logs configuration settings for the specified device.

5. To edit the logs configuration settings, click **Modify**.

   The editable fields open in the work area.

6. In the **Modify Trace Log Settings** section of the page, select the **Trace Log Level** from the list.

   This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164 *The BSD syslog Protocol*. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:

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

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

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

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

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

8. In the **Modify CMPP Log Settings** section of the page configure the **CMPP Log Level**.

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

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

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

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

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

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

Valid levels are:

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

b. **SMPP Log Forwarding IP Addresses**—Enter addresses for forwarding. You can forward SMPP log entries to multiple syslog servers.

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

    This setting indicates the minimum severity of messages that are recorded in the SMTP log. These severity levels correspond to the syslog message severities from RFC 3164 *The BSD syslog Protocol*. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the SMTP log. The levels are:

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

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

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

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

12. Click **Save**.

The log settings are configured.

Analytics Data Stream

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

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

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

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

The ADS feature is configured from the Mode Settings page. See CMP Modes for information on configuring the ADS feature.

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

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

4 Configuring Protocol Routing

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

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

Configuring Diameter Peers

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

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

1. Either in the **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.

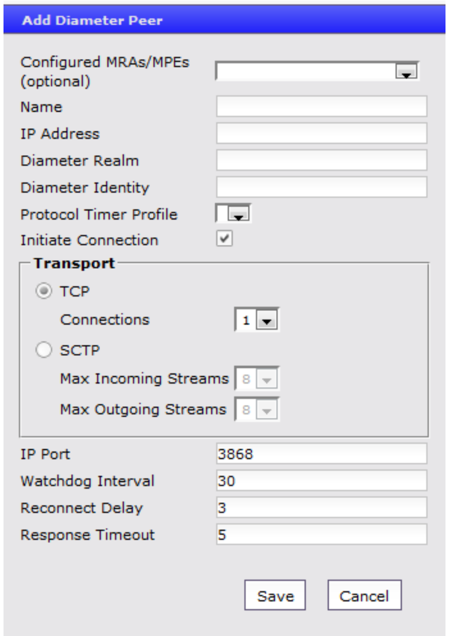
   The content tree displays a list of policy server or MRA groups.
2. From the content tree, select the MPE or MRA device.

   The Administration page for that device opens in the work area.
3. Select the **Diameter Routing** tab.

   The Diameter Routing configuration settings appear.
4. Click **Modify Peers** which opens the Modify the Diameter Peer Table.
5. Add a peer to the table using these steps.
   a. Click **Add**.

      The Add Diameter Peer window opens.

Figure 4-1   Add Diameter Peer



Add Diameter Peer

Configured MRAs/MPEs (optional)	
Name	
IP Address	
Diameter Realm	
Diameter Identity	
Protocol Timer Profile	
Initiate Connection	☑

Transport

● TCP	
Connections	1
○ SCTP	
Max Incoming Streams	8
Max Outgoing Streams	8

IP Port	3868
Watchdog Interval	30
Reconnect Delay	3
Response Timeout	5

b. Enter the following:

- **Configured MRAs/MPEs (optional)**
  If you are defining an existing Policy Management cluster as a Diameter peer, select it from this list; the other fields are populated.
- **Name** (required)
  Name of the peer device (which must be unique within the CMP database).
- **IP Address** (required)
  IP address in IPv4 or IPv6 format of the peer device.

  If not specified, the MPE device uses a DNS lookup to resolve the value in the Diameter Identity field into an IP address and try to connect.
- **Diameter Realm** (required)
  The domain of responsibility for the peer (for example, `Example.com`).
- **Diameter Identity** (required)
  Fully qualified domain name (FQDN) of the peer device (for example, `mpe33.Example.com`).
- **Protocol Timer Profie**
  Select from the list.
- **Initiate Connection**
  Select to initiate an S9 connection for this Diameter peer.
- **Transport**
  Select either **TCP** or **SCTP** (shown as Transport Info in the Diameter peer table). For TCP select **Connections** (range 1 through 8, default 1). For SCTP select **Max Incoming Streams** and **Max Outgoing Streams**(1 to 8 connections, default is 8) which will be shown as Connection Info in the Diameter peer table.
- **IP Port**
  Enter the IP Port number.
- **Watchdog Interval**
  Enter the watchdog interval in seconds. The default is 6 seconds.

- **Reconnect Delay**
  Enter the response time in seconds. The default is 3 seconds.
- **Response Timeout**
  Enter the response timeout interval is seconds. The default is 5 seconds.

c. Click **Save**.

6. Complete these steps to add, edit or delete additional Diameter Peers.
   - Cloning an entry in the table
     a. Select an entry in the table.
     b. Click **Clone**. The Clone window opens with the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is added to the table.
   - Editing an entry in the table
     a. Select the entry in the table.
     b. Click **Edit**. The Edit Response window opens, displaying the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     a. Select the entry in the table.
     b. Click **Delete**. A confirmation message displays.
     c. Click **Delete** to remove the entry. The entry is removed from the table.
7. Click **Save**.

Configuring Diameter Realm Based Peer Routes

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

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

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

To configure the Diameter realm based peer routes:

1. From the Policy Management device (either **Policy Server** or **MRA** section of the navigation pane, select **Configuration**.

   The content tree displays a list of policy server groups.
2. From the content tree, select the **Policy Server** or **MRA** that needs diameter routing.

The Policy Server Administration or MRA Administration page opens in the work area.

3. Select the **Diameter Routing** tab.

   The Diameter Routing configuration settings display.

4. Click **Modify Routes**.

   The Modify the Diameter Route Table page opens.

5. Add a route to the table

   a. Click **Add**.

      The Add Diameter Route (Realm Based Route) window opens.

   b. Configure the route using the following fields.

      - **Diameter Realm**
        For example, `Example.com`.

      - **Application ID**
        Select **Rx** (default), **Gq**, **Ty**, **Gx**, **Gxx**, **Sd**, **Sy**, **Gy**, **S9**, **Vzr**, or **All**.

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

      - **User ID type**
        Select **ANY** (default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.

      - **Value**
        Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use a period followed by an asterisk (.*) as a wildcard character. To add the user ID to the list, click **Add**; to remove one or more user IDs from the list, select them and click **Delete**.

      - **Evaluate as Regular Expression**
        The check box allows the matching of route criteria using regular expression syntax, opposed to the previously supported matching wildcards. Regular expressions must be Java expressions; using any other language expression will result in a failed status

        See Examples of Java Regular Expressions for MRA Routes for more information about using regular expressions for MRA routes.

      - **Action**
        Select **PROXY** (stateful route, default), **RELAY** (stateless route), or **LOCAL** (process on this device).

      - **Server ID**
        Select a destination peer from the list.

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

   c. Click **Save**.

6. (Optional) Add, delete, modify, or order entries.
   - Cloning an entry in the table
     1. Select an entry in the table.
     2. Click **Clone**. The Clone window opens with the information for the entry.
     3. Make changes as required.
     4. Click **Save**. The entry is added to the table.
   - Editing an entry in the table
     1. Select the entry in the table.
     2. Click **Edit**. The Edit Response window opens, displaying the information for the entry.
     3. Make changes as required.
     4. Click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     1. Select the entry in the table.
     2. Click **Delete**. A confirmation message displays.
     3. Click **Delete** to remove the entry. The entry is removed from the table.
   - Ordering the list.
     If you define multiple entries, they are searched in the order displayed in this list. To change the order:
     1. Select an entry.
     2. Click **Up** or **Down**. The search order is changed.
7. Define the default route:
   1. Click **Edit** in the **Default Route** section.
   2. Select the default action: **PROXY**, **RELAY**, or **LOCAL**.
   3. Select the peer server ID.
   4. Click **Save**.
8. To delete the default route, click **Delete**.
9. Click **Save**.

The Diameter realm based peer routes are configured.

Examples of Java Regular Expressions for MRA Routes

The following sample regular expressions are for MRA Routes.

- For E164 numbers ending in 00 to 24: `#E164:1234.*?(?:0\d|1\d|2[0-4])`
- For E164 numbers ending in 25 to 49: `#E164:1234.*?(?:2[5-9]|3\d|4\d)`
- For E164 numbers ending in 50 to 74: `#E164:1234.*?(?:5\d|6\d|7[0-4])`
- For E164 numbers ending in 75 to 99: `#E164:1234.*?(?:7[5-9]|8\d|9\d)`

Loading MPE/MRA Configuration Data when Adding Diameter Peer

When adding a diameter peer, select a peer from the list on the **Diameter Routing** tab. After the peer is selected, the peer configuration fields are automatically populated.

5

Configuring Advanced Device Settings

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

Configuring Expert Settings for an MPE

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.
To configure Expert Settings:

1. To view the device list, 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 device and and select the **Policy Server** tab.

   The configuration settings for the device display.

3. Click **Advanced**.

   The advanced settings for the device display:

   - **Expert Settings**
   - **Service Overrides**
   - **MPE Load Shedding Configuration** (Level 1 to Level 4)

4. Click **Modify**.

   The advanced configuration settings can be edited.

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

   The Edit Expert Setting Value dialog opens.

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

   See Expert Settings for MPE for information about the configurations keys.

7. Click **Save**.

The settings are applied to the selected device.

Expert Settings for MPE

Table 5-1 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

Table 5-1 (Cont.) Expert Settings for MPE

Category	Configuration Key	Description	Default
Database	DB.User.EnableBillingStartDate	Enables the use of the billing date effective name from the profile for the subscriber. This is used as a start date for the plan and is also used to calculate the next reset time.	true
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 to 58060800.	86400 (1 day)
Diameter	DIAMETER.AF.MinAuthLifetime	The minimum lifetime of an AF session. Otherwise the corresponding AF session would be purged subject to the configured grace period. Specified in seconds.	300
Diameter	DIAMETER.AF. 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 AF session can be considered stale and purged. Specified in seconds. Valid range is 0 to 86400.	86400 (1 day)
Diameter	DIAMETER.AF.SignallingSessionAuthLifetime	Indicates the maximum configured period for an Rx sessions containing signaling flow past which the session is considered stale. Specified in seconds. Valid range is 300 to 58060800.	259200 (3 days)
Diameter	DIAMETER.AppsToEvaluateOnTermination	Indicates applications for which policy evaluation is triggered when a terminate request is received. Specified as a comma-separated string containing the names of the applications for which policy engine should evaluate termination requests. DIAMETER. Valid values are: • Gx • Rx • Sd • S9 PolicyExecutionOnSessionTermination must be set to false to use this configuration.	null

Table 5-1 (Cont.) Expert Settings for MPE

Category	Configuration Key	Description	Default
Diameter	DIAMETER.Cleanup.AuditRxSessions	If enabled, an RAR message is sent for auditing. **Note:** This is for future releases and has not been implemented yet.	False
Diameter	DIAMETER.Cleanup.AuditSySessions	If enabled, an SLR (INTERMEDIATE) message is sent for auditing. If disabled, the Sy session is checked for an association with an IP-CAN session. If there are no IP-CAN associations, the Sy session is considered active; otherwise, the session is deleted. **Note:** This is for future releases and has not been implemented yet.	False

Table 5-1 (Cont.) Expert Settings for MPE

Category	Configuration Key	Description	Default
Diameter	DIAMETER.Cleanup.CleanupStaleRxSessions	Determines if the MPE device should consider AF sessions in the regular cleanup cycles. If enabled, AF sessions are considered expired if they have lived longer than the specified AFSessionValidityTime. **Note:** At that point, in future releases, if AuditAFSessions is set to True, an RAR will be sent for auditing the session.	True
Diameter	DIAMETER.Cleanup.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 (6 hours)
Diameter	DIAMETER.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Valid range is 1 to 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.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. MaxDurationForSessionIteration	The maximum duration in seconds to iterate through the sessions. Valid range is 1 through 86400.	7200 (2 hours)

Table 5-1 (Cont.) Expert Settings for MPE

Category	Configuration Key	Description	Default
Diameter	DIAMETER.Cleanup.MaxSessionCleanupRate	The rate (in sessions/sec) at which the cleanup task attempts to clean stale sessions. Valid range is 1 through 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 through 100000.	1000
Diameter	DIAMETER.Cleanup.MaxSessionValidityTime	The maximum amount of time in seconds after which the session is cleaned up on any error. Valid range is 1 through 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. Valid range is 1 through 8640000.	172800 (2 days)
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-dd*T*hh*:*mm*:*ss*) of when it will first run and then repeat at the interval specified.	undefined
Diameter	DIAMETER.ConnectionTimeOut	Defines the timeout value for the connection.	3
Diameter	DIAMETER.ENF.MaxTimeForAnGwFailure	The maximum time allowed after getting indication for SGW failure in which the MPE device does not send any new or updated policies to the P-GW except rules to be removed. Specified in seconds.	3600
Diameter	DIAMETER.ENF.PickUpAllEventTriggers	If enabled, MPE picks up all event triggers from all used policies. If the value is false (disabled), the MPE picks up event triggers from the last policy used.	False
Diameter	DIAMETER.ENF. ReevaluateGeneratedDefaultRule	If set to True, on receipt of a session update request the MPE device evaluates the flow which contains the generated default rule even when there is no new default-EPS-Bearer-QoS information in the request.	False
Diameter	DIAMETER.ENF. RegisterForAnGwChangeWithSGWRest	If the SGW-Rest supported feature was negotiated and the value of this parameter is false, the MPE device checks if AN_GW_CHANGED event trigger is one of the armed event triggers to be installed and removes it. As a result, the MPE device will not register for AN_GW_CHANGE.	False
Diameter	DIAMETER.EnableSessionCleanUp	Enables the DiameterSessionCleanUp Task.	True

Table 5-1 (Cont.) Expert Settings for MPE

Category	Configuration Key	Description	Default
Diameter	DIAMETER.PCEF.NetLocSupportedAccesses	A combination of values used for network location (NetLoc) support. The format is *IPCanType*:*RATType*:*AN-Trusted*. If not set, any types or values are applicable. For example: `THREEGPP_GPRS` means to support NetLoc as if IPCanType=THREEGPP_GPRS. `NON_THREEGPP_EPS:WLAN:TRUSTED` means to support NetLoc when IPCanType=NON_THREEGPP_EPS, RATType=WLAN, and ANTrusted=TRUSTED. `NON_THREEGPP_EPS::TRUSTED` means to support NetLoc when IPCanType=NON_THREEGPP_EPS and ANTrusted=TRUSTED. `::` means all accesses support NetLoc.	THREEGPP_GPRS, THREEGPP_EPS, NONTHREEGPP_EPS:WLAN:TRUSTED
Diameter	DIAMETER.PolicyExecutionOnSessionTermination	If enabled (True), policy evaluation will be triggered for all applications when a terminate request is received. This configuration must be disabled (False) to use DIAMETER.AppsToEvaluateOnTermination to selectively trigger policy evaluation by application.	True
Diameter	DIAMETER.SessionUniquenessControl	If enabled (True), the MPE cluster will maintain session uniqueness and avoid stale session processing.	False
Diameter	DIAMETER.SessionUniquenessControlWaitTime	If enabled (True), the Max-Wait-Time AVP is used in conjunction with the message origination time stamp to determine staleness of message.	False
KPI	KPI.Capacity.Session		1
KPI	KPI.Capacity.TPS		1
SH	SH.Retry.Enabled	If enabled, indicates that the MPE device retries the Sh Requests for UDR, PUR, and SNR to the backup server when the primary server returns one of the defined error codes. PNA messages are not retried. If the backup server returns an error, then retry is not performed on the primary server.	False

Table 5-1 (Cont.) Expert Settings for MPE

Category	Configuration Key	Description	Default
SH	SH.Retry.EnabledOnTimeout	If enabled with the SH.Retry.Enabled setting, allows the MPE to retry an Sh Request to a backup datasource server when there is a response timeout. If the request to backup server times out, then a retry is not performed on the primary server. This setting depends on the configuration of the SH.Retry.Enabled and SH.ResponseTimeout settings. You can configure the SH.ResponseTimeout in the **Service Overrides** section of the Advanced Settings page.	False
SMPP	SMPP.SendSMSNowWhenDeliveryDateInPast	In SMS:SMPP mode, determines if SMS notifications scheduled to be delivered in the past will be dropped or delivered. If false, SMS notifications scheduled to be delivered on a date in the past will be dropped. If true, SMS notifications scheduled to be delivered on a date in the past will be delivered immediately.	False
SMSXML	SMSXML.SendSMSNowWhenDeliveryDateInPast	In SMS:XML mode, determines if SMS notifications scheduled to be delivered in the past will be dropped or delivered. If false, SMS notifications scheduled to be delivered on a date in the past will be dropped. If true, SMS notifications scheduled to be delivered on a date in the past will be delivered immediately.	False
SY	SY.Reconciliation.Enabled	Determines whether the Sy Reconciliation is activated and an audit of Sy sessions will be executed on a recovery from a split-brain scenario.	False
SY	SY.Reconciliation.HoldTimer	The time in seconds after receipt of a notification of recovery from a split-brain scenario the Sy Reconciliation task will wait before starting.	180
SY	SY.Reconciliation.MaxSessionReconcileRate	The rate (in sessions/sec) at which the tasks will attempt to send Sy SLR Messages to reconcile Sy sessions.	50
SY	SY.SendOriginationTimestamp	If enabled (True), the message origination timestamp will be included as part of the initial SLR Sy message.	False

Configuring Expert Settings for an MRA

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

1. To view the device list, from the **MRA** section of the navigation pane, select **Configuration**.

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

2. From the content tree, select the device and select the **MRA** tab.

   The configuration settings for the device display.

3. Click **Advanced**.

   The advanced settings for the device display:

   - **Expert Settings**
   - **Service Overrides**
   - **MPE Load Shedding Configuration** (Level 1 and Level 2)
   - **MRA Load Shedding Configuration** (Level 1 to Level 4)

4. Click **Modify**.

   The advanced configuration settings become editable.

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

   The Edit Expert Setting Value dialog opens.

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

   See Table 5-2 for information about the configurations keys.

7. Click **Save**.

The settings are applied to the selected device.

Expert Settings for MRA

Table 5-2 Expert Settings for MRA

Category	Configuration Key	Description	Default
Admission	ADMISSION.DIAMETER.RequestProcessingLimit	The maximum amount of time in milliseconds a request can be processed before being dropped, if no answer has been sent.	5000
Diameter	DIAMETERDRA.Cleanup.BindingCleanupInterval	The interval in seconds at which the cleanup task that looks for stale bindings occurs. Valid range is 1 through 8640000.	86400 (1 day)
Diameter	DIAMETERDRA.Cleanup.BindingValidityTime	The amount of time in seconds elapsed until a binding is deemed stale. Valid range is 1 through 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

Table 5-2 (Cont.) Expert Settings for MRA

Category	Configuration Key	Description	Default
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-dd*Thh:*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 stale bindings. Valid range is 1 through 40000.	250
Diameter	DIAMETERDRA.Cleanup.MaxBindingIterationRate	The rate (in bindings/sec) at which the cleanup task iterates through the binding database. Valid range is 1 through 100000.	1000
Diameter	DIAMETERDRA.Cleanup. MaxDurationForBindingIteration	The maximum duration in seconds to iterate through the bindings. Valid range is 1 through 2147483647.	21600 (5 hours)
Diameter	DIAMETERDRA.Cleanup.MaxSessionValidityTime	The maximum amount of time in seconds after which the session is cleaned up on any error. Valid range is 1 through 8640000.	864000 (10 days)
Diameter	DIAMETERDRA.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Valid range is 1 through 8640000.	432000 (5 days)
Diameter	DIAMETERDRA.StaticMigrationModeEnabled	Enables the static to stateful MRA migration mode. While in this mode, static routes are used for MPE selection only.	False
Diameter	DIAMETERDRA.Routing.RemoteDiversion	If enabled, the MRA diverts messages remotely when necessary.	False
Diameter	DIAMETERDRA.Routing.LocalDiversion	If enabled, the MRA diverts messages locally when necessary.	True
Diameter	DIAMETERDRA.Routing.FailedDiversionResult	Determines the Result Code to use when the MRA can not perform local or remote diversion. The format is `VendorID:Code`. If the *VendorID* is not needed, use a value of 0 (zero). The default is DIAMETER_TOO_BUSY.	0:3004
Diameter	DIAMETERDRA.ConnectionTimeOut		3
KPI	KPIMRA.Capacity.Bindings		1
KPI	KPIMRA.Capacity.TPS		1

Configuring Service Overrides

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

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

Make service override changes as follows:

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

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

   The configuration settings for the device display.
3. Click **Advanced**.

   The advanced settings for the device display.
4. Click **Modify**.

   The advanced configuration settings can be edited.
5. Select a configuration key in the Service Overrides table and click **Edit**.
   - Adding a key to the table:
     a. 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 server is undetermined.

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

     c. Click **OK**.

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

- Cloning a key in the table:
  a. Select an existing key in the table.
  b. Click **Clone**.
     The Clone Configuration Key Value window opens with the information for the key.
  c. Make changes as required.
  d. Click **Save**.
- Editing a key in the table:
  a. Select an existing key in the table.
  b. Click **Edit**.
     The Edit Configuration Key Value window opens with the information for the key.
  c. Make changes as required.
  d. Click **Save**.
- Deleting a key from the table:
  a. Select an existing key in the table.
  b. Click **Delete**. A confirmation message displays.
  c. Click **Delete** to remove the key.

6. Click **Save**.

The settings are applied to the selected device.

About Overload Controls

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

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

Local Diversion
Selects an MPE device in the MPE pool to handle a new connection for a subscriber who is bound to a busy MPE device.

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

MPE and MRA devices have configurable levels of congestion (busyness) for handling message overload. An MPE device has four congestion levels (Levels 1–4), and an MRA device has two congestion levels (Level 1 and 2). At each level you can define a default action for the level and create rules to handle specific message types. A level action is an action that is taken if none of the rules configured for the level match a message type. For example, for MPE and MRA Level 1, the default level action is **Accept**, which means to bypass load shedding rules instead of rejecting messages.

> **Note:**
>
> When Local or Remote Diversion is not possible, the default result code is DIAMETER_TOO_BUSY. The NO_CAPACITY result code indicates an MRA server has a binding, but the MPE server it points to is currently overloaded, and the MRA server cannot perform local diversion to handle the request. The default result code is configurable.

An MRA device proactively rejects all messages destined for an overloaded MPE at all congestion levels. For example, if an MPE is configured to reject CCR-U messages at Level 2, the MRA device rejects the CCR-U message with DIAMETER_UNABLE_TO_COMPLY instead of forwarding it to the MPE device.

An MRA device subscribes to its pool of MPE devices for load notifications by issuing an LSR message after connection is established. It also subscribes to MPE devices in the backup MRA pool and to all other MRA devices in its association. MRA devices communicate their status using Load Notification (LNR) messages that include a Diversion-Status AVP to indicate whether that MRA device is available.

The Diversion-Status AVP indicates whether an MRA is available for diverting traffic to its MPEs (Remote Diversion). The diversion status is set to DIVERTABLE if none of the MPE devices in an MPE pool are overloaded. The status is set to NOT_DIVERTABLE if at least one MPE device in the MPE pool is overloaded.

The CMP system supports configuration of MPE load shedding rules on the MRA Advanced Configuration page. When you configure the admission rules for an MRA device to reject messages on behalf of an overloaded MPE, there may still be times when the MPE device responds to a message with DIAMETER_TOO_BUSY. In these cases, before forwarding the answer message, the MRA runs the original request through the MPE admission rules and updates the result code with the result code found in the MPE rules.

Configuring MPE and MRA Load Shedding Rules

Use the **Load Shedding Configuration** section of the Advanced Configuration page to edit, reorder, or add new rules at each level of busyness for a device based on the amount of backlog. To reach a configured level of busyness:

- The backlog of outstanding messages in a node crosses a predefined threshold for the level.
- The backlog has been above the busyness level threshold for a minimum amount of time.

At each level, the device can be configured to take one of the following actions (referred to as rules) until the busyness level clears:

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

Refer to MPE Default Load Shedding Rules and MRA Default Load Shedding Rules for more information on default rules.

Note:

Configuration keys must also be used in configuring load shedding options. Contact My Oracle Support for assistance.

Configure the load shedding rules as follows:

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

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

   The configuration settings for the device display.
3. Click **Advanced**.

   The advanced settings for the device display.
4. Click **Modify**.

   The advanced configuration settings can be edited.
5. In the **Load Shedding Configuration** section of the page, select the enabled state.
   - **true** (default)
     Enables load shedding.
   - **false**
     Disables load shedding.
   - **undefined**
     The value for this field is taken from the associated Configuration Template. If there is not a configuration template associated, then the default value is used.
6. Set the Level Action for a busyness level.

   This step is optional. The default Level Action of Accept applies to all levels except MPE Level 4 and MRA Level 2, which has a default Level Action of Drop.

   a. Click ▶ (right arrow) next to the level to expand the level.

   b. Select one of the following default Level Actions:
      - **Accept** all messages.
      - **Drop** all messages.
      - Reject all messages and **Answer with** (select a code from the drop-down list).
      - Reject all messages and **Answer With Code** (enter a code) and **Vendor ID** (enter a vendor ID).
7. Configure the rules for the busyness levels:

   a. Click ▶ (right arrow) next to the level to expand the level.

b. Click **Add** and select the category.

   The Add Load Shedding Rule dialog appears.

c. Enter the values for the load shedding rule:

   - **Name**
     Name of the rule. The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). It cannot begin or end with a hyphen or period, and any labels must be separated by periods.
   - **Application**
     Select the application the rule applies to. You can select **Drma**, **Gx**, **Gxx**, **S9**, **Rx**, **Sh**, or **Sy**.
   - **Message**
     Type of message the rule applies to (which depends on the application chosen).
   - **Request Types** (available only when the CCR message type is selected)
     Select the Request-Type attribute-value pairs (AVPs) that the message must contain. You can select **Initial**, **Update**, and/or **Terminate**.
   - **APNs**
     Enter a CSV list of one or more access point names that the message must contain.
   - **DRMP** (availability dependent on selected application and message type)
     Enter a CSV list of one or more diameter routing message priority codes that the message must contain. The valid range of values is 0 to 15.
   - **Both MPS ID and Reservation Priority Exist** (available only when the AAR message type is selected)
     Determines whether or not to check for the existence of the MPS-Identifier and Reservation-Priority AVPs.

d. Click **OK**.

   The rule is displayed in the table.

8. After a rule is defined, you can clone, edit, or delete it by selecting the rule and clicking the appropriate button.

The settings are applied to the selected device.

MPE Default Load Shedding Rules

You can configure load shedding rules to determine how a device reacts to a processing backlog. This state is called busyness. Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MPE has four busyness levels. With each successive level, the device becomes more aggressive in rejecting or discarding messages in an attempt to prevent the main queue from becoming full. At any level of busyness, requests that have been queued longer than a configurable time are discarded without further processing, since the originator would have abandoned that request.

On the MPE Advanced Configuration page, there is a default action for each Busyness Level. The default level action for levels 1, 2, and 3 is Accept, which means to process the message by bypassing load shedding rules. Level actions are configurable.

The following tables show the default load-shedding rules for an MPE. For configuration information, see the task Configuring MPE and MRA Load Shedding Rules.

Note:

The default rules shown in your system may differ than those listed here depending on how your system is configured.

Table 5-3 MPE Busyness Level 1

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule4	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule14	Accept Gx CCR messages with DRMP priority 0

Table 5-4 MPE Busyness Level 2

Rule Name	Actions
DefaultRule2	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule5	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule7	Reject Rx AAR messages with DIAMETER_TOO_BUSY
DefaultRule15	Accept Gx CCR messages with a DRMP value of 0
DefaultRule17	Accept Rx AAR messages with both the MPS-Identifier and Reservation-Priority AVPs present

Table 5-5 MPE Busyness Level 3

Rule Name	Actions
DefaultRule3	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule6	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule8	Reject Rx AAR messages with DIAMETER_TOO_BUSY
DefaultRule9	Reject Sh PNR messages with DIAMETER_TOO_BUSY
DefaultRule10	Reject Sy SNR messages with DIAMETER_TOO_BUSY
DefaultRule16	Accept Gx CCR messages with a DRMP value of 0
DefaultRule18	Accept RX AAR messages with both the MPS-Identifier and Reservation-Priority AVPs present

Table 5-6 MPE Busyness Level 4

Rule Name	Actions
DefaultRule11	Accept Drma LNR with ACCEPT
DefaultRule12	Accept Drma LSR with ACCEPT
DefaultRule13	Accept Drma RUR with ACCEPT

MRA Default Load Shedding Rules

You can configure load shedding rules to determine how a device reacts to a processing backlog. This state is called busyness. Levels of busyness can be configured to accept, reject, or drop select messages at each level. An MRA has two busyness levels. At each level of busyness, requests that have been queued longer than a configurable time are discarded without further processing, since the originator would have abandoned that request.

On the MRA Advanced Configuration page, there is a default action for each Busyness Level. The default level action is Accept for Level 1, which means to process the message by bypassing load shedding rules. Level actions are configurable.

The following tables show the default load-shedding rules for an MRA. For configuration information, see Configuring MPE and MRA Load Shedding Rules for more information.

> **Note:**
>
> The default rules shown in your system may differ than those listed here depending on how your system is configured.

Table 5-7 MRA Busyness Level 1

Rule Name	Actions
DefaultRule1	Reject Gx CCR messages with DIAMETER_TOO_BUSY
DefaultRule2	Reject Gxx CCR messages with DIAMETER_TOO_BUSY
DefaultRule6	Accept Gx CCR messages with DRMP priority 0

Table 5-8 MRA Busyness Level 2

Rule Name	Actions
DefaultRule3	Accept Drma LNR with ACCEPT
DefaultRule4	Accept Drma LSR with ACCEPT
DefaultRule5	Accept Drma RUR with ACCEPT

Resetting Configuration Keys to Defaults

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

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

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

   The configuration settings for the device display.
3. Click **Advanced**.

   The advanced settings for the device display.
4. Click **Modify**.

   The advanced configuration settings can be edited.

5. Click **Set to Default**.

   A confirmation message displays.

6. Click **OK**.

All the configuration keys for Expert Settings are set to default values.

Filtering the Configuration Keys

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

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

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

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

   The configuration settings for the device display.

3. Click **Advanced**.

   The advanced settings for the device display.

4. (Optional) Click **Modify**.

   The advanced configuration settings can be edited.

5. Click **Filters** to open the filtering popup.

   The filtering popup opens.

6. Specify the filtering parameters using any of the following fields.

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

7. Click **Filter Result**.

   The filtered list of configuration keys displays.

Exporting the Configuration Keys

The Expert Settings or Service Overrides configuration keys can be exported to a comma separated values (CSV) file or to a printable format in a new browser window.
To export the configuration key table:

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

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

   The configuration settings for the device display.
3. Click **Advanced**.

   The advanced settings for the device display.
4. Click **Export**.

   The export list opens.
5. Select the export type.

Option	Description
Save as CSV	A comma-separated value (CSV) file named `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.

6

Configuring Debug Logs

This chapter describes how to configure class-level logging options. Debug logs can be configured at the System Administration level or at the Policy Management device (MPE or MRA) level.

About Debug Logs

Use the CMP server to modify the configuration for each target component on a Policy Management (MPE or MRA) device.

To aid in troubleshooting, you can enable component-specific level logging for the following components:

Tomcat
`logback-tomcat.log`

RC
`logback-rc.xml`

MRA
`logback-mra.xml`

SMSR
`logback-tomcat-rc.xml`

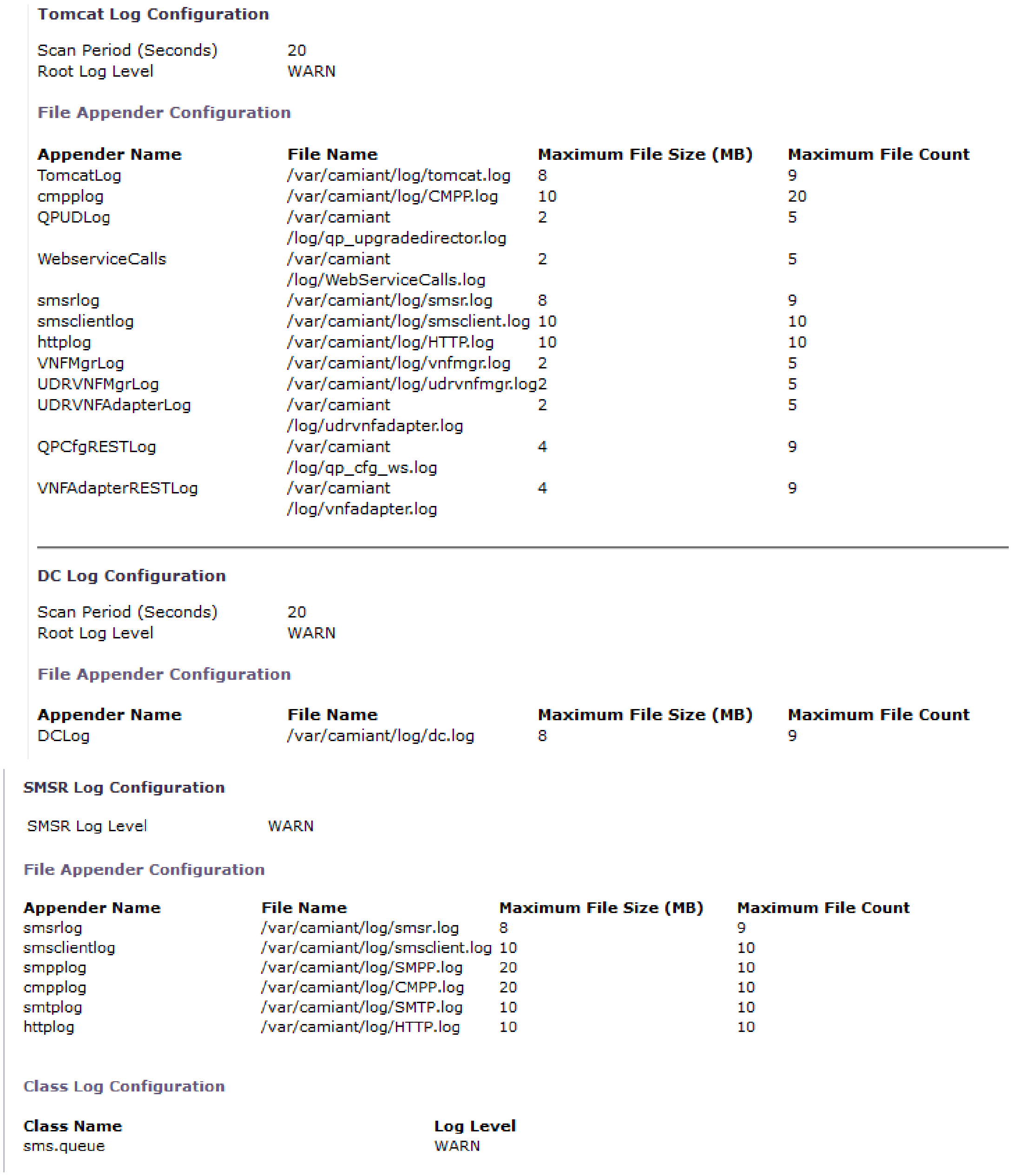
> **Note:**
>
> See Configuring the Manager Logfor details about configuring the default values for debug logs.

About MPE Debug Logs

Debugs logs for the MPE include log configuration for the following components:

- Tomcat Log
- RC Log
- SMSR (SMS Relay)
- DC Log

Figure 6-1   MPE Debug Logs



Tomcat Log Configuration

Scan Period (Seconds)	20
Root Log Level	WARN

File Appender Configuration

Appender Name	File Name	Maximum File Size (MB)	Maximum File Count
TomcatLog	/var/camiant/log/tomcat.log	8	9
cmpplog	/var/camiant/log/CMPP.log	10	20
QPUDLog	/var/camiant/log/qp_upgradedirector.log	2	5
WebserviceCalls	/var/camiant/log/WebServiceCalls.log	2	5
smsrlog	/var/camiant/log/smsr.log	8	9
smsclientlog	/var/camiant/log/smsclient.log	10	10
httplog	/var/camiant/log/HTTP.log	10	10
VNFMgrLog	/var/camiant/log/vnfmgr.log	2	5
UDRVNFMgrLog	/var/camiant/log/udrvnfmgr.log	2	5
UDRVNFAdapterLog	/var/camiant/log/udrvnfadapter.log	2	5
QPCfgRESTLog	/var/camiant/log/qp_cfg_ws.log	4	9
VNFAdapterRESTLog	/var/camiant/log/vnfadapter.log	4	9

DC Log Configuration

Scan Period (Seconds)	20
Root Log Level	WARN

File Appender Configuration

Appender Name	File Name	Maximum File Size (MB)	Maximum File Count
DCLog	/var/camiant/log/dc.log	8	9

SMSR Log Configuration

SMSR Log Level	WARN

File Appender Configuration

Appender Name	File Name	Maximum File Size (MB)	Maximum File Count
smsrlog	/var/camiant/log/smsr.log	8	9
smsclientlog	/var/camiant/log/smsclient.log	10	10
smpplog	/var/camiant/log/SMPP.log	20	10
cmpplog	/var/camiant/log/CMPP.log	20	10
smtplog	/var/camiant/log/SMTP.log	10	10
httplog	/var/camiant/log/HTTP.log	10	10

Class Log Configuration

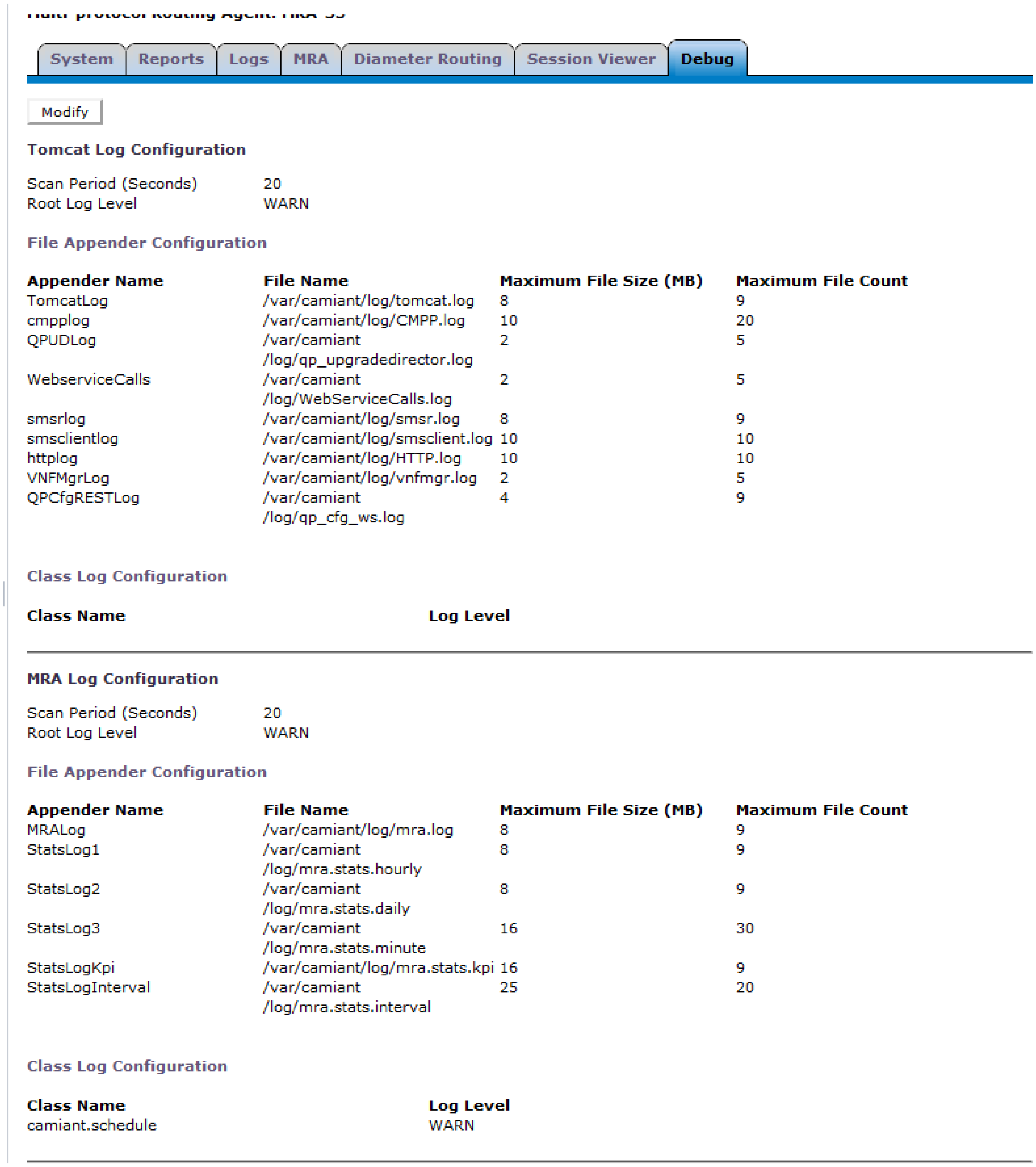
Class Name	Log Level
sms.queue	WARN

About MRA Debug Logs

Debugs logs for the MRA include log configuration for the following components:

- Tomcat Log
- RC Log

Figure 6-2   MRA Debug Logs



Tomcat Log Configuration

Scan Period (Seconds)	20
Root Log Level	WARN

File Appender Configuration

Appender Name	File Name	Maximum File Size (MB)	Maximum File Count
TomcatLog	/var/camiant/log/tomcat.log	8	9
cmpplog	/var/camiant/log/CMPP.log	10	20
QPUDLog	/var/camiant /log/qp_upgradedirector.log	2	5
WebserviceCalls	/var/camiant /log/WebServiceCalls.log	2	5
smsrlog	/var/camiant/log/smsr.log	8	9
smsclientlog	/var/camiant/log/smsclient.log	10	10
httplog	/var/camiant/log/HTTP.log	10	10
VNFMgrLog	/var/camiant/log/vnfmgr.log	2	5
QPCfgRESTLog	/var/camiant /log/qp_cfg_ws.log	4	9

Class Log Configuration

Class Name	Log Level

MRA Log Configuration

Scan Period (Seconds)	20
Root Log Level	WARN

File Appender Configuration

Appender Name	File Name	Maximum File Size (MB)	Maximum File Count
MRALog	/var/camiant/log/mra.log	8	9
StatsLog1	/var/camiant /log/mra.stats.hourly	8	9
StatsLog2	/var/camiant /log/mra.stats.daily	8	9
StatsLog3	/var/camiant /log/mra.stats.minute	16	30
StatsLogKpi	/var/camiant/log/mra.stats.kpi	16	9
StatsLogInterval	/var/camiant /log/mra.stats.interval	25	20

Class Log Configuration

Class Name	Log Level
camiant.schedule	WARN

> **Note:**
>
> The MPE device does not support SMSR (SMS Relay) Log configuration.

Configuring Debug Logs for a Device

> **Note:**
>
> While all CMP users can view debug log settings, only users with the **Administrator** user role can configure debug logs.

> **Note:**
>
> The MPE device does not support SMSR (SMS Relay) Log configuration.

To configure debug logs for a server:

1. From the appropriate (**Policy Server** or MRA section of the navigation pane, select **Configuration**.

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

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

   The Administration page for the device opens in the work area.

3. Select the **Debug** tab.

   The device Administration page shows the configuration settings for supported components (for example, Tomcat Log, RC Log, SMSR Log, or MRA log).

4. Click **Modify**.

   The device's Administration page becomes editable.

5. In the specific **Log Configuration** section (for example, Tomcat Log, RC Log, SMSR Log, or MRA log) enter a value if you want to override the default**Scan Period (seconds)**.

   The default value is 20 seconds.

   > **Note:**
   >
   > The MRA device does not support SMSR (SMS Relay) Log configuration.

6. To override the default value, select the **Root Log Level** from the list.

   Available options are:

   - **Off**—Turns off logging.
   - **Error**—Designates error events which may or may not be fatal to the application.
   - **Warn** (default)—Designates potentially harmful situations.
   - **Info**—Designates informational messages highlighting overall progress of the application.
   - **Debug**—Designates information events of lower importance.
   - **Trace**—Designates informational events of very low importance.
   - **All**—Records all logging levels.

7. To add a **Class Name**, in the **Class Log Configuration** section:
   a. Click **Add Row**.

      A confirmation message appears.
   b. Click **OK**.
   c. Enter the **Class Name**.

      For example, `example.schedule`.
   d. Select the **Log Level** from list.

   > **Note:**
   >
   > The CMP server performs no input validation on the entered **Class Name** or whether the **Class Name** belongs to the particular component.

8. Repeat for each debug component you wish to configure a **Class Name** level log.
9. Click **Save**.

The settings are applied to the selected device.

Deleting a Class Name from a Log File

> **Note:**
>
> While all CMP users can view debug log settings, only users with the **Administrator** user role can configure debug logs.

To delete a per class log for a component:

1. From the appropriate (**Policy Server** or MRA section of the navigation pane, select **Configuration**.

   The content tree displays a list of policy device groups; the initial group is **ALL**.
2. From the content tree, select the policy device.

   The Administration page for the device opens in the work area.
3. Select the **Debug** tab.

   The device Administration page shows the configuration settings.
4. Click **Modify**.

   The Modify page becomes editable.
5. To delete a **Class Name**:
   a. In the Modify page, locate the **Class Name** you want to delete.
   b. Click **Delete** next to the **Log Level**.

> **Note:**
>
> The Class Names `camiant.schedule` and `SMS.queue` are default class names and cannot be deleted.

6. Repeat for each debug component from which you wish to delete a **Class Name**.
7. Click **Save**.

The **Class Name** and **Log Level** are deleted from the selected device.

7

Managing Network Elements

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

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

About Network Elements

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

- Gateway GPRS support node (GGSN)
- Router
- Server

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

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

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

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

Creating a Network Element

You must create a network element for each device associated with any of the MPE devices within the network. To create 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. Click **Create Network Element**.

   The New Network Element page opens.

3. Enter information for the network element:

   a. (Required) **Name** — The name you assign to the network element.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.

b. (Required) **Host Name/IP Address** — Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element.

c. **Backup Host Name** — Alternate address that is used if communication between the MPE device and the primary address for the network element fails.

d. **Description/Location** — Free-form text.

   Enter up to 250 characters.

e. (Required) **Type** — Select the type of network element.

   The supported types are:

   - **PDSN**
     Packet Data Serving Node (with the sub-types **Generic PDSN** or **Starent**)
   - **HomeAgent**
     Customer equipment Home Agent (with the sub-types **Generic HomeAgent** or **Starent**)
   - **GGSN** (default)
     Gateway GPRS Support Node
   - **HSGW**
     HRPD Serving Gateway
   - **PGW**
     Packet Data Network Gateway
   - **SGW**
     Serving Gateway
   - **AF**
     Application Function
   - **DRA**
     Diameter Routing Agent
   - **DPI**
     Deep Packet Inspection device
   - **NAS**
     Network Access Server device

   > **Note:**
   >
   > For more information on managing network elements, see the *Configuration Management Platform Wireless User's Guide*.

f. **Protocol Timer Profile** — The timer profile that sets timeout values for messages in applications/interfaces.

   See Managing Protocol Timer Profiles for more information.

g. **Capability** — This field is valid for some network element types.

   When present, it contains the following options:

   - **TDF-Solicit** — DPI accepts Sd session establishment requests from the MPE device.
   - **Time-Tariff** — PGW and DPI network element types support Time-Tariff functionality.

- **Usage-Report-26** — GGSN, PGW, SGW, and DPI network element types are compatible with usage_report event trigger value 26.

h. **Capacity** — The bandwidth allocated to this network element.

4. In **Policy Servers associated with this Network Element**, select one or more policy servers (MPE devices) to associate with this network element.
5. In **MRAs associated with this Network Element**, select one or more Multi-Protocol Routing Agent (MRA devices) to associated with this network elements.
6. In **Network Element Groups which contain this Network Element**, select one or more groups (see Adding a Network Element to a Network Element Group).
7. Click **Save**.

You have created the definition for a network element and the network element is listed on the Network Element Administration page.

Configuring Options for Network Elements

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

> **Note:**
>
> Configuration changes made in the CMP system could potentially be reverted on an MPE device if the scheduled run time of the OSSI Distributor task on the Management Agent is before the scheduled run time for the CMP system. The discrepancy is resolved when the OSSI Distributor Task runs on the CMP system. See Managing Scheduled Tasks for more information.

Configuring the PDSN Network Element

To configure the packet-switched data network (PDSN) network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the PDSN tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the RADIUS-S features:

   a. **RADIUS Enabled**—Select to enable/disable RADIUS-S support for this network element.

   b. **RADIUS Shared Secret**—Enter the value that is used by the network element to authenticate RADIUS messages sent from the MPE device. This field must be configured with the same value that is provisioned on the network element or the MPE device will not be able to send messages to the network element.

5. Configure the Diameter features:

   a. **Diameter Realm**—Specifies the domain of responsibility for the network element (for example, `galactel.com`).

b. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

> **Note:**
>
> A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

6. Click **Save**.

The PDSN device is defined.

Configuring a GGSN Network Element

To configure a gateway GPRS support node (GGSN) network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the **GGSN** tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the following information:

   a. **IP Domain ID** — Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.

      Enter a string of 0–100 characters, using only letters, digits, periods (.) or hyphens (-). If left empty, IP domain mapping is disabled for this network element.

   b. **Diameter Realm** — Specifies the domain of responsibility for the network element (for example, `example.com`).

   c. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

> **Note:**
>
> A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The GGSN network element is configured.

Configuring the Home Agent Network Element

To configure the Home Agent network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the Home Agent tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the RADIUS-S features:

   a. **RADIUS Enabled**— Select to enable/disable RADIUS-S support for this network element.

   b. **RADIUS Shared Secret**— Enter the value that is used by the network element to authenticate RADIUS messages sent from the MPE device. This field must be configured with the same value that is provisioned on the network element or the MPE device will not be able to send messages to the network element.

5. Configure the Diameter features:

   a. **Diameter Realm**— Specifies the network element's domain of responsibility (for example, `galactel.com`).

   b. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

   > **Note:**
   >
   > A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

   A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

6. Click **Save**.

The Home Agent network element is defined.

Configuring the Radius-BNG Network Element

You can define up to 500 BNG devices.

To configure the Radius-BNG 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 **Radius-BNG** tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the following General information:

   a. **NAS ID**—Enter a unique identification string for this device.

   b. **IP Address**—Enter up to 20 IPv4 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**.

   c. **Subscriber key**—Select a subscriber key from the list of pre-defined keys in the RADIUS dictionary.

      The key is used for looking up subscribers associated with a RADIUS request. If a BNG device is identified while processing the associated request, this value is overridden by the subscriber key specified in the BNG device.

      > **Caution:**
      >
      > You must specify a subscriber key either here or in the BNG device.

5. Configure the following Accounting information.

   > **Note:**
   >
   > Any values entered in this section override the overall settings for MPE devices.

   a. **Interim Update Interval (sec.)**—Enter the default interim update interval. If a RADIUS Accounting-Start message specifies an interim update interval, an MPE device uses the value specified in the message; otherwise, it uses this value.

      Enter an integer from 1–604800 seconds (seven days). The default is 86400 seconds (one day).

   b. **Maximum Missed Updates**—Enter the number of missed updates before the RADIUS session becomes stale and must be purged. This value, multiplied by the **Interim Update Interval**, gives the number of seconds before a RADIUS session becomes stale.

      Enter an integer from 1–10 updates. The default is 3 missed updates.

   c. **Accounting Shared Secret**—Enter the accounting shared secret used to decrypt messages. If specified, this value overrides the value specified in the MPE configuration setting.

      Enter a string. The default is **no shared secret**.

6. Configure the following CoA information:

   a. **CoA Destination Port**—Enter the UDP port used to send CoA messages from an MPE device to this BNG device and to receive CoA-ACK messages.

      The default port is 3799.

b. **Session ID**—Select the session ID (a VSA code and name that identifies the session identifier) from the list.

   The default is **44/Acct-Session-Id**.

c. **Destination**—Enter an IP address or fully qualified domain name that specifies where the CoA message should be sent while processing Accounting requests.

d. **CoA Shared Secret**—Enter a shared secret value for CoA messages.

   Enter a string. The default is **no shared secret**. If entered, this value overrides the overall setting for MPE devices.

e. **Sub-session ID**—Select the sub-session ID from the list. This is a VSA for a chosen vendor ID that is used to identify a sub-session created by the BNG on receipt of a CoA message, so that the CoA is not sent in response to an Accounting-Start or Interim-Update message for a sub-session.

f. **Sub-session pattern**—Enter a regular expression pattern to match against the Sub-Session ID. If the pattern matches, then a CoA message is not sent for the corresponding Accounting-Start or Interim-Update message.

7. Click **Save**.

The Radius-BNG network element is configured.

Configuring the HSGW Network Element

To configure the HRPD Serving Gateway (HSGW) network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the **HSGW** tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the following information:

   a. **IP Domain ID** — This field is reserved for future use.

   b. **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).

   c. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

   > **Note:**
   >
   > A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

   A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The HSGW network element is configured.

Configuring the PGW Network Element

To configure the packet data network gateway (PGW) network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the **PGW** tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the following information:

   a. **IP Domain ID**—Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.

      Enter a string of 0–100 characters, using only letters, digits, periods (.) or hyphens (-). If left empty, IP domain mapping is disabled for this network element.

   b. **Diameter Realm**—Specifies the domain of responsibility for the network element (for example, `galactel.com`).

   c. **MIP6 Host Identity**—Specifies the Mobile IPv6 (MIPv6) host.

   d. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

      > **Note:**
      >
      > A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The PGW network element is configured.

Configuring the SGW Network Element

To configure the serving gateway (SGW) network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the **SGW** tab and then click **Modify**.

The Modify Network Element page opens.

4. Configure the following information:

   a. **IP Domain ID**—This field is reserved for future use.

   b. **Diameter Realm**—Specifies the domain of responsibility for the network element (for example, `example.com`).

   c. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

      > **Note:**
      >
      > A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The SGW network element is configured.

Configuring the AF Network Element

To configure the application function (AF) 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 AF network element you want to configure.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the AF tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the Diameter features:

   a. **IP Domain ID** — Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.

      Enter a string of 0-100 characters, using only letters, digits, periods (.) or hyphens (-). If left empty, IP domain mapping is disabled for this network element.

   b. **Diameter Realm**— Specifies the network element's domain of responsibility (for example, `example.com`).

   c. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

> **Note:**
>
> A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The AF network element is configured.

Configuring the DRA Network Element

To configure the Diameter Routing Agent (DRA) 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 DRA network element you want to configure.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the DRA tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the Diameter features:

   a. **IP Domain ID**—Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.

      Enter a string of 0-100 characters, using only letters, digits, periods (.) or hyphens (-). If left empty, IP domain mapping is disabled for this network element.

   b. **Diameter Realm**—Specifies the network element's domain of responsibility (for example, `example.com`).

   c. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

> **Note:**
>
> A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The DRA network element is configured.

Configuring a DPI Network Element

To configure deep packet inspection (DPI) network element:

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

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

2. From the content tree, select a network element with a type of DPI.

   > **Note:**
   >
   > If the list does not contain an element with the appropriate type, you must first define the network element of that type. See Creating a Network Element.

   The Network Element Administration page opens in the work area.

3. On the Network Element Administration page, select the **DPI** tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the following information:

   a. **IP Domain ID**—This field is reserved for future use.

   b. **Diameter Realm**—Specifies the domain of responsibility for the network element (for example, `example.com`).

   c. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

      > **Note:**
      >
      > A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. (TDF-Solicit fields) Configure the following traffic detection function fields.

   > **Note:**
   >
   > Traffic detection function fields are only available when the network capacity is TDF-Solicit. See Creating a Network Element for more information.

   a. **SCTP Enabled** (available if DPI capability is **TDF-Solicit**)—By selecting the check box, you connect to the traffic detection function (TDF) using the SCTP protocol. TCP is the default connection protocol.

b. **Allow direct connection from MPE** (available if DPI capability is **TDF-Solicit**)—By selecting the check box, TDF connects directly to Sd with the MPE device (bypassing the MRA device).

c. **TDF Port** (available if DPI capability is **TDF-Solicit**)—Enter the port number used to communicate with the TDF device. The default port is 3868.

d. **Watch Dog Interval** (available if DPI capability is **TDF-Solicit**)—Enter the watchdog interval in seconds. The default is 6 seconds.

e. **Response Timeout** (available if DPI capability is **TDF-Solicit**)—Enter the response timeout interval in seconds. The default is 5 seconds.

f. **Reconnect Delay** (available if DPI capability is **TDF-Solicit** and **Allow direct connection from MPE** is selected)—Enter the response time in seconds. The default is 3 seconds.

g. **Associated MRA identity** (available if DPI capability is **TDF-Solicit**)—Select the MRA device from the list.

   You cannot associate a DPI device with an MRA device if you have selected **Allow direct connection from MPE**.

h. **Backup TDF Identity** (available if DPI capability is **TDF-Solicit**)—Select the backup TDF device from the list.

6. Click **Save**.

The DPI device is configured.

Configuring a DSR Network Element

To configure an Oracle Communications Diameter Signaling Router (DSR) network element:

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

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

2. From the content tree, select a network element.

   The Network Element Administration page opens in the work area.

3. Select the **DSR** tab and then click **Modify**.

   The Modify Network Element page opens.

4. Configure the following information:

   a. **Diameter Realm**—Specifies the network element's domain of responsibility (for example, `galactel.com`).

   b. **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.example.com`).

> **Note:**
>
> A vendor-specified host name and realm name (such as `ne.example.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. Click **Save**.

The DSR device is defined.

Configuring the NAS Network Element

To configure the network access server (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. 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. Click **Save**.

The NAS network element is configured.

Finding a Network Element

The **Search** function lets you find a specific network element within a large configuration. You can also use the function to locate all of the Cable Modem Termination Systems (CMTS) and MPE devices associated with a specified subscriber IP address or subnets. To use the network element search function:

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

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

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

   The Network Element Administration page opens in the work area.

3. Click **Search**.

   The Network Element Search Criteria window opens.

4. Enter the search criteria:

   - **Name**
     The name assigned to the network element.

- **Host Name/IP Address**
  The domain name or IP address in IPv4 or IPv6 format of the network element.
- **Description**
  The information pertaining to the network element that helps identify it within the network. Enter up to 250 characters.

> **Note:**
>
> Searches are not case sensitive. You can use the wildcard characters `*` and `?`.

If a subscriber IP address is entered with a mask code (up to 32 for IPv4, or up to 128 for IPv6), then the associated MPE device is displayed. If the mask is left blank, then the input IP subnet is treated as an IP address, and the mask code is set automatically to 32 for IPv4 or 128 for IPv6.

5. After entering search criteria, click **Search**.

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

Modifying a Network Element

To modify a network element:

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

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

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

   The Modify Network Element page opens.
4. Modify the network element information.

   For a description of the fields contained on this page, see Creating a Network Element.
5. Click **Save**.

The network element definition is modified.

Deleting Network Elements

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

To delete a network element:

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

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

The Network Element Administration page opens in the work area, displaying all defined network elements.

3. From the work area, click 🗑 (trash can icon) located to the right of the network element.

   A confirmation message displays.

4. Click **OK**.

You have deleted the network element definition.

Deleting Multiple Network Elements

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

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

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

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

   The Network Element Administration page opens in the work area.

3. Click **Bulk Delete**.

   The Bulk Delete Network Elements page opens.

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

5. (Optional) Filter the search by entering a search pattern (for example, `cm*`) and click **Filter**.

   By default, the **Search Pattern** entry box contains an asterisk (*) to match all network elements.

6. Click **Bulk Delete**.

   A confirmation message displays.

7. Click **OK**.

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

Associating a Network Element with an MPE Device

To associate a network element with an MPE device:

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

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

2. From the content tree, select the MPE device.

   The Policy Server Administration page opens in the work area.

3. Select the **Policy Server** tab.

   The Associations section lists the network elements associated with the MPE device.

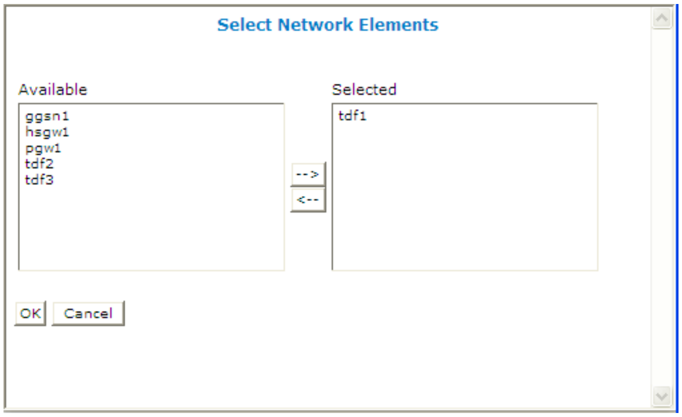
4. Click **Modify**.

   The Modify Policy Server page opens.

5. To the right of the list of network elements in the Associations section, click **Manage**.

   The Select Network Elements window opens.
   For example:

Figure 7-1 Select Network Elements



Select Network Elements

Available

ggsn1
hsgw1
pgw1
tdf2
tdf3

Selected

tdf1

6. Select the network elements in the **Available** list and click **-->**.

   If there are 50 or fewer defined network elements, they appear in the **Available** list. Select a network element from the **Available** list and click **-->**. The network element is moved to the **Selected** list.

   If there are more than 50 defined network elements, the **Available** list is initially blank. To add available items, enter a search string in the **Search Patterns** field. Searches are not case sensitive. You can use the wildcard characters '*' and '?'. Click **Filter**. The network elements are moved to the **Selected** list.
7. Click **OK**.

   The selected network elements are added to the list of network elements managed by this MPE device.
8. To associate a network element group with the MPE device, select the group from the list of network element groups located under **Associations**.
9. Click **Save**.

The network element is associated with this MPE device.

Disassociating a Network Element with an MPE Device

To disassociate a network element with an MPE device:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the MPE device.

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

   The Associations section lists the network elements associated with the MPE device.
4. Click **Modify**.

   The Modify Policy Server page opens.
5. To the right of the list of network elements in the Associations section, click **Manage**.

   The Select Network Elements window opens.

6. Select the network element from the **Selected** list and click **<--** (left arrow icon). To select multiple entries, press the Ctrl or Shift key and select the entries.
7. Click **OK**.

   The selected network elements are moved to the list of available network elements.
8. Click **Save**.

The network element is disassociated with this MPE device.

Working with Network Element Groups

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

Creating a Network Element Group

Network element groups exist in a distributed network to perform specific duties.
Use this procedure if you are creating a network element group to perform specific functions in your distributed network. After you create a network group, you can then create network elements to associate with devices such as an MPE or MRA.

To create a network element group:

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

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

   The Network Element Administration page opens in the work area.
3. Click **Create Group**.

   The **Create Group** page opens.
4. Enter the name of the new network element group.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.
5. Enter a text description and location of the network group.
6. Click **Save**.

You have created a network element group.

Adding a Network Element to a Network Element Group

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

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

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

   The Network Element Administration page opens in the work area, displaying the contents of the selected network element group.
3. Click **Add Network Element**.

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

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

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

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

5. Click **Save**.

The network element is added to the network element group.

Creating a Network Element Sub-group

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

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

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

2. From the content tree, select the network element group.

   The Network Element Administration page opens in the work area, displaying the contents of the selected network element group.

3. Click **Create Sub-Group**.

   The Create Group page opens.

4. Enter the name of the new sub-group.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

5. Enter a text description of the sub-group.

6. Click **Save**.

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

Deleting a Network Element from a Network Element Group

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

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

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

2. From the content tree, select the network element group or sub-group.

The Network Element Administration page opens in the work area, displaying the contents of the selected network element group or sub-group.

3. Remove the network element using one of the following methods:

   - On the Network Element Administration page, click the 🗑 (trash can) icon, located to the right to the network element.
   - From the content tree, select the network element; the Network Element Administration page opens. Click the **System** tab and then click **Remove**.

   A confirmation message appears.

4. Click **OK**.

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

Modifying a Network Element Group or Sub-Group

To modify a network element group or sub-group:

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

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

2. From the content tree, select the network element group or sub-group.

   The Network Element Administration page opens in the work area.

3. Click **Modify**.

   The Modify Group page opens.

4. Modify the name, description, or both.
5. Click **Save**.

The group or sub-group is modified.

Deleting a Network Element Group or Sub-group

Deleting a network element group also deletes any associated sub-groups. However, any network elements associated with the deleted groups or sub-groups remain in the **ALL** group, from which they can be used again if needed. You cannot delete the **ALL** group.
To delete a network element group or sub-group:

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

   The content tree displays a list of network element groups.

2. From the content tree, select the network element group or sub-group.

   The Network Element Administration page opens in the work area, displaying the contents of the selected network element group or sub-group.

3. Click **Delete**.

   A confirmation message displays.

4. Click **OK** to delete the group.

The network element group or sub-group is deleted.

8

Managing Protocol Timer Profiles

This chapter describes how to define and manage protocol timer profiles within the CMP system.

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

About Protocol Timer Profiles

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

> **Note:**
>
> A timer configured at the peer level takes precedence over a value configured at the global level.

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

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

Table 8-1 lists the Diameter applications and message types supported.

Table 8-1 Supported Diameter Applications and Messages

Application / Interface	Message
Gx	CCR, RAR
Rx	AAR, RAR, STR, ASR

Table 8-1 (Cont.) Supported Diameter Applications and Messages

Application / Interface	Message
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

About Wait Times for Message Timeouts

Message timeouts for applications that are added as data sources, such as Sh and Sy, have advanced configuration settings that allow specific response timeout values to be configured for that particular application. You can use service overrides to set the timeout in increments of 1 sec or you can set the time out in increments of 100 ms using Protocol Timer Profiles. You use the following service overrides to adjust the timeout wait for messages:

DRADRMA.ResponseTimeout
The amount of time when an MRA device considers a request timed out. The default is 5 seconds. To set the time out in increments of 100 ms, use Protocol Timer Profiles to set the timeout.

DIAMETER.ResponseTimeout
The amount of time when an MPE device considers a request timed out. The default is 5 seconds. To set the time out in increments of 100 ms, use Protocol Timer Profiles to set the timeout.

SH.ResponseTimeout
The amount of time when an Sh response is timed out. The default is 3 seconds.

SY.ResponseTimeout
The amount of time when an Sy response is timed out. The default is 3 seconds.

The amount of wait time in seconds before a response from an outstanding request times out between:

- MRA Site 1 and MRA Site 2
  The DRADRMA.ResponseTimeout is used for requests to the MPE devices it manages and to the associated/backup MRA device. The DRADRMA.ResponseTimeout defaults to 5 seconds.
- MRA Site 1 and MPE Site 1

  Verify that the MRA device does not timeout requests before the MPE device returns an answer. When setting the DRADRMA.ResponseTimeout service override, the value for DRADRMA.ResponseTimeout must be greater than or equal to the DIAMTER.ResponseTimeout service override. The following are example of factors that can affect the MPE devices capability to provide a timely response:

  - For Sh or Sy requests, the synchronous or on-demand lookup configuration for the data source in the MPE device.

  - If direct reply is disabled for AF requests, you must consider the timeout of the Gx-RAR request
  - When Sd is deployed, the Sd session must be established before making a reply to the Gx CCR-I request.

  For example: If the DRADRMA.ResponseTimeout expert setting is set to 4 seconds, a reasonable DIAMTER.ResponseTimeout value is 3 seconds, and then data source time out value of SH.ResponseTimeout or SY.ResponseTimeout is 2 seconds. If we go to finer granularity as to message type level, we need to set protocol timer profile globally or per peer.

- MPE Site 1 and SPR/UDR
  Verify that the MPE device does not timeout requests before the application (Sy or Sh) returns an answer. When setting the DIAMTER.ResponseTimeout service override, the value for DIAMTER.ResponseTimeout must be greater than or equal to the application service override (SH.ResponseTimeout or SY.ResponseTimeout).

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 a **Name** for the profile.

   A name is subject to the following rules:

   - The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
   - The name is case insensitive (uppercase and lowercase are treated as the same).
   - The maximum length is 255 characters.

4. (Optional) Enter a **Description**.

   Information that defines the profile.

5. 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.

6. Click **Save**.

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

Viewing a Protocol Timer Profile

To view a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.

   The content tree displays the **Protocol Timer Profiles** folder.

2. Select a profile.

   The configuration for the profile displays in the work area.

3. Change the view of the list using the following options:

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

The Protocol Timer Profile Timeout configuration displays by Application and Interface Message type. Timeout values are in milliseconds (msec).

Modifying a Protocol Timer Profile

A Protocol Timer Profile defines timeout values for messages in applications/interfaces.
To modify a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.

   The content tree displays the **Protocol Timer Profiles** folder.

2. Select a profile.

   The configuration for the profile displays in the work area.

3. Change the view of the list using the following options:

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

4. Click **Modify**.

   The Protocol Timer Profile Adminstration page opens with editable fields.

5. Modify the information.

   See Message Timeout Defaults for more information on the fields.

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

6. Click **Save**.

The profile is updated.

Deleting a Protocol Timer Profile

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

> **Note:**
>
> You cannot delete a Protocol Timer Profile that is associated with a device or group.

To delete a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.

   The content tree displays the **Protocol Timer Profiles** folder.
2. You can delete a profile using one of the following methods:
   - Select the **Protocol Timer Profiles** folder and then click **Delete** (🗑). A confirmation message displays. Click **OK** to delete.
   - Select a profile from the **Protocol Timer Profiles** folder and then click **Delete**. A confirmation message displays. Click **OK** to delete.

The profile is deleted.

Message Timeout Defaults

The following table shows the default timeout for specific message types within an application. The timeout value is in milliseconds, however the value can only be specified in increments of 100ms.

> **Note:**
>
> Because the MPE and MRA devices check for expired timers using a granularity of 100ms, an expired message is detected within a window of 100ms after the message has expired.

Table 8-2 Supported Diameter Applications, Message Types, and Timeout

Application / Interface	Message	Default timeout (msec)
Gx	CCR	5000
	RAR	5000
Rx	AAR	5000

Table 8-2 (Cont.) Supported Diameter Applications, Message Types, and Timeout

Application / Interface	Message	Default timeout (msec)
	RAR	5000
	STR	5000
	ASR	5000
S9	CCR	5000
	RAR	5000
Rx over S9	AAR	5000
	RAR	5000
	STR	5000
	ASR	5000
Sh	UDR	3000
	SNR	3000
	PNR	3000
	PUR	3000
Sy	SLR	3000
	STR	3000
	SNR	3000
Gy	CCR	5000
	RAR	5000
	ASR	5000
Sd	CCR	5000
	TSR	5000
	RAR	5000
Gxx	CCR	5000
	RAR	5000
VZr	SDR	5000

9
Managing Charging Servers

This chapter describes how to define and manage charging servers within the CMP system.

A charging server is an application that calculates billing charges.

About Charging Servers

A charging server is an application that calculates billing charges for a wireless subscriber. The CMP system supports both online and offline charging servers:

- An online charging server (OCS) calculates charges against a prepaid account for an event and returns information on how long the subscriber can use the service; it can affect, in real time, the service rendered.
- An offline charging server (OFCS) calculates charges for a service to an account, and does not affect (in real time) the service rendered.

Defining a Charging Server

To define a charging server:

1. From the navigation pane, select **Charging Servers**.

   The content tree displays the **Charging Servers** group.

2. Select the **Charging Servers** group.

   The Charging Server Administration page opens in the work area.

3. Click **Create Charging Server**.

   The New Charging Server page opens.

4. (Required) Enter the **Name** for the charging server.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

5. Enter the **Description/Location**.

   Free-form text that identifies the charging server within the network. Enter up to 250 characters.

6. (Required) Enter the **Host Name**.

   The FQDN (fully qualified domain name assigned) to the charging server.

7. Enter the **Port** number on which the charging server is listening for messages.

   If left blank, port 3868 is used.

8. Select the **Transport** protocol used to communicate with the charging server:

   Available options include:

   - **tcp**
     Transmission Control Protocol (used with TACACS+)

- **udp**
  User Datagram Protocol (used with RADIUS)

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

- **sctp**
  Stream Control Transmission Protocol

9. Select the Authentication, Authorization, and Accounting (AAA) **Protocol** used to communicate with the charging server.

   Available options include:

   - **diameter**
   - **radius**
     RADIUS uses UDP Transport protocol.

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

10. Select if transport **Security** is used to communicate with the charging server.
11. Click **Save**.

The charging server is displayed on the Charging Server Administration page.
After you define charging servers, you can select them as default charging servers when configuring an MPE device (see Configuring MPE Protocol Options) or use them in policy actions in the Policy Wizard (see *Policy Wizard Reference*).

Modifying a Charging Server

To modify the definition of a charging server:

1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.

   The Charging Server Administration page opens in the work area, listing the defined charging servers.

2. Select the charging server you want to modify.

   The Charging Server Administration page displays information about the charging server.

3. Click **Modify**.

   The Modify Charging Server page opens.

4. Modify charging server information as required.

   For a description of the fields contained on this page, see Defining a Charging Server.

5. Click **Save**.

The charging server definition is modified.

Deleting a Charging Server

To delete a charging server:

1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.

   The Charging Server Administration page opens in the work area and lists the defined charging servers.

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

   - From the work area, click 🗑 (**Delete** icon), located to the right of the charging server name.
   - From the content tree, select the charging server name and click **Delete**.

   A confirmation message displays.

3. Click **OK** to delete the charging server.

The charging server definition is removed from the list.

Associating a Charging Server with an MPE Device

To associate a charging server with an MPE device:

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

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

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

   The Policy Server Administration page opens in the work area.

3. Select the **Policy Server** tab.

   The Default Charging Servers section of the page lists charging servers associated with this policy server.

4. Click **Modify**.

   The Modify Policy Server page opens.

5. In the Default Charging Servers section, select the following:

   - Primary Online Server
   - Primary Offline Server
   - Secondary Online Server
   - Secondary Offline Server

6. Click **Save**.

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

Defining Charging Methods with an MPE Device

When default charging methods are configured, the MPE can provision the Online and Offline AVP values at the session level in CCA-initial message. The charging method information can be supplied or configured in different sources. The following list indicates the priority used to decide the default charging method used:

1. PCRF default configuration, as described above
2. PGW, as supplied in CCR message
3. SPR, specified in ONCHA and OFFCHA fields in user profile
4. PCRF policy engine

If GW supplies default charging method in CCR-initial request, PCRF will always put default charging method AVPs in CCA-initial message, even though there is no change to the values in which case PCRF simply copies the values from request to reply.

To define the charging method for an MPE device:

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

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

   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, select the **Policy Server** tab.

   The page lists displays the configuration of the policy server.
4. Click **Modify**.

   The Modify Policy Server page opens.
5. In the Default Charging Methods section, select the **Default Online Charging Method** and the **Default Offline Charging Method** from the lists.
6. Click **Save**.

The charging methods are defined for this MPE device.

10 Managing SMS Gateways

This chapter describes how to create, manage, and associate Short Message Service (SMS) gateways.

An SMS gateway manages the sending and receiving of SMS transmissions to or from a wireless network.

SMS gateways are only available in either Wireless mode with SMPP enabled, or in Wireless-C mode with CMPP enabled.

About SMS Gateways

An SMS gateway manages the sending and receiving of SMS transmissions to or from a wireless network. It sits between the subscriber who needs to send/receive SMS and the short message service center (SMSC). The SMS gateway is available when Wireless mode has SMPP enabled or Wireless-C mode has CMPP enabled.

After you have defined SMS gateways, you associate them with the MPE device to mange the sending and receiving of SMS messages. You can define a maximum of 10 gateways. The default gateway is configured in the Policy Server Configuration section using the Policy Server tab.

Creating an SMS gateway

You can create a maximum of 10 SMS gateways. You must be in either Wireless mode with SMPP enabled, or in Wireless-C mode with CMPP enabled to use SMS gateway

To create an SMS gateway:

1. From the **Policy Server** section of the navigation pane, select **SMS Gateways**.

   The content tree displays the **SMS Gateways** folder.

2. Click **Create SMS Gateway**.

   The New SMS Gateway page opens.

3. Enter information for the SMS gateway:
   - For SMPP mode, see SMPP SMS Gateway Options.
   - For Wireless-C mode, see CMPP SMS Gateway Options.

4. Click **Save**.

You have created an SMS gateway and the gateway is listed on the SMS Gateway Administration page.

CMPP SMS Gateway Options

Name
Unique name for the SMS Gateway.

Description/Location
A description of the SMS gateway that can include information about the location.

CMPP Enabled
If selected, this gateway is enabled.

SMSC Host
The SMSC host address.

SMSC Port
The SMSC port number. The default 7890.

Source Address
The source address of the CMPP client.

Shared Secret
The name of the shared secret, which is used to generate the authenticator source.

Registered Delivery
Specify whether to receive a delivery receipt. The default is **No delivery receipt**.

Service Id
The service ID. Enter a string value with a 10-character length.

Message Format
The options are:

- ASCII Encoding (default)
- Message Write Card Operation
- Binary Message
- UCS2 Encoding
- GBK Encoding

> **Note:**
>
> To support Chinese characters in the message content, the format should be UCS2 or GBK.

Policy Servers associated with this SMS Gateway

Select the Policy Servers to associate with this SMS gateway. Select **All** to associate the gateways with all the defined Policy Servers. You can also remove an association in this section by clearing the selection.

SMPP SMS Gateway Options

Name
Unique name for the SMS Gateway.

Description/Location
A description of the SMS gateway that can include information about the location.

SMPP Enabled
If selected, this gateway is enabled.

Validate Message Length
If selected the message length is validated. The default is to validate the message length.

SMPP Longe 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. The default is to support long messages.

Delivery Method For Long Message
The message delivery methods for long messages are:

- Undefined, Segmentation and Reassembly (SAR) (default)
- Message Payload

Primary Server Configuration

SMSC Host
The IP address of the primary SMSC store-and-forward server, which accepts SMS messages from the relay server.

SMSC Port
The port number on which the primary SMSC store-and-forward server is listening for SMS messages. The default port is 2775.

ESME System ID
The External Short Messaging Entity (ESME) system ID for the primary ESME system.

ESME Password
The password of the primary ESME. 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
Repeat the primary ESME system password for verification.

Secondary Server Configuration

(Optional) You can configure a secondary server to handle SMS messages.

SMSC Host
The IP address of the primary SMSC store-and-forward server, which accepts SMS messages from the relay server.

SMSC Port
The port number on which the primary SMSC store-and-forward server is listening for SMS messages. The default port is 2775.

ESME System ID
The External Short Messaging Entity (ESME) system ID for the primary ESME system.

ESME Password
The password of the primary ESME. 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
Repeat the primary ESME system password for verification.

SMPP Address and Encoding Configuration

ESME Source Address
Enter the source address for a submit operation in SMPP. The default is none.

ESME Source Address TON
Select the source address Type of Number (TON) from the 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 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 menu:

- SMSC Default Alphabet (default)
- 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 KanjiJIS(X 212-1990)

SMSC Default Encoding Scheme
Select the default encoding scheme for SMSC messages from the menu::

- UTF-8
- GSM7

Request Delivery Receipt
Select the global default behavior when evaluating the policy action send SMS from the menu:

- No Delivery Receipt (default)
- Receipt on success and failure
- Receipt on failure

Policy Servers associated with this SMS Gateway

Select the Policy Servers to associate with this SMS gateway. Select **All** to associate the gateways with all the defined Policy Servers. You can also remove an association in this section by clearing the selection.

Modifying an SMS Gateway

To modify an SMS Gateway:

1. From the **Policy Server** section of the navigation pane, select **SMS Gateways**.

   The content tree displays the **SMS Gateways** folder.
2. From the content tree, select the network element.

   The SMS Gateways Administration page opens in the work area.
3. Click **Modify**.

   The Modify SMS Gateway page opens.
4. Modify the SMS gateway information.

   For a description of the fields contained on this page, see Creating an SMS gateway.
5. Click **Save**.

The SMS gateway definition is modified.

Deleting SMS Gateways

Before deleting an SMS gateway, you must disassociate the gateway from all the Policy Servers. See Disassociating an SMS Gateway from all Policy Servers.

Deleting an SMS gateway definition removes it from the list of gateways that a Policy Management device can use to send SMS messages. To delete an SMS gateway 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 an SMS gateway:

1. From the **Policy Server** section of the navigation pane, select **SMS Gateways**.

   The content tree displays the **SMS Gateways** folder.

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

   The SMS Gateways Administration page opens in the work area, displaying all defined network elements.

3. From the work area, click 🗑 (trash can icon) located to the right of the SMS gateway.

   A confirmation message displays.

4. Click **OK**.

You have deleted the SMS gateway definition.

Associating SMS Gateways with an MPE Device

To associate SMS gateways with an MPE device:

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

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

2. From the content tree, select the MPE device.

   The Policy Server Administration page opens in the work area.

3. Select the **Policy Server** tab.

   The Associations section lists the SMS gateways associated with the MPE device.

4. Click **Modify**.

   The Modify Policy Server page opens.

5. To the right of the list of SMS gateways in the Associations section, click **Manage**.

   The Select SMS Gateways window opens.

6. Select one or more gateways in the **Available** list and click **-->** (right arrow icon).

   The gateway is moved to the **Selected** list.

7. Click **OK**.

   The selected network elements are added to the list of SMS gateways managed by this MPE device.

8. Click **Save**.

The SMS gateway is associated with this MPE device.

Associating an SMS Gateway with multiple Policy Servers

To associate an SMS gateway with multiple Policy Servers:

1. From the **Policy Server** section of the navigation pane, select **SMS Gateways**.

   The content tree displays the **SMS Gateways** folder.

2. From the content tree, select the SMS gateway.

The SMS Gateway Administration page opens in the work area.

3. Click **Modify**.

   The Modify SMS Server page opens.

4. In the Policy Servers associated with this SMS Gateway select the Policy Servers to associate with this gateway:

5. Click **Save**.

The SMS gateway is associated with the selected Policy Servers.

Disassociating an SMS Gateway from a Policy Server

To disassociate an SMS gateway from a Policy Server:

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

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

2. From the content tree, select the Policy Server device.

   The Policy Server Administration page opens in the work area.

3. Select the **Policy Server** tab.

   The Associations section lists the SMS gateways associated with the Policy Server.

4. Click **Modify**.

   The Modify Policy Server page opens.

5. To the right of the list of SMS gateways in the Associations section, click **Manage**.

   The Select SMS Gateways window opens.

6. Select the SMS gateway in the **Selected** list and click <-- (left arrow icon). To select multiple entries, press the Ctrl or Shift key and select the entries.

7. Click **OK**.

   The selected network elements are moved to the list of available SMS gateways.

8. Click **Save**.

The SMS gateway is disassociated with this MPE device.

Disassociating an SMS Gateway from all Policy Servers

To disassociate an SMS gateway from all Policy Servers:

1. From the **Policy Server** section of the navigation pane, select **SMS Gateways**.

   The content tree displays the **SMS Gateways** folder.

2. From the content tree, select the SMS gateway.

   The SMS Gateway Administration page opens in the work area.

3. Click **Modify**.

   The Modify SMS Server page opens.

4. In the Policy Servers associated with this SMS Gateway:

   - If all the Policy Server are selected, the **ALL** checkbox contains a checkmark (☑). Click **ALL** once to disassociate all the Policy Servers.

- If one or more of the servers are selected but not all, the **ALL** checkbox is partially shaded (). Click **ALL** twice to clear the checkbox.

5. Click **Save**.

The SMS gateway is disassociated from all Policy Servers.

11

Mapping Serving Gateways to MCCs/MNCs

This chapter describes how to map serving gateways (SGW) to mobile country codes (MCCs) and mobile network codes (MNCs) in the CMP system.

About Mapping Serving Gateways to MCCs/MNCs

It is possible that an SGSN (Serving GPRS Support Node) does not provide a GGSN (Gateway GPRS Support Node) with accurate or complete mobile country code (MCC) or mobile network code (MNC) information. If not, the GGSN cannot pass this information on to the PCRF (including an MPE device), reducing the PCRF's ability to detect specific roaming scenarios. The MCC/MNC mapping table provides a mechanism for the MPE device to convert an SGSN IP address (a value the GGSN can determine without SGSN input) to the proper MCC/MNC value. You can map multiple serving gateways to each MCC/MNC pair. After the MCC/MNC values are determined, they can be used in policies to differentiate subscriber treatment based on the specific roaming scenario.

Creating a Mapping

To create a mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.

   The content tree displays the **Serving Gateway/MCC-MNC Mappings** group.

2. Select the **Serving Gateway/MCC-MNC Mappings** group.

   The Serving Gateway/MCC-MNC Mappings Administration page opens in the work area, listing available mappings.

3. Click **Create Serving Gateway/MCC-MNC Mapping**.

   The New Serving Gateway/MCC-MNC Mapping page opens.

4. Enter the following information:

   a. **Name** (required) — The name assigned to the mapping.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_). The maximum length is 250 characters.

   b. **Description** — A descriptive phrase.

   c. **MCC-MNC** (required) — The MCC-MNC pair, in the format *mccmnc*; for example, 310012 for Verizon Wireless in the United States.

   d. **Serving Gateway IP Address/Subnet** (required) — The IP address or subnet, in IPv4 or IPv6 format, of a serving gateway.

      - To add an address to the mapping list, enter it and click **Add**.
      - To remove one or more mappings from the list, select them and click **Delete**.

5. Click **Save**.

The mapping is created and stored in the **Serving Gateway/MCC-MNC Mappings** group.

Modifying a Mapping

To modify a Serving Gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.

   The content tree displays the **Serving Gateway/MCC-MNC Mappings** group.

2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.

   The Serving Gateway/MCC-MNC Mappings Administration page opens, displaying the list of defined mappings.

3. Select the mapping you want to modify.

   Mapping information is displayed.

4. Click **Modify**.

   The Modify Serving Gateway/MCC-MNC Mapping page opens.

5. Modify mapping information as required.

   For a description of the fields contained on this page, see Creating a Mapping.

6. Click **Save**.

The mapping is modified.

Deleting a Mapping

To delete a serving gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.

   The content tree displays the **Serving Gateway/MCC-MNC Mappings**.

2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.

   The Serving Gateway/MCC-MNC Mappings Administration page opens, displaying the list of defined mappings.

3. Delete the mapping using one of the following methods:

   - From the work area, click **Delete** (🗑), located to the right of the mapping you want to delete.
   - From the content tree, select the mapping and click **Delete**.

   A confirmation message displays.

4. Click **OK** to delete the Serving Gateway/MCC-MNC mapping.

The mapping is deleted.

12

Managing a Subscriber Profile Repository

This chapter describes how to define and manage an optional Subscriber Profile Repository (SPR) using the CMP system.

An SPR is a system for storing and managing subscriber-specific policy control data as defined in the 3GPP standard.

> **Note:**
>
> For information on operating Oracle Communications Enhanced Subscriber Profile Repository devices, refer to the *Enhanced Subscriber Profile Repository User's Guide*.

About Subscriber Profile Repositories

A Subscriber Profile Repository (SPR) is a system for storing and managing subscriber-specific policy control data as defined under the 3GPP standard.

An SPR can be deployed in environments where the MPE device needs access to a separate repository for subscriber data. The SPR acts as a centralized repository for this data so that multiple MPE devices can access and share the data. This data can include profile data (pre-provisioned information that describes the capabilities of each subscriber), quota data (information that represents the subscriber's use of managed resources), or other subscriber-specific data.

The following SPR systems can be used in the CMP system:

- The Oracle Communications Subscriber Database Management (SDM) product includes interfaces for provisioning subscriber information, as well as managing, changing, and accessing this information. These interfaces include an application programming interface for XML provisioning of subscriber profile data, as well as an interactive user interface through the Configuration Management Platform system using a proprietary RESTful API interface.
  The SDM system is built upon an existing software base and technology. It not only manages static provisioned subscriber data, but also dynamic intra- and inter-session data from MPE devices—for example, when it is critical to store inter-session quota data centrally so that it can be retrieved upon the next subscriber attachment, wherever that attachment occurs within the network. Intra-session data such as mappings from IP addresses to MSISDNs becomes important as well, especially when managing enforcement points such as DPI devices and optimization gateways where MSISDN/IMSI data is not available. With this the Subscriber Database Management system provides both a storage and notification platform for policy operations, as well as a platform for provisioning.

  For detailed information on the Subscriber Database Management system, see the Subscriber Data Management documentation.
- The Oracle Communications User Data Repository (UDR) is a highly-scalable, consolidated database back end for subscriber and profile data. User Data Repository

utilizes multiple application front ends with the database. UDR supports the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application, a function used for the storage and management of subscriber policy control and pool data. XML-REST and XML-SOAP interfaces are used by Enhanced Subscriber Profile Repository for creating, retrieving, modifying, and deleting subscriber and pool data.

For detailed information on the UDR, see the User Data Repository documentation.

- A customer-specified SPR.
  See the Subscriber Profile Repository documentation for more information.

To use an SPR with the CMP system, you must perform the following actions:

- Configuring the CMP System to Manage SPR Subscriber Data
- Configuring the SPR Connection

You can also modify an SPR connection. See Modifying the SPR Connection for details.

Configuring the CMP System to Manage SPR Subscriber Data

The CMP system can manage SPR subscriber data. Before this can occur, the CMP operating mode must support managing SPR clusters.

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

To reconfigure the CMP operating mode:

1. From the **Help** section of the navigation pane, select **About**.

   The About page opens, displaying the CMP software release number.
2. Click the **Change Mode** button.

   Consult with My Oracle Support for information on this button.

   The Mode Settings page opens.
3. In the Mode section, select the mode **Diameter 3GPP**, **Diameter 3GPP2**, or **PCC Extensions**, as appropriate.
4. At the bottom of the page, select **Manage SPR Subscriber Data**.
5. Click **OK**.

   The browser page closes and you are automatically logged out.
6. Refresh the browser page.

   The Welcome page opens.

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

Configuring the SPR Connection

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

To configure the SPR connection:

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

   The SPR Connection Configuration page opens in the work area, displaying connection information.

2. On the SPR Connection Configuration page, click **Modify**.

   The Configuration page opens.

3. Enter information as appropriate for the SPR system:

   a. **SPR Operation Mode** (required) —Select from the list:

      - **SDM RESTful API** (default)

   b. **Remote Port**—Enter the port (a number from 1 to 65535) to listen on for SPR traffic.

      The default port is 8787.

   c. **Secure Connection**—Select to establish a secure connection.

   d. **SDM Profile Fields**—Defines the custom fields for the SDM profile.

      Enter the field name in the field and click **Add**. To remove a field from the list, select the field and click **Delete**.

   e. **SDM Pool Fields**—Defines the custom fields for the SDM pool.

      Enter the field name in the field and click **Add**. To remove a field from the list, select the field and click **Delete**.

4. Click **Save**.

The SPR connection is configured.

Modifying the SPR Connection

To modify the SPR connection:

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

   The SPR Connection Configuration page opens in the work area, displaying connection information.

2. Click **Modify**.

   The Configuration page opens.

3. Modify the configuration information.

   See Configuring the SPR Connection for information on the fields on this page.

4. Click **Save**.

The SPR connection configuration is modified.

About Subscriber Profiles

A subscriber profile defines the general information for the subscriber, as well as feature-specific information such as, quotas, pools, and so on.

The CMP system allows you to perform the following subscriber profile management actions:

- Finding a Subscriber Profile
- Creating a Subscriber Profile

- Modifying a Subscriber Profile
- Deleting a Subscriber Profile

Creating a Subscriber Profile

If an SPR database is configured to use the RESTful API interface, you can manually create a subscriber profile.
To create a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Click **Create Subscriber Profile**.

   The New Subscriber Profile page opens in the work area.

3. Enter the following information:

   a. Select the **Data Source Primary Diameter Identity**.

      You can select any SPR device configured for the Policy Management network.

   b. In the **Key Fields** section, enter one format:

      - **NAI**
        Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name.

        A valid user name consists of the characters &, *, +, 0 thought 9,?, a through z, _, A through Z, {, }, !, #, $, %, ', ^, /, =, `, |, ~, -, optionally separated by a period (.).

        A valid realm name consists of the characters 0 through 9, a through z, and A through Z separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.

      - **E.164 (MSISDN)**
        Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).

      - **IMSI**
        International Mobile Subscriber Identity. Enter up to 15 Unicode digits.

   c. Optionally, in the **Subscriber Information** section, enter the following:

      - **Account ID**
        Free-form string that identifies the account for the subscriber. You can enter up to 255 characters.

      - **Billing Day**
        The day of the month on which the quota for the subscriber is reset.

        For a UDR or SDM system, the valid range is 0 through 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 tier for the subscriber. Enter a tier name defined in the CMP database; or, if you click **Manage**, a window opens from which you can select a tier name. In order to add a tier, you must enter the tier name prior to clicking **Manage**. See Managing Subscribers for information on managing tiers

        .

- **Entitlements**
  The entitlements for the subscriber. Enter the entitlement names; or, if you click **Manage**, a window opens from which you can enter or select entitlement names defined in the CMP database. See Managing Subscribers for information on managing entitlements.

  > **Note:**
  >
  > Entitlements are defined external to the CMP system.

- **Custom**
  Free-form strings representing custom subscriber fields. You can enter up to 255 characters per field. By default, five fields are available, but if the subscriber profile has more than five custom fields defined, the page displays them. Click **Add** to create additional fields as needed.
- **User Billing Type**
  The type of billing. Enter a value of 0 (online charging) or 1 (offline charging). The default value is 1.
- **User Notify MSISDN**
  The mobile number used to send messages or reminders to users. Enter a character string of 1 through 15 characters in length.
- **User Status** (not visibile with V4 profile)
  The quota status for the user. This value determines whether the user is within quota. Enter a value between 1 and 100.
  - A value of 1 means the user is within the quota.
  - A value of 2 means the user is outside the quota.
  - A value of 3 means the user exceeds the value of the top-up.
  - Values of 4 through 50 are used for united expansion in Group Company.
  - Values of 51 through 100 are used for expansion in companies in each province.

  If the user status has a value of 2 or 3, the value is reset to the default (0) on the date configured by the **Billing Day** field.
- **Package Type** (optional with V4 profile)
  Indicates if the user is subscribing to the package.
- **Operate Time** (required with V4 profile)
  The length of time the package is available. Specified in the 24-hour format of *yyyymmddhhmmss*, where *hh* is a 24-hour format.

4. Click **Save**.

The subscriber profile is created.

Finding a Subscriber Profile

After the SPR devices are defined, you can search them for a subscriber profile.
To find a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select the **Data Source Primary Diameter Identity**.

   This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.

3. Select the **Key Type**:

   - **E.164 (MSISDN)** (default) — search by Mobile Station International Subscriber Directory Number. This is a number of up to 15 digits.
   - **IMSI** — search by International Mobile Subscriber Identity. This is a number of up to 15 digits.
   - **NAI** — search by Network Access Identifier.
   - **Pool ID** — search by quota pool identifier.

4. **Key String** — enter a search string in the format appropriate for the selected key type.

   The string must match exactly; partial or wildcard searching is not supported.

5. Click **Search**.

   The Subscriber Profile page opens, displaying information about the subscriber.

   > **Note:**
   >
   > If no matching subscriber profile is found, the page displays the message `No matching user is found`.

6. Click **Back to Search Page**.

   The Subscriber Profile Administration page opens.

Modifying a Subscriber Profile

To modify a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select the subscriber profile you want to modify.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Click **Modify**.

   The Subscriber Profile Administration page opens.

4. Modify subscriber profile information as required.

   For a description of the fields contained on this page, see Creating a Subscriber Profile.

5. Click **Save**.

The subscriber profile is modified.

Deleting a Subscriber Profile

Using the RESTful API operation mode, you can delete a subscriber profile. See Configuring the SPR Connection for information on setting the operation mode.

To delete a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Search for the subscriber profile you want to delete.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Click **Delete**.

   A confirmation message displays.

4. Click **OK** to delete the subscriber profile.

The subscriber profile is deleted.

About Subscriber Quota Categories

A subscriber quota category defines a category's name, type (that is, quota (plan), pass, rollover, top-up, or default rollover), consumption time, volumes, state, and so on.

The CMP system allows you to perform the following subscriber quota category management actions:

- Viewing Subscriber Quota Information Associated with a Subscriber
- Adding a Subscriber Quota Category
- Modifying a Subscriber Quota Category
- Deleting a Subscriber Quota Category

Adding a Subscriber Quota Category

To add a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Search for the subscriber profile you want to view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **Quota** tab.

   The Quota Usage information is shown in the work area.

4. Click **Create**.

   The Quota Usage page opens.

5. If there are more than 10 quotas, a message displays prompting you to add more. Click **Yes**.

6. Enter the following information:

   a. **CID**: A unique identifier assigned by the CMP system. Rollovers and top-ups have the CID of their associated plan.

> **Note:**
>
> This information is assigned by the system, and you should not change it. The CID is assigned to a quota plan when it is created in the CMP. All usage for the quota plan is tracked through this CID. During migration scenarios, customer must make sure that the quota plan's CID on the new CMP matches the CID on an old CMP, otherwise all previous quota usage will be discarded.

b. **Name** (required): Select the name of a quota. You cannot add the same quota twice for a subscriber. See the *Policy Wizard Reference* for information on creating quotas.

c. **Type**: Select the type of quota defined in the CMP system. You can select **quota** (plan), **pass**, **rollover**, **top-up**, or **default rollover**.

d. **Time (seconds)**: Enter a value, in seconds, to track time consumption.

   The valid range is: -2^{63} to 2^{63}– 1 (a 64-bit value).

e. **Total Volume (bytes)**: Enter a value, in bytes, to track bandwidth volume consumption.

   The valid range is: -2^{63} to 2^{63}– 1 (a 64-bit value).

f. **Upstream Volume (bytes)**: Enter a value, in bytes, to track upstream bandwidth volume consumption.

   The valid range is: -2^{63} to 2^{63}– 1 (a 64-bit value).

g. **Downstream Volume (bytes)**: Enter a value, in bytes, to track downstream bandwidth volume consumption.

   The valid range is: -2^{63} to 2^{63}– 1 (a 64-bit value).

h. **Service Specific Event**: Enter a value representing service-specific resource consumption.

   The valid range is: -2^{63} to 2^{63}– 1 (a 64-bit value).

i. **Next Reset Time** (required): Enter a date and time after which the quotas need to be reset, in the format *yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*[*Z*] (for example, `2011-11-01T00:00:01-5:00`).

   Alternatively, click 📅 (calendar) and select a date, enter a time, and optionally select a UTC offset (time zone). Click **OK**.

j. **Quota State**: This field is an internal identifier and should not be defined by the user.

k. **RefInstanceID**: The CID of the associated plan. This field only applies to a top-up type quota.

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

7. Click **Save**.

The subscriber quota is defined.

Viewing Subscriber Quota Information Associated with a Subscriber

To view the subscriber quotas information associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Search for the subscriber profile.

   The profile information is shown. (See Finding a Subscriber Profile for information on locating a subscriber profile.)

3. Select the **Quota** tab.

   The Subscriber Profile Quota Usage page opens. The table provides the following information:

   - **Name**
     Quota name defined in the CMP system.
   - **Time Usage**
     Usage counter, in seconds, to track time-based resource consumption.
   - **Time Limit**
     Time limit, in seconds, defined in the named quota.
   - **Total Volume Usage**
     Usage counter, in bytes, to track volume-based resource consumption.
   - **Total Volume Limit**
     Volume limit, in bytes, defined in the named quota.
   - **Upstream Volume Usage**
     Usage counter, in bytes, to track upstream bandwidth volume-based resource consumption. Also known as Input Volume.
   - **Upstream Volume Limit**
     Upstream volume limit, in bytes, defined in the named quota.
   - **Downstream Volume Usage**
     Usage counter, in bytes, to track downstream bandwidth volume-based resource consumption. Also known as Output Volume.
   - **Downstream Volume Limit**
     Downstream volume limit, in bytes, defined in the named quota.
   - **Service Specific Event**
     Usage counter to track service-specific resource consumption.
   - **Service Specific Event Limit**
     Resource consumption limit defined in the named quota.
   - **Next Reset Time**
     The time after which the usage counters need to be reset.
   - **CID**
     A unique identifier, assigned by the CMP system. Top-ups and rollovers have the CID of their associated plan.
   - **Type**
     Defines whether the data is for a quota (plan), pass, rollover, top-up, or default rollover.
   - **Quota State**

An internal identifier, which defines whether the option selected in the **Type** field is active or expired.

- **RefInstanceId**
  The CID of the plan.

4. Click **Back to Search Page**.

You have viewed the subscriber quota information.

Modifying a Subscriber Quota Category

To modify a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Search for the subscriber profile you want to view.

   The profile information is shown. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **Quota** tab.

   The Subscriber Profile Quota Usage page opens.
4. Click the **Name** of the quota you want to modify.

   The Quota Usage page opens, displaying information about the quota.
5. Modify the subscriber quota information as required.

   For a description of the fields contained on this page, see Adding a Subscriber Quota Category.
6. Click **Save**.

The subscriber quota category is modified.

Deleting a Subscriber Quota Category

To delete a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Search for the subscriber profile you want to modify.

   The profile information is shown. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **Quota** tab.

   The Subscriber Profile Quota Usage page opens.
4. In the list of quotas:
   - Use the check boxes to select the quota or quotas you want to delete.
   - To select all quotas, click **All**.
   - To deselect all quotas, click **None**.
5. Click **Delete**.

   A confirmation message displays.

6. Click **OK**.

   The quota or quotas are removed from the list.

The subscriber quota categories are deleted.

About Subscriber Entity States

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

The CMP system allows you to perform the following subscriber entity state actions:

- Viewing Subscriber Entity States Associated with a Subscriber
- Creating a Subscriber Entity State Property
- Modifying a Subscriber Entity State Property
- Deleting a Subscriber Entity State Property

Creating a Subscriber Entity State Property

To create a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select the subscriber profile you want to modify.

   That profile information is shown. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **State** tab.

   The entity state information is shown.

4. Click **Create**.

   The Create Property page opens.

5. Enter the following information:

   a. **Name** — The name assigned to the property.

      The name cannot be blank and must be unique within this list of properties.

   b. **Value** — The property value.

      The value cannot be blank.

6. Click **Save**.

   The profile information page opens and displays the message `Properties created successfully`.

7. To create additional properties, repeat steps 4 through 6.

   If you exceed 100 states, you are prompted whether you want to add more. Click **Yes** to continue, or **No** to stop.

8. Click **Back to Search Page**.

   The page displays the message `Properties created successfully`.

The subscriber entity state property is defined.

Viewing Subscriber Entity States Associated with a Subscriber

To view the subscriber entity states associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Search for the subscriber profile you want to view.

   That subscriber profile information is shown. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Click the **State** tab.

   Entity state information is shown.

4. Click **Back to Search Page**.

You have viewed the subscriber entity states.

Modifying a Subscriber Entity State Property

You can modify the value (but not the name) of a subscriber profile entity state property. To modify a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select the subscriber profile you want to modify.

   The profile information is shown. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **State** tab.

   The entity state information is shown.

4. In the list of entity state properties, click the property you want to modify.

   The Modify Property page opens.

5. Modify the property value as required.

   The value cannot be blank.

6. Click **Save**.

The subscriber entity state property value is modified.

Deleting a Subscriber Entity State Property

To delete a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Search for the subscriber profile you want to modify.

   The profile information is shown. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **State** tab.

   The entity state information is shown.

4. In the list of entity state properties:
   - Use the check boxes to select the property or properties you want to delete.
   - To select all properties, click **All**.
   - To deselect all properties, click **None**.
5. Click **Delete**.

   A confirmation message displays.
6. Click **OK**.

   The property or properties are removed from the list.

The subscriber entity state properties are deleted.

About Pool Profiles

A pool profile groups information (such as, billing day, tier, and entitlements) for a subscriber to provide services to families and businesses.

Subscribers who share a pool profile are members of the same pooled quota group. Pool members have a common pool profile, pool quota usage, pool state, and pool dynamic quota.

The CMP system allows you to perform the following pool profile management actions:

- Querying by Pool ID
- Adding a Member to a Basic Pooled Quota Group
- Modifying a Pool Profile
- Deleting a Pool Profile

Querying by Pool ID

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

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select **Pool ID** in the **Key Type** list, enter a **Key String** and click **Search**.

   The Pool Group Quota Profile page opens with the search results. The following tabs display:
   - **Pool Profile**
   - **Pool Quota**
   - **Pool State**
3. You can select the **Modify**, **Delete**, or **Back to Search Page** options.

Adding a Member to a Basic Pooled Quota Group

You can use pooled quota groups to create a shared pool profile for multiple subscribers. A basic pool can include up to 25 subscribers as pooled quota group members. You can add members or modify the membership list from the CMP when the pool is a basic pool.

> **Note:**
>
> The **Modify Membership** button is hidden when the pool is an enterprise pool. Pooling information for enterprise pools, including pool membership, is provisioned from the SPR.

To add a member to a pooled quota group:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Use the **Search** function to find the pool quota group.

   a. Select the **Data Source Primary Diameter Identity**.

      This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.

   b. Select **Pool ID** as the **Key Type**.

   c. In the **Key String** field, enter the Pool ID of the pool quota group.

      The Pool ID must match exactly; partial or wildcard searching is not supported.

   d. Click **Search**.

   The Pool Profile page opens.

3. On the Pool Profile tab, click **Modify Membership Information**.

   The Pool Profile Configuration page opens.

4. In the **Membership Information** section of the page, enter the following:

   a. **Key Type**—The type of subscriber identifier. You can select one of the following:

      - **E.164 (MSISDN)**
        Mobile Station International Subscriber Directory Number.
      - **IMSI**
        International Mobile Subscriber Identity.
      - **NAI**
        Network Access Identifier.

   b. **Key String**—Enter the key string for the subscriber.

      > **Note:**
      >
      > When associating a subscriber, you must enter the subscriber **Key String**.

   c. Click **Add** to add the subscriber to the pooled quota group.

   A confirmation message is displayed.

   > **Note:**
   >
   > Click **Cancel** to return to the Pool Profile page.

5. Click **Save**.

The member is added to the pooled quota group.

Modifying a Pool Profile

You can modify a pool profile to make changes to the subscriber information or membership information.
To modify a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of the **Pool ID.**

   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.

   The Pool Profile page opens with Pool Profile as the default.
4. Click **Modify**.

   The Subscriber Profile Configuration page opens.
5. Modify any of the field information.
6. Click **Save**.

The pool profile is modified.

Deleting a Pool Profile

To delete a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID.**

   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.

   The Pool Profile page opens with **Pool Profile** as the default.
4. Click **Delete**.

   A confirmation message displays.
5. Click **OK**.

The pool profile is deleted.

About Pool Quota Profiles

A pool quota profile sets usage quota parameters. This allows the CMP system to track and display usage threshold events. Policies may refer to a pool quota profile. Refer to the *Policy Wizard Reference* for additional information.

The CMP system allows you to perform the following pool quota profile management actions:

- Creating a Pool Quota Profile
- Modifying a Pool Quota Profile

- Deleting a Pool Quota Profile

Creating a Pool Quota Profile

The CMP system uses a pool quota profile for tracking and displaying usage threshold events. To create a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID.**
3. Enter a **Key String** and click **Search**.

   The Pool Profile page opens.
4. Click **Pool Quota Profile**.

   The Quota Usage section displays.
5. Click **Create**.
6. Enter the following:
   a. **Name**—Select the name of the pool state.
   b. **Type**—Select the quota being assigned to the pool:
      - **quota** (plan)
      - **pass**
      - **top-up**
      - **roll-over**
      - **roll-over-def**

      > **Note:**
      >
      > If you select **roll-over-def**, rollover units are consumed before top-up units unless the highest priority top-up expires in the next 24 hours.

   c. **Time** (seconds)—The amount of time attributed to the quota in seconds.
   d. **Total Volume** (bytes)—The amount of volume attributed to a length of time.
   e. **Upstream Volume** (bytes)—Traffic from the handset (or other device) to the network.
   f. **Downstream Volume** (bytes)—Traffic directed to the handset or other device.
   g. **Service Specific Event**—Tracks text information.
   h. **Next Reset Time**—The reset date and time of the subscriber or pool quota usage.

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

7. Click **Save**.

The pool quota profile is created.

Modifying a Pool Quota Profile

To make changes to the subscriber information or membership information, modify the pool quota profile.
To modify a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID.**
3. Enter a **Key String** and click **Search**.

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

4. Click **Pool Quota Profile**.

   The Pool Quota Profile view displays.

5. Select the profile that you want to modify.
6. Modify any of the fields.

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

7. Click **Save**.

The pool quota profile is modified.

Deleting a Pool Quota Profile

To delete a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID.**

   The Data Source Primary Diameter Identity and Key Type are selected.

3. Enter a **Key String** and click **Search**.

   The Pool Profile page opens.

4. Click **Pool Quota Profile**.

   The Quota Usage section displays.

5. Select the name of the profile you want to delete and click **Delete**.

   A confirmation message displays.

6. Click **OK**.

   The selected properties are deleted.

About Pool States

When using an Sh ProfileV3 or ProfileV4 data source, you can use Pool States. A pool state consists of a name-value pair that is associated with the quota pool. For more information, see Configuring MPE Protocol Options.

The CMP system allows you to perform the following pool state actions:

- Creating a Pool State
- Modifying a Pool State
- Deleting a Pool State

Creating a Pool State

When using an Sh ProfileV3 or ProfileV4 data source, you can create a pool state. For more information, see Configuring MPE Protocol Options.
To create a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.

   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.

   The Subscriber Profile page opens.
4. Select the **Pool State** tab.

   The Pool Profile page opens.
5. Click **Create**.

   The Create Property section displays.
6. Enter the following:
   - **Name** — The name of the pool state.
   - **Value** — The value can be any string, for example, `ProfileV3` or `ProfileV4`.
7. Click **Save**.

The pool state is created. The Pool Entity State Properties section displays the **Pool Quota Group Key Fields** and the **Pool ID**.

Modifying a Pool State

If you want to make changes to the subscriber information or membership information, you can modify the pool state.
To modify a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity** and the **Key Type** of **Pool ID**.

   The Data Source Primary Diameter Identity and Key Type are selected.

3. Enter a **Key String** and click **Search**.

   The Subscriber Profile page opens.
4. Select the **Pool State** tab.

   The **Pool Entity State Properties** section displays.
5. Click the **Name** of the pool state that you want to modify.

   The **Modify Property** section displays.
6. The **Name** and **Value** fields are displayed but you can only modify the **Value** field.
7. Modify the **Value** field.
8. Click **Save**.

The system saves the modified pool state.

Deleting a Pool State

To delete a pool state:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.

   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String** and click **Search**.

   The Subscriber Profile page opens.
4. Select the **Pool State** tab.

   The **Pool Entity State Properties** section is displayed.
5. Select a check box for one or more properties to delete and click **Delete**.

The specified properties are deleted.

About Subscriber Dynamic Quotas

A subscriber dynamic quota allows subscriber access based on time-limited subscriber quotas.

The CMP system allows you to perform the following dynamic quota management actions:

- Viewing Subscriber Dynamic Quota Information
- Adding a Subscriber Dynamic Quota Category
- Modifying a Subscriber Dynamic Quota Category
- Resetting a Subscriber Dynamic Quota
- Deleting a Subscriber Dynamic Quota Category

Adding a Subscriber Dynamic Quota Category

To add a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Find the subscriber profile you want to view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the Dynamic Quota tab.

   The Dynamic Quota page is displayed.

4. Click **Create**.

   The Create Subscriber Dynamic Quota page opens. If you exceed 10 dynamic quotas, you are prompted with a message to add more; click **Yes** to continue, or **No** to stop.

5. Enter the following information:

   - **InstanceID**
     A unique identifier.

     > **Note:**
     >
     > Do not enter a colon (:) as part of this identifier.

   - **Name**
     Select the name of a dynamic quota.
   - **Description/Location**
     Free-form text.
   - **Type**
     Select the type of quota defined in the CMP system. You can select **pass** or **top-up**.
   - **Priority**
     Defines the order in which the dynamic quota is processed.

     The range is -32768 to 32767 (Max 16-bit short). Higher priority passes are used before lower priority passes. A higher number indicates a higher priority.
   - **Initial Time Limit (seconds)**
     The initial value for time units granted by the dynamic quota.
   - **Initial Total Volume Limit (bytes)**
     The initial value for total volume units granted by the dynamic quota.

     The valid range is -2^{63} to 2^{63}– 1 (64-bit value).
   - **Initial Upstream Volume Limit (bytes)**
     Enter a value, in bytes, to track upstream bandwidth volume consumption.

     The valid range is -2^{63} to 2^{63}– 1 (64-bit value).
   - **Initial Downstream Volume Limit (bytes)**
     Enter a value, in bytes, to track downstream bandwidth volume consumption.

     The valid range is -2^{63} to 2^{63}– 1 (64-bit value).
   - **Initial Service Specific Limit (events)**
     Enter a value representing service-specific resource consumption.

     The valid range is -2^{63} to 2^{63}– 1 (64-bit value).
   - **Purchase Time**
     The date and time that the dynamic quota was purchased.

     For the **Purchase Time**, **Active Time**, and **Expire Time** fields, use the format *yyyy-mm-dd*T*hh*:*mm*:*ss*[*Z*] (for example, `2011-11-01T00:00:01-5:00`). Alternatively, click on the calendar icon, and from the window that opens, select a date, enter a time, and optionally select a UTC offset (time zone). Click **OK**.

- **Active Time**
  The time period during when the dynamic quota can be used.
- **Expire Time**
  The date and time the dynamic quota expires. If undefined, the dynamic quota does not expire.
- **Duration (seconds)**
  The amount of time after the first use that the dynamic quota expires.
- **Interim Reporting Interval (seconds)**
  If the units are granted from a top-up, then the **Interim Reporting Interval** is:
  - The number of seconds until the next quota reset
  - The interim reporting interval defined for the plan
  - The time until the top-up expires
  - The time until a higher priority top-up becomes active

  If the units are granted from a pass, then the **Interim Reporting Interval** is:
  - The interim reporting interval defined for the pass
  - The time until the pass expires
  - The earliest time that the current time will be outside the valid time period (if defined)
  - The time until a higher priority pass becomes active

6. Click **Save**.

The subscriber quota is defined and the page displays the message `Quota created successfully`.

Viewing Subscriber Dynamic Quota Information

To view the dynamic quota information associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Search for the subscriber profile you want to view.

   The Subscriber Profile page opens. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **Dynamic Quota** tab.

   The Dynamic Quota Usage page opens. The page provides the following information:

   - **Name**
     Name of the dynamic quota.
   - **Time Limit**
     Time limit, in seconds, defined for the dynamic quota.
   - **Total Volume Limit**
     Volume limit, in bytes, defined for the dynamic quota.
   - **Upstream Volume Limit**
     Upstream volume limit, in bytes, defined for the dynamic quota.

- **Downstream Volume Limit**
  Downstream volume limit, in bytes, defined for the dynamic quota.
- **Service Specific Event Limit**
  Resource consumption limit defined for the dynamic quota.
- **Purchase Time**
  The time the dynamic quota was purchased.
- **Active Time**
  The time that the dynamic quota is in effect.
- **Expire Time**
  The time that the dynamic quota expires.
- **Type**
  Defines whether the dynamic quota is a pass or top-up.
- **Priority**Defines the order in which the dynamic quota is processed.
- **InstanceId**
  A unique identifier for the dynamic quota.

4. Click **Back to Search Page**.

You have viewed the subscriber dynamic quota information.

Modifying a Subscriber Dynamic Quota Category

To modify a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **Dynamic Quota** tab.

   The Dynamic Quota page is displayed.
4. Select the name of the quota you want to modify.

   The Modify Subscriber Dynamic Quota page opens, displaying information about the dynamic quota.
5. Modify subscriber quota information.

   For a description of the fields contained on this page, see Adding a Subscriber Dynamic Quota Category.
6. Click **Save**.

The subscriber dynamic quota category is modified.

Resetting a Subscriber Dynamic Quota

If you reset a dynamic quota, then the time, total volume, upstream volume, downstream volume and service specific events limit values that were provisioned in the **SPR>Profile Data** option are replaced with the initial values that were configured in the **Quota Profiles** or **Quota Conventions** option.

To reset a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **Dynamic Quota** tab.

   The Dynamic Quota page is displayed.
4. Select the quotas you want to reset.

   To select all dynamic quotas, click **All**. To deselect all dynamic quotas, click **None.**
5. Click **Reset**.

   A confirmation message displays.
6. Click **Ok** to reset the values.
7. Click **Save**.

The subscriber dynamic quota values are reset.

Deleting a Subscriber Dynamic Quota Category

To delete a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to modify.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **Dynamic Quota** tab.

   The Dynamic Quota page is displayed.
4. In the list of quotas, use the check boxes to select the dynamic quotas you want to delete.

   To select all dynamic quotas, click **All**. To deselect all dynamic quotas, click **None**.
5. Click **Delete**.

   A confirmation message displays.
6. Click **OK**.

The subscriber dynamic quota categories are deleted.

About Subscriber Services

A subscriber can be given access according to one or more service packages. A subscriber service is composed of a service code, start date/time, end date/time, and so on.

The CMP system allows you to perform the following service actions:

- Viewing Defined Services
- Adding a Service
- Modifying a Service

- Deleting a Service

Adding a Service

To add a service to 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 view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **Service** tab.

   The Service information appears in the work area.

4. Click **Create**.

   The Service Info page opens.

5. Enter the following information:

   a. **Service Code** (required)—The code for the service. A service code is a numeric string that is 1 to 32 numbers in length.

   b. **User Billing Type** — The type of billing. Enter a value of 0 (online charging) or 1 (offline charging). The default value is 1.

   c. **Start Date** — The start date and time for the service. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.

   d. **End Date** — The ending date and time for the service. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.

   e. **Usage State** — Indicates if the package volume should be exceeded. Enter a value of 1 (do not exceed) or 2 (exceed). The default value is 1.

   f. **Operate Time** (required)—The length of time the package is available. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.

   g. **Custom*x*** — 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.

6. Click **Save**.

The service is defined.

Viewing Defined Services

To view defined services:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select the subscriber profile you want to view.

Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **Service** tab.

   The list of defined services displays in the work area.

4. Click **Back to Search Page**.

Modifying a Service

To modify a defined service:

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 **Service** tab.

   The Service information appears in the work area.

4. Locate the service in the list and click the Service Code.

   The Service Info pages opens.

5. Click **Modify**.

   The fields become editable.

6. Modify service information.

   For a description of the fields contained on this page, see Adding a Service.

7. Click **Save**.

The service is updated.

Deleting a Service

To delete a defined services:

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 **Service** tab.

   The list of defines service appears in the work area.

4. Select one or more services using the checkbox to the left of the service.

5. Click **Delete**.

   A confirmation displays.

6. Click **Save**.

The selections are deleted.

About User Session Policies

A subscriber may be allowed access according to one or more session policies. A user session policy is composed of a policy code, start date/time, end date/time, and so on.

The CMP system allows you to perform the following user session policy management actions:

- Viewing a Defined User Session Policy
- Adding a User Session Policy
- Modifying a User Session Policy
- Deleting a User Session Policy

Adding a User Session Policy

To add a user session policy to 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 view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **User Session Policy** tab.

   The Session information appears in the work area.

4. Click **Create**.

   The User Session Policy Info page opens.

5. Enter the following information:

   a. **Policy Code** (required)—The code for the policy. A policy code is a numeric string that is 1 to 32 numbers in length.

   b. **Notification Cycle** — The notification cycle of the subscribed policy. Valid options are:

      - **0**— day
      - **1**—week
      - **2**—double week
      - **3**—month
      - **4**—double month
      - **5**—season
      - **6**—half year
      - **7**—billing cycle

   c. **Terminal Type** — The available terminal type. A terminal type is a alphanumeric string that is 1 to 32 characters in length.

   d. **Start Date** — The start date and time for the service. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.

   e. **End Date** — The ending date and time for the service. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.
   f. **Operate Time** (required)—The length of time the package is available. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.
   g. **Custom*x*** — 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.
6. Click **Save**.

The user session policy is defined.

Viewing a Defined User Session Policy

To view a defined user session policy:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.
2. Select the subscriber profile you want to view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **User Session Policy** tab.

   The list of defined user sessions displays in the work area.
4. Click **Back to Search Page**.

Modifying a User Session Policy

To modify a defined user session policy:

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 **User Session Policy** tab.

   The Service information appears in the work area.
4. Locate the service in the list and click the Service Code.

   The UserSession Policy pages opens.
5. Click **Modify**.

   The fields become editable.
6. Modify user session policy information.

   For a description of the fields contained on this page, see Adding a User Session Policy.
7. Click **Save**.

The user session policy is updated.

Deleting a User Session Policy

To delete a defined user session policy:

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 **User Session Policy** tab.

   The list of defines service appears in the work area.
4. Select one or more user session policy using the checkbox to the left of the service.
5. Click **Delete**.

   A confirmation displays.
6. Click **OK** to delete the items.

The selections are deleted.

About User Location Policies

A subscriber may be allowed access according to one or more user location policies. A user location policy is composed of a code, service or policy code, user location (for example, area code), operation date/time, and so on.

The CMP system allows you to perform the following user location management actions:

- Viewing Defined User Locations
- Adding a User Location
- Modifying a User Location
- Deleting a User Location

Adding a User Location

To add a user location policy to 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 view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)
3. Select the **User Location** tab.

   The User Location information displays in the work area.
4. Click **Create**.

   The User Location page opens.
5. Enter the following information:

   a. **Code** (required)—The code for the policy. A policy code is a numeric string that is 1 to 32 numbers in length.
   b. **Code Type**—The service code or policy code for the user location.
   c. **User Location**—The area code for the network access.
   d. **Operate Time** (required)—The length of time the package is available. Specified in the format of *yyyymmddhhmmss*, where *hh* is a 24 hour format. This field is automatically filled with the current time and date.
   e. **Custom*x*** — 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.

6. Click **Save**.

The user location is defined.

Viewing Defined User Locations

To view defined user locations:

1. From the **SPR** section of the navigation pane, select **Profile Data**.

   The Subscriber Profile Administration page opens.

2. Select the subscriber profile you want to view.

   Profile information is displayed. (See Finding a Subscriber Profile for information on finding a subscriber profile.)

3. Select the **User Location** tab.

   The list of defined user locations displays in the work area.

4. Click **Back to Search Page**.

Modifying a User Location

To modify a defined user location:

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 **User Location** tab.

   The User Location information appears in the work area.

4. Locate the service in the list and click the Service Code.

   The UserSession Policy pages opens.

5. Click **Modify**.

   The fields become editable.

6. Modify user location information.

   For a description of the fields contained on this page, see Adding a User Location.

7. Click **Save**.

The user location is updated.

Deleting a User Location

To delete a defined user location:

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 **User Location** tab.

   The list of defined user locations are displayed in the work area.

4. Select one or more user location using the checkbox to the left of the location.
5. Click **Delete**.

   A confirmation displays.

6. Click **OK** to delete the items.

The user locations are deleted.

13 Managing Subscribers

This chapter describes how to create and manage subscriber tiers and quota usage within the Configuration Management Platform system.

> **Note:**
>
> The actual options you see depend on whether or not your Configuration Management Platform system is configured to operate with a Subscriber Profile Repository. For information about the Oracle Communications Subscriber Database Management product, see the Subscriber Database Management documentation. For information about the Oracle Communications User Data Repository product, see the User Data Repository documentation.

Creating a Subscriber Tier

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

1. From the **Subscriber** section of the navigation pane, select **Tiers**.

   The content tree displays the **Tiers** folder.
2. Select the **Tiers** folder.

   The Tier Administration page opens.
3. Click **Create Tier**.

   The New Tier page opens.
4. Enter information as follows:
   1. **Name** (required) — Name of the tier.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
   2. **Description/Location** — Free-form text.

      Enter up to 250 characters.
   3. **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.
   4. **Upstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the upstream direction in bits per second.

      You can enter a value followed by M or G; for example, 10M for 10 megabits per second.
5. Click **Save**.

You can now use the tier in policy rules.

Deleting a Tier

To delete a tier:

1. From the **Subscriber** section of the navigation pane, select **Tiers**.

   The **Tiers** folder appears in the content tree.

2. Delete the tier using one of the following methods:

   - From the work area, click 🗑 (trash can icon), located to the right of the tier.
   - From the content tree, select the tier and click **Delete**.

   A confirmation message displays.

3. Click **OK**.

You have deleted the tier.

Creating an Entitlement

Entitlements are defined within a Subscriber Profile Repository. You can define entitlement names in the CMP database. After you define entitlements, you can use them in policy rules. To create an entitlement:

1. From the **Subscriber** section of the navigation pane, select **Entitlements**.

   The content tree displays the **Entitlements** folder.

2. Select the **Entitlements** folder.

   The Entitlement Administration page opens.

3. Click **Create Entitlement**.

   The New Entitlement page opens.

4. Enter information as follows:

   a. **Entitlement ID** (required) — Name of the tier.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

   b. **Description/Location** — Free-form text.

      Enter up to 250 characters.

5. Click **Save**.

The entitlement is created in the CMP database, and you can now refer to it in a policy rule.

Deleting an Entitlement

To delete an entitlement:

1. From the **Subscriber** section of the navigation pane, select **Entitlements**.

   The **Entitlements** folder appears in the content tree, and a list of defined entitlements appears in the work area.

2. Delete the entitlement using one of the following methods:

- From the work area, click 🗑 (trash can icon), located to the right of the entitlement you wish to delete.
- From the content tree, select the entitlement and click **Delete**.

A confirmation message displays.

3. Click **OK**.

The entitlement is deleted.

Displaying Static Session and Binding Data for a Subscriber

You can display static session and binding data for a specific subscriber from the Policy Management device that is managing the session. Depending on how the data is indexed on the device, you can search for a subscriber by IMSI, MSISDN, IP address, or NAI. You can also delete obsolete sessions.

> **Note:**
>
> This function is not supported by Policy Management devices before release 7.5.

To display the static session and binding data for a subscriber:

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

   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. Select the Policy Management device managing the session you want to view.

   The Policy Server Administration page opens in the work area.
3. Select the **Session Viewer** tab.

   The **Session Viewer** page opens.
4. Enter search information as follows:

   a. **Identifier type** (required)—Select one of the following identifier types:

      - **NAI** (default)
      - **E.164(MSISDN)**
      - **IMSI**
      - **Diameter Session ID**
      - **Diameter IPv4Address**
      - **Diameter IPv6Prefix**

      The identifier types you can specify are determined by the configuration of the Policy Management device. For example, if the **Index By NAI** setting is not specified on the device, then you cannot select **NAI**.

      > **Note:**
      >
      > When searching primary Gx sessions by IPv6 prefix, only 64-bit masks are supported.

   b. **Identifier name**—Free-form text.

      Enter up to 250 characters.

   c. Select **Show advanced details** to view the detailed (that is, verbose) results.

5. Click **Search**.

   If sessions are available for the subscriber, Subscriber Session Data page appears. Figure 13-1 shows an example. If the subscriber has correlated secondary sessions, the correlated secondary session data is also displayed.

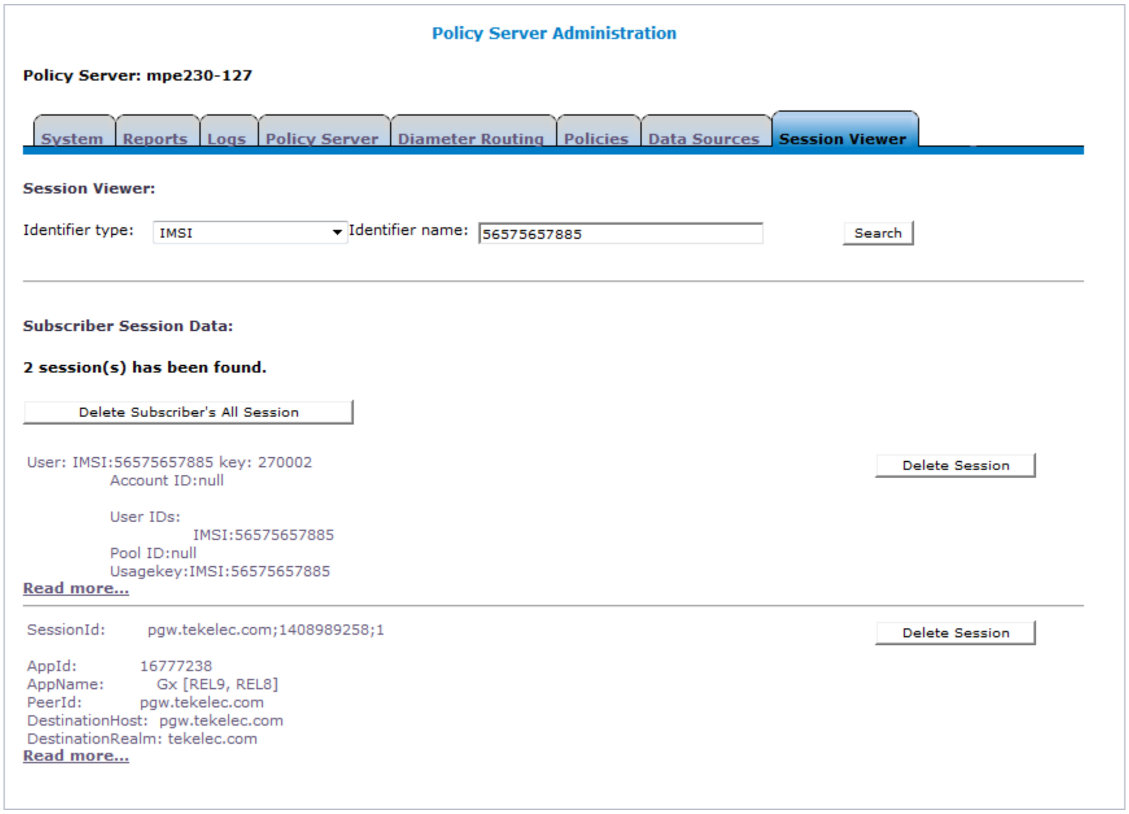
If you are viewing subscriber data from a stateful MRA system, subscriber binding data is displayed, including an identifier for the MPE device handling sessions for that subscriber. If that MPE device is managed by this CMP system, you can click the identifier to view session data from the MPE device.

> **Note:**
>
> If an external system generates data that, when translated to ASCII, creates illegal characters, they are displayed by the Session Viewer as question marks (?).

For each session displayed from an MPE device, you can click **Delete Session** to delete the session. For each subscriber displayed from an MPE device, you can click **Delete Subscriber's All Session** to delete all sessions for that subscriber. For each session binding displayed from an MRA device, you can click **Delete Binding** to delete the binding. This deletes the record in the appropriate database.

> **Caution:**
>
> Only obsolete sessions should be deleted. If you delete an active session, there is no signal to any associated gateways or external network elements.

Figure 13-1   Session Viewer Page



Policy Server: mpe230-127

Session Viewer:

Identifier type: IMSI Identifier name: 56575657885

Subscriber Session Data:

2 session(s) has been found.

```
User: IMSI:56575657885 key: 270002
          Account ID:null

          User IDs:
                    IMSI:56575657885
          Pool ID:null
          Usagekey:IMSI:56575657885
```

```
SessionId:      pgw.tekelec.com;1408989258;1

AppId:          16777238
AppName:            Gx [REL9, REL8]
PeerId:         pgw.tekelec.com
DestinationHost:  pgw.tekelec.com
DestinationRealm: tekelec.com
```

14 Managing Policy Front End Devices

This chapter describes how to define and manage Policy Front End (also known as MRA) devices in the CMP system.

For an overview of the MRA see Multi-Protocol Routing Agent Devices.

> **Note:**
>
> For more information on using MRA servers, refer to the *Policy Front End Wireless User's Guide*.

15 System-Wide Reports

This chapter describes the reports available on the function of Policy Management systems in your network. Reports can display platform alarms, network protocol events, and Policy Management application errors.

KPI Dashboard

The KPI Dashboard provides a multi-site system-level summary of performance and operational health indicators. The display includes indicators for:

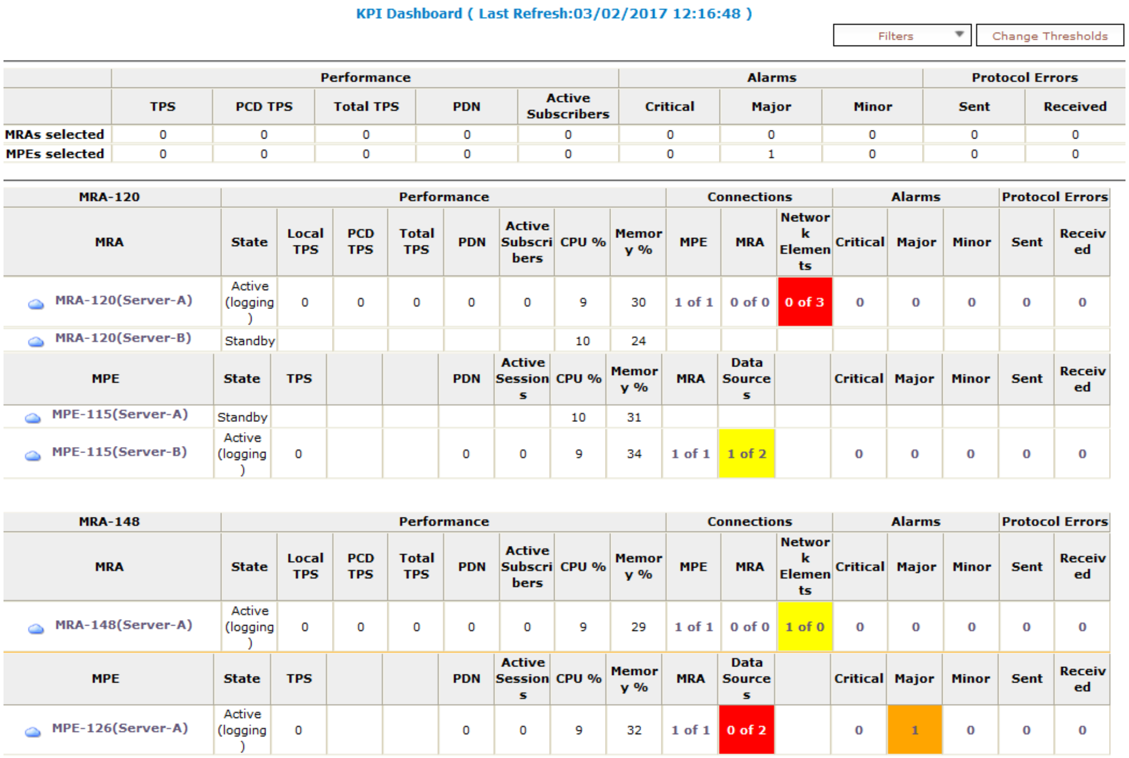
- Offered load (transaction rate)
- System capacity (counters for active sessions)
- Inter-system connectivity
- Resource utilization (memory, CPU)
- System status
- Alarms
- Protocol errors

The KPI dashboard displays the indicators for all the systems on a single page, with each MRA KPIs in a separate table when MRA systems are managed by the CMP system or with all MPE KPIs in one table when MRA systems are not managed by the CMP system (that is, an MPE-only deployment). Each row within a table represents a single system (either an MPE or MRA server). The table cells are rendered using a color scheme to highlight areas of concern that is well adopted by the telecommunication industry. The table contents are periodically refreshed every 10 seconds; this time period is not configurable. The color changing thresholds are user configurable.

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

Figure 15-1 illustrates the dashboard’s contents when MRA systems are managed by the CMP system.

Figure 15-1 Example of KPI Dashboard with MRA Devices Managed by the CMP System



KPI Dashboard (Last Refresh:03/02/2017 12:16:48)

	Performance					Alarms			Protocol Errors	
	TPS	PCD TPS	Total TPS	PDN	Active Subscribers	Critical	Major	Minor	Sent	Received
MRAs selected	0	0	0	0	0	0	0	0	0	0
MPEs selected	0	0	0	0	0	0	1	0	0	0

MRA-120	Performance								Connections			Alarms			Protocol Errors	
MRA	State	Local TPS	PCD TPS	Total TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
MRA-120(Server-A)	Active (logging)	0	0	0	0	0	9	30	1 of 1	0 of 0	0 of 3	0	0	0	0	0
MRA-120(Server-B)	Standby						10	24								
MPE	State	TPS			PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
MPE-115(Server-A)	Standby						10	31								
MPE-115(Server-B)	Active (logging)	0			0	0	9	34	1 of 1	1 of 2		0	0	0	0	0

MRA-148	Performance								Connections			Alarms			Protocol Errors	
MRA	State	Local TPS	PCD TPS	Total TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
MRA-148(Server-A)	Active (logging)	0	0	0	0	0	9	29	1 of 1	0 of 0	1 of 0	0	0	0	0	0
MPE	State	TPS			PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
MPE-126(Server-A)	Active (logging)	0			0	0	9	32	1 of 1	0 of 2		0	1	0	0	0

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
- PCD TPS
- Total TPS
- PDN
- Active Subscribers
- Critical Alarm Count
- Major Alarm Count
- Minor Alarm Count
- Protocol Errors Sent
- Protocol Errors Received

Note:

Isolated MPE devices are not included in the aggregation counts.

When there are no MRA devices managed by the CMP system, the displayed headings are:

- Name of MPE
- Performance:
  - State
  - TPS
  - PDN
  - Active Sessions
  - CPU %
  - Memory %
- Connections
  - Data Sources
  - Network Elements
- Alarms
  - Critical
  - Major
  - Minor
- Protocol Errors
  - Sent
  - Received

In the top right corner there is a **Change Thresholds** button that allows you to change threshold settings used to determine cell coloring. When MRA devices are managed by the CMP system, a button on the top left corner lists each of the MRA devices with a check box that allows the user to enable/disable the table for that MRA device.

Individual servers are identified by name and the order in which they were defined within their cluster (Server-A, Server-B, Server-C). If any of these are set to Reverse Site Preference, then an “R” will appear by the server's State. For the standby or spare server, several columns are not populated (since those servers are not active); the only columns that contain data are: Status, CPU%, and Memory%. For Connections, Alarms, and Protocol Errors, the column's information is a hyperlink that will open a more detailed report.

A cloud icon (☁) indicates that the server is executing on a virtual machine.

If a monitored system is unreachable, or if the data is unavailable for some reason, then the status is set to `Off-line` and the values in all the associated columns is cleared. In this situation, the entire row is displayed with the error color (red). If a monitored system does not support KPI retrieval then the status is set to `N/A` and the values in all the associated columns are cleared. No coloring is applied.

The columns that display information in the form of X (Y%) (e.g. TPS and PDN Connections”/ “Sessions) correspond to the following: X represents the actual numeric value and Y represents the % of rated system capacity that is consumed. If the system is executing on a virtual machine, values for TPS, Sessions, and Active Subscribers are only calculated if capacity values are explicitly set. See Configuring Advanced Device Settings for more information.

The columns that display connection counts are displayed in the form X of Y where X is the current number of connections and Y is the configured number of connections. When X and Y are not the same, the column uses the warning color to indicate a connectivity issue, unless X is 0, in which case the error color is displayed.

The Alarm and Protocol Errors columns display the number of current events. If there are any Critical or Major alarms, then these cells will be colored red or yellow, respectively.

> **Note:**
>
> To learn more about an alarm and how to resolve it, refer to the *Troubleshooting Reference* for this release.

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

Mapping Display to KPIs

The following tables explain how each of the columns in the KPI dashboard are mapped to a specific statistic in the KPI statistics. On the initial KPI Dashboard window, KPIs for each MRA and MPE device are shown. Since the tables contain row entries for the active, standby and spare servers (if georedundancy is configured), the mapping is described for all three servers. Table 15-1 shows the mappings for MRA devices; Table 15-2 shows the mappings for MPE devices when the MRA devices are managed by the CMP system; and Table 15-3 shows the mappings for MPE devices when the MRA devices are not managed by the CMP system.

Table 15-1 KPI Definitions for MRA Devices

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby and spare server (spare only shows Status, CPU % and Memory%)**
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	None
Active Subscribers	CurrentMRABindingCount and CurrentMRABindingPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
MPE Connections	A value in the form X of Y, where: X is CurrentMPEConnectionCount Y is ConfiguredMPEConnectionCount	None
MRA Connections	A value in the form `X of Y`, where: `X` is CurrentMRAConnectionCount `Y` is ConfiguredMRAConnectionCount	None

Table 15-1 (Cont.) KPI Definitions for MRA Devices

KPI Dashboard Column	Mapping to Statistics	
	Active server	Standby and spare server (spare only shows Status, CPU % and Memory%)
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 15-2 KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	Standby server
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	None
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

Table 15-2 (Cont.) KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Table 15-3 KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
Name	Not derived from statistics	Not derived from statistics
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
Active Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
SPR Connections	A value in the form `X of Y`, where: `X` is CurrentSPRConnectionCount `Y` is ConfiguredSPRConnectionCount	None
Network Element Connections	A value in the form `X of Y`, where: `X` is CurrentConnectedNECount `Y` is ConfiguredConnectedNECount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Clicking on an MRA or MPE name opens the **Reports** tab. See the **Reports** tab for the device for details on reports.

Mapping Reports Display to KPIs

From the KPI Dashboard, you can click any MPE or MRA system shown to open the Reports page. From there, a variety of statistics and measurements can be viewed. In the following tables, these statistics are mapped to their names as they appear in OSSI XML output.

- Table 15-4
- Table 15-5
- Table 15-6
- Table 15-7
- Table 15-8
- Table 15-9
- Table 15-10
- Table 15-11
- Table 15-12
- Table 15-13
- Table 15-14
- Table 15-15
- Table 15-16
- Table 15-17
- Table 15-18
- Table 15-19
- Table 15-20
- Table 15-21
- Table 15-22
- Table 15-23
- Table 15-24
- Table 15-25

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

Table 15-4 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

Table 15-4 (Cont.) Policy Statistics

Display	MPE	MRA	Name
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 15-5 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 15-6 Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
AAR messages received/sent	Y	Y	AAR Recv Count\AAR Send Count
AAR Initial messages received/sent	Y	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR Modification messages received/sent	Y	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages received/ sent	Y	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages received/sent	Y	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages received/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count
ASA success messages received/ sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages received/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/ sent	Y	Y	RAA Recv Success Count\RAA Send Success Count

Table 15-6 (Cont.) Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages received/sent	Y	Y	STR Recv Count\STR Send Count
STR messages timeout	Y	Y	STR Timeout Count
STA success messages received/ sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages received/sent	Y	Y	STA Recv Failure Count\STA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Cleanup ASA received	Y	Y	ASA Received Count
Cleanup ASR sent	Y	Y	ASR Sent Count
Current number of active sponsored sessions	Y	N	Current Sponsored Session Count
Max sponsored active sessions	Y	N	Max Sponsored Session Count
Current number of active sponsors	Y	N	Current Sponsor Count
Max number of sponsors	Y	N	Max Sponsor Count
Current number of active service providers	Y	N	Current Service Provider Count
Max number of service providers	Y	N	Max Service Provider Count
Currently active emergency sessions	Y	N	Current Emergency Session Count
Max active emergency sessions	Y	N	Max Active Emergency Session Count

Table 15-7 Diameter AF Peer Stats (in Diameter AF Stats window)

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

Table 15-8 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

Table 15-8 (Cont.) Diameter Policy Charging Enforcement Function (PCEF) Statistics

Display	MPE	MRA	Name
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Currently active emergency sessions	Y	N	Current Emergency Session Count
Max active emergency sessions	Y	N	Max Active Emergency Session Count

Table 15-9 Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Connections	N	Y	Conn Count
Currently OK peers	N	Y	Peer Okay Count
Currently down/suspect/reopened peers	N	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	N	Y	Msg In Count\Msg Out Count
CCR messages sent/received	N	Y	CCR Recv Count\CCR Send Count
CCA success messages recd/sent	N	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count

Table 15-9 (Cont.) Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
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 15-10 Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

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

Table 15-10 (Cont.) Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

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	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter BBERF connections	Y	Y	

Table 15-11 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

Table 15-11 (Cont.) Diameter TDF Statistics

Display	MPE	MRA	Name
CCA-U failure messages received/ sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/ sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/ sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/ sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
TSR messages received/sent	Y	Y	
TSA success messages received/ sent	Y	Y	
TSA failure messages received/sent	Y	Y	
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter TDF connections	Y	Y	

Table 15-12 Diameter Sh / Sh Peer Statistics

Display	MPE	MRA	Name
Connections	Y	N	Conn Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Msg In Count\Msg Out Count
Messages retried due to error response	Y	N	
Messages retried due to response timeout	Y	N	
UDR messages received/sent	Y	N	UDR Messages Received Count\UDR Messages Sent Count
UDR messages timeout	Y	N	UDR Timeout Count
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages retried due to error response	Y	N	
UDR messages retried due to response timeout	Y	N	
UDR messages from session updates	Y	N	

Table 15-12 (Cont.) Diameter Sh / Sh Peer Statistics

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

Table 15-13 Diameter S9 Statistics

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

Table 15-13 (Cont.) Diameter S9 Statistics

Display	MPE	MRA	Name
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	N	CCR Messages Received Count\CCR Messages Sent Count
CCR messages timeout	Y	N	CCRTimeout Count
CCA success messages received/sent	Y	N	CCA Success Messages Received Count\CCA Success Messages Sent Count
CCA failure messages received/sent	Y	N	CCA Failure Messages Received Count\CCA Failure Messages Sent Count
CCR-I messages received/sent	Y	N	CCR-I Messages Received Count\CCR-I Messages Sent Count
CCR-I messages timeout	Y	N	CCRTimeout Count
CCA-I success messages received/sent	Y	N	CCA-I Success Messages Received Count\CCA-I Success Messages Sent Count
CCA-I failure messages received/sent	Y	N	CCA-I Failure Messages Received Count\CCA-I Failure Messages Sent Count
CCR-U messages received/sent	Y	N	CCR-U Messages Received Count\CCR-U Messages Sent Count
CCR-U messages timeout	Y	N	CCRUTimeout Count
CCA-U success messages received/sent	Y	N	CCA-U Success Messages Received Count\CCA-U Success Messages Sent Count
CCA-U failure messages received/sent	Y	N	CCA-U Failure Messages Received Count\CCA-U Failure Messages Sent Count
CCR-T messages received/sent	Y	N	CCR-T Messages Received Count\CCR-T Messages Sent Count
CCR-T messages timeout	Y	N	CCRTTimeout Count
CCA-T success messages received/sent	Y	N	CCA-T Success Messages Received Count\CCA-T Success Messages Sent Count
CCA-T failure messages received/sent	Y	N	CCA-T Failure Messages Received Count\CCA-T Failure Messages Sent Count
RAR messages received/sent	Y	N	RAR Messages Received Count\RAR Messages Sent Count
RAR messages timeout	Y	N	RARTimeout Count
RAA success messages received/sent	Y	N	RAA Success Messages Received Count\RAA Success Messages Sent Count
RAA failure messages received/sent	Y	N	RAA Failure Messages Received Count\RAA Failure Messages Sent Count
Currently active inbound sessions	Y	N	Active Inbound Sessions Count

Table 15-13 (Cont.) Diameter S9 Statistics

Display	MPE	MRA	Name
Max active inbound sessions	Y	N	Maximum Active Inbound Sessions Count
Currently active outbound sessions	Y	N	Active Outbound Sessions Count
Max active outbound sessions	Y	N	Maximum Active Outbound Sessions Count

Table 15-14 Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently okay peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
DBR messages received/sent	N	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	N	Y	DBRTimeout Count
DBA success messages received/sent	N	Y	DBARecv Success Count\DBASend Success Count
DBA failure messages received/sent	N	Y	DBARecv Failure Count\DBASend Failure Count
DBA message received/sent–binding found	N	Y	Binding Found Recv Count\Binding Found Send Count
DBA messages received/sent – binding not found	N	Y	Binding Not Found Recv Count\Binding Not Found Send Count
DBA messages received/sent – PCRF down	N	Y	Binding Found Pcrf Down Recd Count\ Binding Found Pcrf Down Send Count
DBA messages received/sent – all PCRFs down	N	Y	All Pcrfs Down Recv Count\ All Pcrfs Down Send Count
DBR-Q messages received/sent	N	Y	
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	

Table 15-14 (Cont.) Diameter Distributed Routing and Management Application (DRMA) Statistics

Display	MPE	MRA	Name
DBR-T messages received/sent	N	Y	
DBR-T messages timeout	N	Y	
DBA-T success messages received/sent	N	Y	
DBA-T failure messages received/ sent	N	Y	
DBR-S messages received/sent	N	Y	
DBR-S messages timeout	N	Y	
DBA-S success messages received/sent	N	Y	
DBA-S failure messages received/ sent	N	Y	
RUR messages received/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages received/ sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages received/ sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages received/sent	Y	Y	LNRRecv Count\ LNRSend Count
LNR messages timeout	Y	Y	LNRTimeout Count
LNA success messages received/ sent	Y	Y	LNARecv Success Count\ LNASend Success Count
LNA failure messages received/ sent	Y	Y	LNARecv Failure Count\ LNASend Failure Count
LSR messages received/sent	Y	Y	LSRRecv Count\ LSRSend Count
LSR messages timeout	Y	Y	LSRTimeout Count
LSA success messages received/ sent	Y	Y	LSARecv Success Count\ LSASend Success Count
LSA failure messages received/sent	Y	Y	LSARecv Failure Count\ LSASend Failure Count
SQR messages received/sent			
SQR messages timeout			
SQA messages received/sent			
SQA messages timeout			
Session found received/sent			
Session not found received/sent			
Diameter DRMA connections			

Note:

The statistics listed in Table 15-15 apply only to MRA devices.

Table 15-15 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 15-16 Diameter Sy Statistics

Display	MPE	MRA	Name
Connections	Y	N	Current Connections Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Messages In Count\Messages Out Count
SLR messages received/sent	Y	N	SLR Messages Received Count\SLR Messages Sent Count
SLR messages timeout	Y	N	SLRTimeout Count
SLA success messages received/ sent	Y	N	SLA Success Messages Received Count\SLA Success Messages Sent Count
SLA failure messages received/sent	Y	N	SLA Failure Messages Received Count\SLA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SMR Messages Sent Count
SNA success messages received/ sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/ sent	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
STR messages received/sent	Y	N	STR Messages Received Count\STR Messages Sent Count
STR messages timeout	Y	N	STRTimeout Count
STA success messages received/ sent	Y	N	STA Success Messages Received Count\STA Success Messages Sent Count

Table 15-16 (Cont.) Diameter Sy Statistics

Display	MPE	MRA	Name
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 15-17 RADIUS Statistics

Display	MPE	MRA	Name
Connections	Y	Y	
Total messages in/out	Y	Y	Messages In Count\ Messages Out Count
Total RADIUS messages received	Y	Y	
Total RADIUS messages send		Y	
Messages successfully decoded	Y	Y	
Messages dropped	Y	Y	
Total errors received	Y	Y	
Total errors sent	Y	Y	
Accounting Start sent	Y	Y	
Accounting Start received	Y	Y	Accounting Start Count
Accounting Stop sent	Y	Y	
Accounting Stop received	Y	Y	Accounting Stop Count
Accounting Stop received for unknown reason	Y	Y	
Accounting On sent	Y	Y	
Accounting On received	Y	Y	
Accounting Off sent	Y	Y	
Accounting Off received	Y	Y	
Accounting Response sent	Y	Y	Accounting Response Count
Accounting Response received	Y	Y	
Duplicates detected	Y	Y	Duplicated Message Count
Unknown/Unsupported messages received	Y	Y	
Interim Update Received	Y	Y	Accounting Update Count
Interim Update Received for unknown reason	Y	Y	
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

Table 15-17 (Cont.) RADIUS Statistics

Display	MPE	MRA	Name
COA-ACK received	Y	Y	CoA Success Count
COA-NAK sent	Y	Y	
COA-NAK received	Y	Y	CoA Nck Count
Parsed under 100m(icro)s	Y	Y	
Parsed under 200m(icro)s	Y	Y	
Parsed under 500m(icro)s	Y	Y	
Parsed under 1m(illi)s	Y	Y	
Parsed over 1m(illi)s	Y	Y	
Total Parse Time	Y	Y	
Average Parse Time	Y	Y	
Maximum Parse Time	Y	Y	
Unknown BNG. Message dropped	Y	Y	Unknown Gateway Request Count
Unknown BNG. Account Start dropped	Y	Y	
Unknown BNG. Account Stop dropped	Y	Y	
Unknown BNG. Interim Update dropped	Y	Y	
Stale sessions deleted	Y	Y	
Stale sessions deleted due to missed Interim Update	Y	Y	
Stale sessions deleted on Account-On or Account-Off	Y	Y	
Invalid subscriber key. Message dropped	Y	Y	
Invalid subscriber identifier specified. Message dropped	Y	Y	Unknown Subscriber Request Count

Table 15-18 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 15-18 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

Table 15-18 (Cont.) Diameter Latency Statistics

Display	MPE	MRA	Name
Avg Processing Time recd/sent (ms)	Y	Y	Avg Trans In Time\ Avg Trans Out Time
Processing Time recd/sent <time frame> (ms)	Y	Y	Processing Time [0-20] ms Processing Time [20-40] ms Processing Time [40-60] ms Processing Time [60-80] ms Processing Time [80-100] ms Processing Time [100-120] ms Processing Time [120-140] ms Processing Time [140-160] ms Processing Time [160-180] ms Processing Time [180-200] ms Processing Time [>200] ms

Table 15-19 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 15-20 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 15-21 Diameter Connection Error Statistics

Display	MPE	MRA	Name
Total errors received	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error received	Y	Y	Last Error In Time
Last time for total error sent	Y	Y	Last Error Out Time
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 15-22 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 15-23 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

Table 15-23 (Cont.) Sh Data Source Statistics

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

Table 15-23 (Cont.) Sh Data Source Statistics

Display	MPE	MRA	Name
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 15-24 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 15-25 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 MaxTransactionsPerSecond	Y	Y	For MPE, maximum transactions per second for the previous interval For MRA, maximum local transactions per second for the previous interval
Interval MaxPCDTransactionsPerSecond	N	Y	Maximum PCD transactions per second for the previous interval
Interval MaxMRATotalTransactionsPerSecond	N	Y	Maximum MRA total transactions per second for the previous interval
Interval MaxMRABinding Count	N	Y	Maximum MRA bindings for the previous interval
Interval MaxPDNConnectionCount	N	Y	Maximum PDN connections for the previous interval
Interval MaxSessionCount	Y	Y	Maximum session count for the previous interval

About Color Threshold Configuration

The KPI Dashboard Configuration dialog appears when you click the **Change Thresholds** button located in the top right corner of the KPI Dashboard.

The dialog shows the current settings for the specified parameters. You can modify the values and click **Save** to put the new values into effect. The values are saved so the next time the dashboard is opened it uses the new values.

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

Cancel
Closes the dialog without any changes to the KPI dashboard display.

Reset
Restores the values to their defaults. The TPS and Session limits for the Policy Management device are set to the officially supported rates for the current software release.

Subscriber Activity Log

The CMP system can perform real-time tracing of Gx, Rx, SOAP, TCP provisioning, and Sh protocol messages for a subscriber from multiple MPE devices.

Subscriber tracing is activated using a global CMP configuration setting (see Configuring the Activity Log). After activation, traces for subscriber diameter application messages are merged from all MPE devices in the network to the CMP system. Messages are selected for tracing based on a subscriber identification. Allowable subscriber ID types are:

- IMSI
- MSISDN_E.164
- NAI
- UE IPv4/IPv6 address
- Session ID

Up to 100 subscriber IDs can be configured in the subscriber configuration window. Up to 20 subscribers can be enabled for tracing.

> **Note:**
>
> Tracing subscriber activity affects performance.

After activating subscriber tracing, you can perform the following tasks using the **Subscriber Activity Log** option under **System Wide Reports**:

- View the subscriber activity log.
- Modify subscriber activity log settings. This task includes adding subscribers for tracing.

- View and modify the log backup settings.
- View the real-time subscriber activity log data display window.
- View the subscriber activity log history.

Subscriber Activity Log Limitations

The Subscriber Activity Log has the following limitations:

- Because of the additional processing required for the Subscriber Activity Log, only 20 subscribers can be enabled for logging, and only 10 subscribers can be viewed.
- There is also a limit to the overall amount of data that can be recorded by the system.
- Most MRA messages are not shown in the log because MRA messages do not have user IDs or bindings for a secondary session and cannot be traced.
- CCR-U is rejected by Diameter validation as an invalid message. There is no correlation between the established session and this message.
- For UDR/UDA and CCA-T, use NAI, E164, or IMSI , not Ipv4 or Ipv6.

Viewing a Subscriber Activity Log

To view the activity of a subscriber:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log page opens.
2. If there are no subscribers in the **Subscriber Identifier List**, add one or more subscribers. See Adding Subscriber Identifiers for information on adding subscribers.
3. In the **Subscriber Identifier List** section, click **View** for a subscriber.

   The log for the subscriber opens.

The workspace displays the trace data in real time for the selected subscriber.
The **Trace Time** field shows the start time of the real-time data trace. The **End Time** field shows the day and time when the log is set to stop. The **Description** field shows the first 50 characters of the description for the Subscriber Identifier. The full description displays in the real-time page view.

You can perform the following actions in this window:

- Select a specific time in the **Time Index** list to display messages that appear during a specific time period.
- Select a message type from the **Activity Type** list to filter messages in the window by message type. The message types are:
  - **All** (default)
  - **Gx**
  - **Rx**
  - **GxLite**
  - **Gxx**
  - **Gy**
  - **Sd**

  - **Sh**
  - **Sy**
  - **LDAP**
  - **Policy**
  - **MDF Provisioning**
  - **SPR Provisioning**
  - **MGW Provisioning**
- Select to enable or disable the **Automatic Scroll**. When enabled, the output scrolls in the window. When disabled, the window does not scroll, and new messages are added at the bottom of the window.
- Click **Pause** to temporarily keep messages from being added to the window. If selected, the button changes to **Resume**. Click **Resume** for new real-time data to be added to the window.

> **Note:**
>
> If the day and time in the **End Time** setting is in the past, then clicking **Resume** displays a message directing you to change the **End Time** setting.

- Click **Export** to export the currently displayed trace logs to a text file.

Configuring Subscriber Activity Logs

To configure subscriber activity logs:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log Settings page opens.
2. Click **Modify**.

   A new Subscriber Activity Log Settings page opens, containing fields for configuring the log.
3. In the Configuration section, configure the following information:
   a. **Trace Enable**—When selected, warning level trace logs are generated for errors that occur during subscriber activity processing.

   b. **Include MRA**—When selected, the system will check the MRA devices in subscriber tracing checks and include them in the warning level trace logs.

   c. **Severity**—Select the level of messages written to the log: **INFO** (default), **NOTIFY**, or **DEBUG**.

   d. **Activity Type**—Select the types of information to include in the log. The types available are **Protocol** and **Policy**. By default, all activity types are selected.

   > **Note:**
   >
   > To reduce the volume of logging and improve performance, select the activity types to narrow the focus of the log.

4. Add subscriber identifiers. See Adding Subscriber Identifiers for more information.
5. Configure the backup settings for the log. See Configuring Subscriber Activity Log Backup Settings for more information.
6. Click **Save**.

You have defined and saved the Subscriber Activity Log configuration.

Adding Subscriber Identifiers

Before adding subscribers, configure the Subscriber Activity Log. See Configuring Subscriber Activity Logs.
To add subscriber identifiers to the activity log:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log Settings page opens.
2. Select the **Configuration** tab.
3. Click **Modify**.

   The Subscriber Activity Log page opens, containing fields for configuring the log.
4. To add subscribers to the log in the **Subscriber Identifier List**:
   a. Click **Add**.

      The Add Subscriber Identifier window opens.

   b. Select the type of identifier and enter the subscriber identifier:
      - **IMSI** (default)
        International Mobile Subscriber Identity. Enter up to 15 Unicode digits.
      - **E.164 (MSISDN)**
        Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
      - **NAI**
        Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters &*+0-9?a-z_A-Z{}!#$%'^/=`|~-, optionally separated by a period (.). A valid realm name consists of the characters 0-9a-zA-Z- separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
      - **IPv4Address**
        An IPv4 address in the standard dot format.
      - **IPv6Address**
        An IPv6 address, in the standard 8-part colon-separated hexadecimal string format, and the subnet mask in CIDR notation from 0–128.
      - **SessionID**
        A valid session ID. A valid session ID consists of the characters &*+0-9?a-z_A-Z{}!#$%'^/=`|~-.
5. To select a date and time to stop tracing:
   a. Click 📅 to open the Select Date window.

   b. Select a date on the calendar.

   c. Enter a time using the format *hh:mm*. Valid values for *hh* are 00 to 23. Valid values for *mm* are 00 to 59.

6. Select **Enable** to start the trace for the subscriber ID.
7. (Optional) Enter a description about the trace for this subscriber. Enter up to 1000 characters.

   > **Note:**
   >
   > Only the first 50 characters appear in the list view.

8. Click **Save**.
9. (Optional) Add, edit, or delete subscribers.
   - Cloning an entry in the table
     a. Select an entry in the table.
     b. Click **Clone**. The Clone window opens with the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is added to the table.
   - Editing an entry in the table
     a. Select the entry in the table.
     b. Click **Edit**. The Edit Response window opens, displaying the information for the entry.
     c. Make changes as required.
     d. Click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     a. Select the entry in the table.
     b. Click ✕ **Delete**. A confirmation message displays.
     c. Click **Delete** to remove the entry. The entry is removed from the table.
10. Click **Save**.
    - Click **Save**.

The Subscriber Identifier List is populated with the defined subscribers. You have defined and saved the subscribers in the Subscriber Identifier List. The Subscriber Identifier List displays the information configured for the subscriber identifier and the status of that subscriber.

Table 15-26 Status and Related Icons

Status	Icon	Condition
Running	✓	Indicates the log is currently active (running). This status occurs when: • The **End Time** has not been reached or has just turned null. • **Enable** is selected.

Table 15-26 (Cont.) Status and Related Icons

Status	Icon	Condition
Disabled	❗	Indicates the log is not active. This status occurs when **Enable** is not selected and the **End Time** has not been reached.
Expired	❓	Indicates the log is no longer active. This status occurs when the **End Time** is reached.

Configuring Subscriber Activity Log Backup Settings

To configure the subscriber activity logs backup settings:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log Settings page opens.
2. Select the **Log Backup Settings** tab.
3. Click **Modify**.

   The Configuration page opens.
4. Configure the log backup settings:
   a. Select **Enabled Subscriber Activity log Backup** to create a backup of the log.

   b. In the **First Running Time** field, enter a date and time to start the backup in the format *mm/dd/yyyy hh*:*mm* (for example, `01/01/2015 12:15`).

      > **Note:**
      >
      > The date must be in the future.

      Alternatively, click 📅 (calendar) and select a date and click **Enter**.

   c. In **Run Interval(hours)**, set the time between backup runs. Valid values are from 1 to 99,999. The default is 24 hours.

   d. In **Max Keep Days**, set the maximum number of day to keep the log. Valid values are from 1 to 60. The default is 60 days.

   e. In **Folder Max Size(MB)**, set the maximum size of the backup storage folder. The default is 16000 MB.

   Backup Destination Folder indicates the storage location for the backup files (for example, `/var/camiant/subtracing`).
5. Click **Save**.

You have configured the Subscriber Activity Log backup settings.

Editing a Subscriber Identifier

To edit a subscriber identifier:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log Settings page opens.

2. Click **Modify**.

   A new Subscriber Activity Log Settings page opens, containing fields for configuring the log.

3. In the **Subscriber Identifier List** section, select a subscriber and identifier and click **Edit**.

   The Edit Subscriber Identifier window opens.

4. Edit the identifier.
5. Click **Save**.

You have edited a subscriber identifier.

Deleting a Subscriber Identifier from the Activity Log

To delete one or more subscriber identifiers from the Activity Log:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log Settings page opens.

2. Click **Modify**.

   A new Subscriber Activity Log Settings page opens, containing fields for configuring the log.

3. In the **Subscriber Identifier List** section, select a subscriber. Press the Ctrl or Shift key to select multiple subscribers. Click **Delete**.

   A confirmation message displays.

4. Click **Delete** to delete the subscriber identifiers.

   The subscriber identifier or identifiers are removed from the list.

You have deleted one or more subscriber identifiers.

Viewing Subscriber Activity Log History

To view the activity log history for subscribers:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.

   The Subscriber Activity Log Settings page opens in the work area.

2. Click **Activity Log History**.

   The Subscriber Activity Log History Log window opens, displaying the activity log.

3. Filter the display by using one or more of the following criteria and clicking **Filter**:

   - Start Date

> **Note:**
>
> If the trace start date and end date are both entered, then the window displays the logs that occur between the two time points.

- End Date
- Identifier Type
- Identifier Value
- Activity Type
- Server
- Contains Text

A filtered view of the history displays.

From the log window you can optionally do the following:

- Click a message summary to display the content for the selected message in the bottom pane of the window.
- Click **Reset** to reset the filter conditions to their defaults. The log is refreshed to show all messages.
- Click **Export** to export the filtered trace logs data into a text file. The traced messages are exported in descending order according to the time stamp.

Viewing the Trending Reports

To view the trending reports, from the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

The navigation pane displays the four trending reports. The reports display separate aggregate MPE and MRA statistics in graph tables.
The trending report columns display the following data:

- **MRA Binding Count**
  The number of bindings (for example, UE or Policy rules and charge function MPE pairs) which are maintained in the MRA system.

  > **Note:**
  >
  > A binding is the MRA routing information. The UE stores the user identity UE NAI, UE IP addresses, the selected MPE identity IP-CAN session, and APN if it is available.

- **PDN Connection Count**
  The number of PDN connections that communicate to the Diameter network elements.
- **Session Count**
  The number of Diameter sessions (for example, Gx or Gy) which are maintained in the MPE device.
- **Transaction Per Second**
  The number of Diameter requests and answer pairs processed in a second.

Viewing MRA Binding Count

The MRA binding count determines the number of MRA bindings between user equipment (UE) and MPE devices maintained in the MRA system. This is recorded by the counter MaxMRABindingCount.

To view the MRA Binding Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The content tree displays a list of trending reports.

2. From the content tree, select **MRA Binding Count**.

   The MRA Binding Count page displays the MRA Binding Count graph.

The following report options are available:

- **Refresh**
  You are provided with the most recently updated graph.
- **Search Filter**
  You can specify which MRA devices are graphed (all or specific devices) and which counters to graph (all or binding counts for MRA devices, which for this report is the same thing). You can also specify the graph parameters:
  - **Start Date & Time**
    The start date and time for the graph. Click 📅 (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration**
    Displays the time duration of the data. A list provides the following options:
    * **24 hours** (default)
    * **2 days**
    * **3 days**
    * **4 days**
    * **5 days**
    * **6 days**
    * **7 days**
  - **Show Aggregation**
    If you check this box, the aggregated data for all MRA devices is displayed in the graph.
- **Settings**
  The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format**
  The most recently updated graph is displayed in a separate window.
- **View Raw Data**
  The interval data statistics are displayed in a separate window.
- **Export CSV**
  A comma-separated value (CSV) file named `Export_MRA Binding Count.csv` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
- **View Summary**

The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing PDN Connection Count

This report plots the counter Interval MaxPDNConnectionCount for each managed MPE and MRA device.

To view the PDN Connection Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The content tree displays a list of trending reports.

2. From the content tree, select **PDN Connection Count**.

   The PDN Connection Count page displays the PDN Connection Count MRA and policy server (MPE device) graphs.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph table.
- **Search Filter** — You can specify which MPE and MRA devices are graphed (all or specific devices) and which counters to graph (all, PDN connections for MPE devices, or PDN connections for MRA devices). You can also specify the graph parameters:
  - **Start Date & Time** — The start date and time for the graph. Click 📅 (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration** — Displays the time duration of the data. A list provides the following options:
    - **24 hours** (default)
    - **2 days**
    - **3 days**
    - **4 days**
    - **5 days**
    - **6 days**
    - **7 days**
  - **Show Aggregation** — If you check this box, the aggregated data for all selected MPE or MRA content is displayed in the graph.
- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_PDN Connection Count.csv` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing Session Count

The session counts determine the number of Gx or Gy sessions maintained in the MPE device, graphed over time periods equal to the KPI interval length (by default 15 minutes). The session count is recorded by the counter MaxSessionCount.

To view the Session Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The content tree displays a list of trending reports.

2. From the content tree, select **Session Count**.

   The Session Count page displays the Session Count for policy server (MPE) device graph.

The following report options are available:

- **Refresh**
  You are provided with the most recently updated graph.
- **Search Filter**
  You can specify which MPE devices are graphed (all or specific devices) and which counters to graph (all or session counters for MPE devices, which for this report is the same thing). You can also specify the graph parameters:
  - **Start Date & Time**
    The start date and time for the graph. Click 📅 (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration**
    Displays the time duration of the data. A list provides the following options:
    - **24 hours** (default)
    - **2 days**
    - **3 days**
    - **4 days**
    - **5 days**
    - **6 days**
    - **7 days**

    > **Note:**
    >
    > The durations available depend on the settings of the OM Statistics scheduled task.
  - **Show Aggregation** — If you check this box, the aggregated data of all selected MPE content is displayed in the graph.
- **Settings**
  The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format**
  The most recently updated graph is displayed in a separate window.
- **View Raw Data**
  The interval data statistics are displayed in a separate window.

- **Export CSV**
  A comma-separated value (CSV) file named `Export_Session Count.csv` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
- **View Summary**
  The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing Transaction Per Second

Transactions per second is defined as the number of Diameter request or Diameter answer pairs processed in a second, graphed over time periods equal to the KPI interval length (by default 15 minutes). Transactions are recorded by the counter MaxTransactionsPerSecond.

To view the Transaction Per Second trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The content tree displays a list of trending reports.
2. From the content tree, select **Transaction Per Second**.

   The Transaction Per Second page displays the Transaction Per Second graph.

The following report options are available:

- **Refresh**
  You are provided with the most recently updated graph.
- **Search Filter**
  You can specify which Policy Management devices are graphed (all or specific devices) and which counters to graph (all or TPS for each class of Policy Management device). You can also specify the graph parameters:
  - **Start Date & Time**
    The start date and time for the graph. Click 📅 (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration**
    Displays the time duration of the data. A list provides the following options:
    - **24 hours** (default)
    - **2 days**
    - **3 days**
    - **4 days**
    - **5 days**
    - **6 days**
    - **7 days**
  - **Show Aggregation**
    If you check this box, the aggregated data for all selected devices is displayed in the graph.
- **Settings**
  The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format**
  The most recently updated graph is displayed in a separate window.

- **View Raw Data**
  The interval data statistics are displayed in a separate window.
- **Export CSV**
  A comma-separated value (CSV) file named `Export_Transaction Per Second.csv` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
- **View Summary**
  The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Custom Trending Reports

Along with the four pre-configured trending reports, you can create custom trending reports based on one or more counters.

The following statistics are associated with the MPE server type:

- AFRatTypeStats
- DiameterAfLatencyStats
- DiameterBberfLatencyStats
- DiameterBberfStats
- DiameterCTFStats
- DiameterDrmaLatencyStats
- DiameterDrmaStats
- DiameterPcefLatencyStats
- DiameterPcefStats
- DiameterShLatencyStats
- DiameterShStats
- DiameterSyLatencyStats
- DiameterSyStats
- DiameterTdfLatencyStats
- DiameterTdfStats
- IntervalStats
- KpiStats
- PDNConnectionAPNStats
- PdnRatTypeStats
- PolicyStats

The following statistics are associated with the MRA server type:

- DiameterMraAfLatencyStats
- DiameterMraAfStats
- DiameterMraBberfLatencyStats
- DiameterMraBberfStats

- DiameterMraCtfStats
- DiameterMraDraStats
- DiameterMraDrmaLatencyStats
- DiameterMraDrmaStats
- DiameterMraPcefLatencyStats
- DiameterMraPcefStats
- DiameterMraTdfLatencyStats
- DiameterMraTdfStats
- IntervalMraStats
- KpiMraStats

After creation, customized trending reports appear in the **Trending Reports** list following the pre-configured Trending Reports in alphabetical order.

Creating a Custom Trending Report

To create a custom trending report:

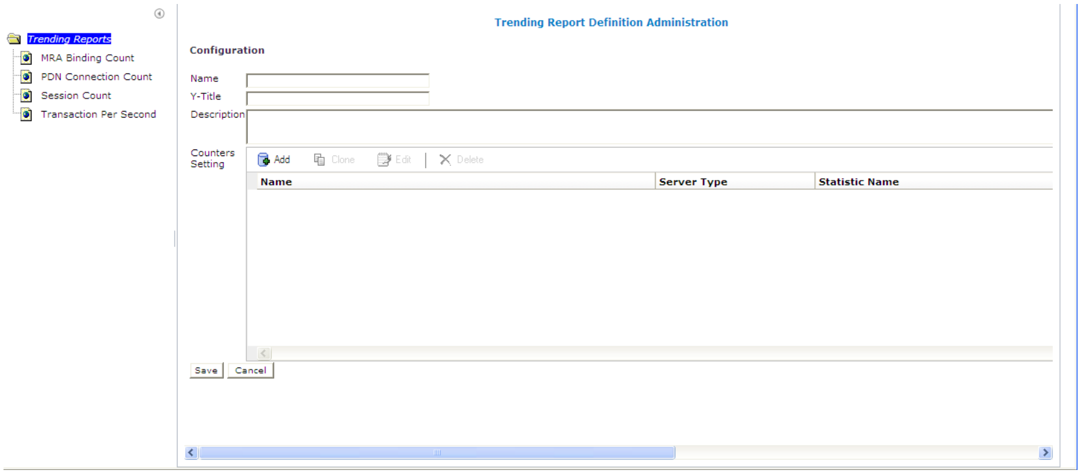
1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The Trending Report Definition Administration page opens.

2. Click **Create Trending Report Definition**.

   A new Trending Report Definition Administration page opens, containing fields for configuring a customized trending report.
   See Figure 15-2 shows a sample.

Figure 15-2 Trending Report Definition Configuration Page



Trending Report Definition Administration

Configuration

Name
Y-Title
Description
Counters Setting

Name	Server Type	Statistic Name

3. Enter the following information for the new trending report:

   a. **Name**—The name of the trending report.

      The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

   b. **Y-title**—The title of the Y series.

      The title can contain up to 40 characters and cannot begin or end with a space.

   c. **Description**—The description of the trending report.

      The description can contain up to 250 characters and cannot begin or end with a space.

4. Add counters to the report:

   a. Click **Add** next to the **Counters Setting** field.

      The Add Stats Definition popup opens.

   b. Enter a name for the counter in the **Name** field.

      The name can contain up to 40 characters, cannot contain double quotes (") or commas (,), and cannot begin or end with a space.

   c. Select the server type from the **Server Type** list.

   d. Select a statistic from the **Statistic Name** list.

      After selecting a statistic, all counters supported by that statistic populate the **Counter Name** list.

   e. Select a counter from the **Counter Name** list.

   f. Click **Save** to add the counter to the **Counters Setting** list.

      You have added a single counter to the trending report. You can continue to add individual counters to the report, using this step. You can also add counters by cloning an existing counter (described in the following step).

5. (Optional) Add, edit, or delete reports.

   - Cloning an entry in the table

     a. Select an entry in the table.

     b. Click **Clone**. The Clone window opens with the information for the entry.

     c. Make changes as required.

     d. Click **Save**. The entry is added to the table.

   - Editing an entry in the table

     a. Select the entry in the table.

     b. Click **Edit**. The Edit Response window opens, displaying the information for the entry.

     c. Make changes as required.

     d. Click **Save**. The entry is updated in the table.

   - Deleting a value from the table

     a. Select the entry in the table.

     b. Click ✕ **Delete**. A confirmation message displays.

     c. Click **Delete** to remove the entry. The entry is removed from the table.

6. Click **Save**.

You have defined and saved a custom trending report. The custom trending report appears, in alphabetical order by name, in the list of custom trending reports.

Editing a Custom Trending Report

You can edit any of the configured information for an existing custom trending report. You can also add, edit, or delete the counters associated with the report.

To edit a custom trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The Trending Report Definition Administration page opens.

2. Select the custom trending report.

   The report opens.

3. Click **Settings.**

   The Trending Report Definition Administration page displays for the report.

4. Click **Modify**.

   You can edit the **Name**, **Y-Title**, or **Description** of the report. You can also add, edit, or delete the counters associated with the report. See Creating a Custom Trending Report for additional information.

Deleting a Custom Trending Report

You can delete any of the existing custom trending reports. You cannot delete the pre-configured trending reports.

To delete a custom trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

   The Trending Report Definition Administration page opens.

2. Select the custom trending report.

   The report opens.

3. Click **Settings.**

   The Trending Report Definition Administration page displays for the report.

4. Click **Delete**.

   A confirmation message displays.

5. Click **OK**.

You have deleted the report.

Viewing Alarms

To view alarms or the alarms history:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.
2. Select the report to view.

The navigation pane displays the available alarms reports.

Viewing Active Alarms

The Active Alarms summary provides an aggregate view of time stamped alarm notifications for Policy Management systems. The display is refreshed every ten seconds and appears in the upper right corner of all CMP pages. Alarms remain active until they are reset.
The Active Alarms report provides details about active alarms. To view the Active Alarms report:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.

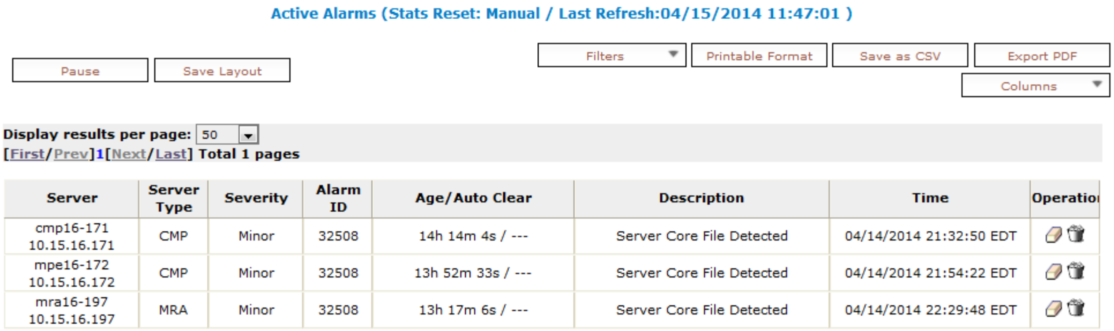
   The **Alarms** section expands to show the available alarm reports.

2. Select **Active Alarms**.

   The Active Alarms report opens in the work area.

Figure 15-3 shows a sample active alarm report.

Figure 15-3   Sample Active Alarms Report



Active Alarms (Stats Reset: Manual / Last Refresh:04/15/2014 11:47:01)

Display results per page: 50
[First/Prev]1[Next/Last] Total 1 pages

Server	Server Type	Severity	Alarm ID	Age/Auto Clear	Description	Time	Operatio
cmp16-171 10.15.16.171	CMP	Minor	32508	14h 14m 4s / ---	Server Core File Detected	04/14/2014 21:32:50 EDT	
mpe16-172 10.15.16.172	CMP	Minor	32508	13h 52m 33s / ---	Server Core File Detected	04/14/2014 21:54:22 EDT	
mra16-197 10.15.16.197	MRA	Minor	32508	13h 17m 6s / ---	Server Core File Detected	04/14/2014 22:29:48 EDT	

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 #unique_429.

> **Note:**
>
> Alarms generated by Policy Management systems running software lower than release 7.5 are mapped to these levels as follows: Emergency or Critical map to Critical; Alert or Error map to Major; Warning or Notice map to Minor.

The Age/Auto Clear column shows how long an alarm has been active (that is, how long since it was raised) and how long the alarm will display before being automatically cleared. The Auto Clear time is shown as `---` (three hyphens) if the alarm is not automatically cleared.

The following options are available:

- To sort the report on any column, click the column title.
- To display online help for an alarm, click its ID.
- To hide an alarm, click the hide icon (), located to the right of each row. All instances of alarms with that ID reported from that server are hidden from display (but shown in the Hidden Filter, which you can use to restore the display of those alarms).

> **Note:**
>
> Hiding an alarm only affects the current user. Other users will see the alarm if they display the Active Alarms page.

- To manually clear an alarm, click the Clear icon (🗑), located to the right of each row. You are prompted, `This alarm will be cleared. Are you sure?` Click **OK**.
- To pause the display of alarms, click **Pause**. To resume the display, click **Refresh**.
- To select what information is displayed, click **Columns** and select from the list.
- To control what alarms and alarm classes are displayed on the page, click **Filters** and select from the list:
  - The **Search Filter** tab has three controls. The **Server** control lets you display alarms from all servers (default) or a specific server. The **Server Type** control lets you display alarms from all Policy Management products (default) or just **CMP**, **MRA**, or **MPE** systems. The **Severity** control lets you display alarms of all severities (default), critical and major alarms, critical alarms, major alarms, or minor alarms.
  - The **Hidden Filter** tab shows alarms, by server and alarm ID, that are currently hidden from display. Click 🗑, to the right of an entry, to remove it from the list of hidden items and display it in the page again.
- To save your formatting changes to the report page, click **Save Layout**.
- **Printable Format**—The current alarms are displayed in a separate window.
- **Save as CSV**—A comma-separated value (CSV) file named `report.csv` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.
- **Export PDF**—A Portable Document Format (PDF) file named `report.pdf` is generated, suitable for a spreadsheet application, and a standard File Download window opens, so you can save or open the file.

Viewing the Alarm History Report

The Alarm History Report displays historical alarm information.

To view the alarm history report:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.

   The **Alarms** section expands to show the available alarm reports.
2. Select **Alarm History Report**.

   The Alarm History report opens.

> **Note:**
>
> If you are using Internet Explorer, the window appears behind the main window.

The window displays up to 50,000 alarms, sorted by age.

> **Note:**
>
> If you wish to view the most recent alarms, and there are more than 50,000 alarms in the database, specify a start date/time that includes the present.

3. To view older alarms, reduce the number of alarms displayed, or locate a specific alarm or group of alarms, you can define filtering criteria using the following fields:
   - **Start Date**
     Filter out alerts before a specific date/time. Click the calendar icon to specify a date/time.
   - **End Date**
     Filter out alerts after a specific date/time. Click the calendar icon to specify a date/time.
   - **Severity**
     Filter alerts by severity level. Select a level from the list. The default is **All**.
   - **Cluster or Server**
     Select the cluster or server within the cluster to view the alarms.
   - **Active Alarms**
     Select to view only active alarms; the default is to display both active and cleared alarms.
   - **Aggregate**
     Select to aggregate alarms that have the same IP address, alarm ID, and severity. (This function is limited to 50,000 alarms.)
4. After entering filtering information, click **Filter** to refresh the display with the filtering applied.

   The alarm list is filtered.
5. Click **Close**.

Alarms contain the following information:

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

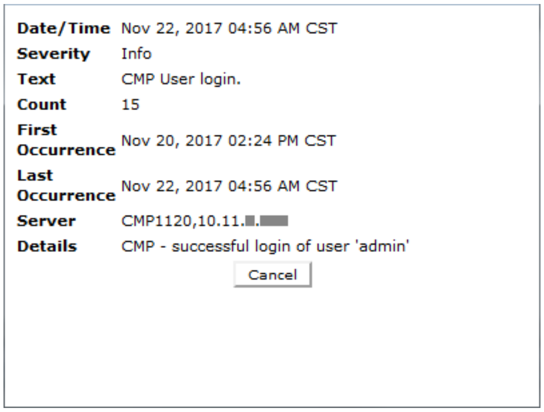
> **Note:**
>
> Alarms generated by Policy Management systems running software lower than release 7.5 are mapped to these levels as follows: Emergency or Critical map to Critical; Alert or Error map to Major; Warning or Notice map to Minor.

- **Alarm ID**
  When clicked, the alarm ID provides online help information.
- **Text**
  User-readable text of the alert.
- **OAM VIP**
  OAM IP address in IPv4 or IPv6 format.
- **Server**
  Name and IP address, in IPv4 or IPv6 format, or FQDN of the device from which this alarm was generated.

To view alert details, click (binoculars icon), located to the right of the alert. A window displays additional information.

For example:

Figure 15-4 Alert Details



Date/Time	Nov 22, 2017 04:56 AM CST
Severity	Info
Text	CMP User login.
Count	15
First Occurrence	Nov 20, 2017 02:24 PM CST
Last Occurrence	Nov 22, 2017 04:56 AM CST
Server	CMP1120,10.11.[redacted].[redacted]
Details	CMP - successful login of user 'admin'

Viewing Session Reports

To view the session reports, from the **System Wide Reports** section of the navigation pane, select **Sessions**.

The navigation pane displays the available session reports.

Viewing the AF Session Report

The application function (AF) session report shows information on the current and maximum number of AF sessions for each specific radio access technology type (RAT-Type) for each MPE device.

The following RAT-Types are supported:

- WLAN (0)—Wireless local area network
- VIRTUAL (1)—Virtual network
- UTRAN (1000)—Universal Terrestrial Radio Access Network
- GERAN (1001)—GSM EDGE Radio Access Network
- GAN (1002)—Generic Access Network
- HSPA_EVOLUTION (1003)—High Speed Packet Access Evolution
- EUTRAN (1004)—Evolved UTRAN
- CDMA2000_1x (2000)
- HRPD (2001)—High Rate Packet Data
- UMB (2002)—Ultra Mobile Broadband
- EHRPD (2003)—Enhanced HRPD

To view the AF session report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **AF Session Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **Associated MRA**—The MRA device managing this device, or N/A if no MRA device is managing this device. (If your CMP system is not configured to manage MRA devices, this option is not available.)
- **Server Name**—The name defined for the server.
- **Server Type**—Either **MPE** or **MRA**. All MPE devices managed by an MRA device are displayed together, followed by a row for that MRA device that represents the total counts for all MPE devices managed by that MRA device. Any MRA devices not managed by an MRA device are displayed after the last configured MRA device.
- **WLAN - Current**—The current number of WLAN connections to this device.
- **WLAN - Max**—The highest number of WLAN connections recorded to this device.
- **Virtual - Current**—The current number of Virtual connections to this device.
- **Virtual - Max**—The highest number of Virtual connections to this device.
- **UTRAN - Current**—The current number of UTRAN connections to this device.
- **UTRAN - Max**—The highest number of UTRAN connections recorded to this device.
- **GERAN - Current**—The current number of GERAN connections to this device.
- **GERAN - Max**—The highest number of GERAN connections recorded to this device.
- **GAN - Current**—The current number of GAN connections to this device.
- **GAN - Max**—The highest number of GAN connections recorded to this device.

- **HSPA_EVOLUTION - Current**—The current number of HSPA_EVOLUTION connections to this device.
- **HSPA_EVOLUTION - Max**—The highest number of HSPA_EVOLUTION connections recorded to this device.
- **EUTRAN - Current**—The current number of EUTRAN connections to this device.
- **EUTRAN - Max**—The highest number of EUTRAN connections recorded to this device.
- **CDMA2000_1X - Current** —The current number of CDMA2000_1X connections to this device.
- **CDMA2000_1X - Max**—The highest number of CDMA2000_1X connections recorded to this device.
- **HRPD - Current**—The current number of HRPD connections to this device.
- **HRPD - Max**—The highest number of HRPD connections recorded to this device.
- **UMB - Current**—The current number of UMB connections to this device.
- **UMB - Max**—The highest number of UMB connections recorded to this device.
- **EHRPD - Current**—The current number of EHRPD connections to this device.
- **EHRPD - Max**—The highest number of EHRPD connections recorded to this device.

The first row in the table displays the total for all configured MRA devices.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server Name**—Filter in all servers (default), server totals only, or one specific server.
- **Server Type**—Filter in all server types (default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA**—Filter in all MRA devices (default), totals only, or one specific MRA device. (If your CMP system is not configured to manage MRA devices, this option is not available.)

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; an AF Session Report window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

Viewing the PDN Connection Report

The PDN Connection Report shows information on the current and maximum number of packet data network (PDN) connections for each specific radio access technology type (RAT-Type) for each MPE device.

The following RAT-Types are supported:

- WLAN (0)—Wireless local area network
- UTRAN (1000)—Universal Terrestrial Radio Access Network

- GERAN (1001)—GSM EDGE Radio Access Network
- GAN (1002)—Generic Access Network
- HSPA_EVOLUTION (1003)—High Speed Packet Access Evolution
- EUTRAN (1004)—Evolved UTRAN
- CDMA2000_1x (2000)
- HRPD (2001)—High Rate Packet Data
- UMB (2002)—Ultra Mobile Broadband
- EHRPD (2003)—Enhanced HRPD
- UNKNOWN (-1)

To view the PDN Connection report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **PDN Connection Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **Associated MRA**—The MRA device managing this device, or N/A if no MRA device is managing this device. (If your CMP system is not configured to manage MRA devices, this option is not available.)
- **Server Name**—The name defined for the server.
- **Server Type**—Either **MPE** or **MRA**. All MPE devices managed by an MRA device are displayed together, followed by a row for that MRA device that represents the total counts for all MPE devices managed by that MRA device. Any MRA devices not managed by an MRA device are displayed after the last configured MRA device.
- **WLAN - Current**—The current number of WLAN connections to this device.
- **WLAN - Max**—The highest number of WLAN connections recorded to this device.
- **UTRAN - Current**—The current number of UTRAN connections to this device.
- **UTRAN - Max**—The highest number of UTRAN connections recorded to this device.
- **GERAN - Current**—The current number of GERAN connections to this device.
- **GERAN - Max**—The highest number of GERAN connections recorded to this device.
- **GAN - Current**—The current number of GAN connections to this device.
- **GAN - Max**—The highest number of GAN connections recorded to this device.
- **HSPA_EVOLUTION - Current**—The current number of HSPA_EVOLUTION connections to this device.
- **HSPA_EVOLUTION - Max**—The highest number of HSPA_EVOLUTION connections recorded to this device.
- **EUTRAN - Current**—The current number of EUTRAN connections to this device.
- **EUTRAN - Max**—The highest number of EUTRAN connections recorded to this device.

- **CDMA2000_1X - Current** —The current number of CDMA2000_1X connections to this device.
- **CDMA2000_1X - Max**—The highest number of CDMA2000_1X connections recorded to this device.
- **HRPD - Current**—The current number of HRPD connections to this device.
- **HRPD - Max**—The highest number of HRPD connections recorded to this device.
- **UMB - Current**—The current number of UMB connections to this device.
- **UMB - Max**—The highest number of UMB connections recorded to this device.
- **EHRPD - Current**—The current number of EHRPD connections to this device.
- **EHRPD - Max**—The highest number of EHRPD connections recorded to this device.
- **UNKNOWN - Current**—The current number of connections of unclassified type to this device.
- **UNKNOWN - Max**—The highest number of connections of unclassified type recorded to this device.

The first row in the table displays the total for all configured MRA devices.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server Name**
  Filter in all servers (default), server totals only, or one specific server.
- **Server Type**
  Filter in all server types (default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA**
  Filter in all MRA devices (default), totals only, or one specific MRA device. (If your CMP system is not configured to manage MRA devices, this option is not available.)

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a PDN Connection Count Report window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

Viewing the PDN APN Prefix Report

The PDN APN prefix report shows information on PDN connection counts per access point name (APN) prefix.

To view the PDN APN prefix report:

1. From the **System Wide Reports** section of the navigation pane, select **Sessions**.
2. Select **PDN APN Prefix Report**

The first row in the table displays the total values for all configured servers.

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:

- Sort the report on any column by clicking the column title.
- Pause the display of connections by clicking **Pause**. To resume the display, click **Refresh**.
- Displaying another page of the report by clicking **First**, **Prev**, **Next**, **Last**, or the specific page number.

Customizing the PDN APN Prefix Report

The PDN APN prefix report shows information on PDN connection counts per access point name (APN) prefix.

To view the PDN APN prefix report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **PDN APN Prefix Report**.

1. From the **System Wide Reports** section of the navigation pane, select **Sessions**.
2. Select **PDN APN Prefix Report**
3. Customize the report.

   You can customize the information that is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

   - **APN**
     The access point name.
   - **Server Name**
     The server name.
   - **Server Type**
     Either **MPE** or **MRA**.
   - **Current**
     The current number of PDN connection counts for each prefix that have been matched on each server.
   - **Max**
     The highest number of PDN connection counts for each prefix that have been matched on each server.

   The first row in the table displays the total values for all configured servers.

   You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

   - **APN**
     Filter in all APN prefixes (default), all PDN connections without a configured APN prefix match (OtherAPNs), or APN prefix totals only.
   - **Server Name**
     Filter in all servers (default), server totals only, or one specific server.
4. Click **Save Layout**.

Filtering the PDN APN Prefix Report

The PDN APN prefix report shows information on PDN connection counts per access point name (APN) prefix.

To filter the PDN APN prefix report:

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **APN**
  Filter in all APN prefixes (default), all PDN connections without a configured APN prefix match (OtherAPNs), or APN prefix 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 Prefix 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.

1. From the **System Wide Reports** section of the navigation pane, select **Sessions**.
2. Select **PDN APN Prefix Report**.
3. Click **Filters**.
4. Define the filtering criteria.
   - **APN**
     Filter in all APN prefixes (default), all PDN connections without a configured APN prefix match (OtherAPNs), or APN prefix totals only.
   - **Server Name**
     Filter in all servers (default), server totals only, or one specific server.

Printing the PDN APN Prefix Report

The PDN APN prefix report shows information on PDN connection counts per access point name (APN) prefix.

To print the PDN APN prefix report:

You can display the report in a format suitable for printing. ;

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.

1. From the **System Wide Reports** section of the navigation pane, select **Sessions**.
2. Select **PDN APN Prefix Report**
3. Click **Pause** to hold the current values.

   The display is refreshed automatically every ten seconds. To resume, click **Refresh**.

4. Click **Printable Format**.

   The PDN APN Prefix Statistics Report window opens.

5. Use the browser print function to print the report.
6. Click **Refresh** to resume the reports updates every 10 seconds.

Exporting the PDN APN Prefix Report

The PDN APN prefix report shows information on PDN connection counts per access point name (APN) prefix.

To export the PDN APN prefix report:.

1. From the **System Wide Reports** section of the navigation pane, select **Sessions**.
2. Select **PDN APN Prefix Report**
3. Click **Pause** to hold the current values.

   The display is refreshed automatically every ten seconds. To resume, click **Refresh**.

4. You can export the report as a CSv file or as a PDF file.
   - To export as a CSV file, **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.
   - To export as a PDF file. 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.
5. Click **Refresh** to resume the reports updates every 10 seconds.

Viewing Other Reports

To view the miscellaneous reports:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select the report to view.

The navigation pane displays the available reports.

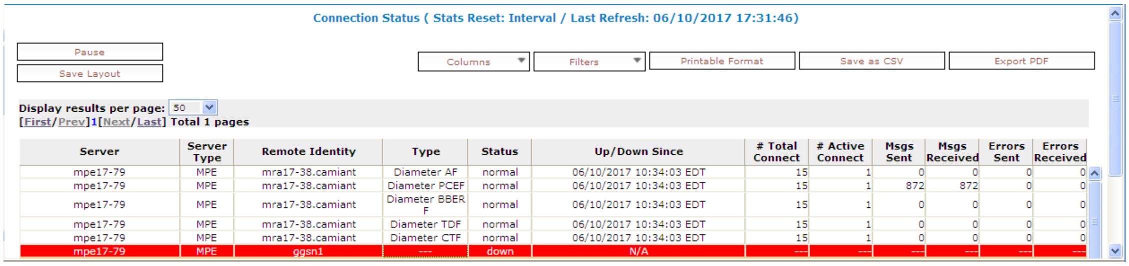
Viewing the Connection Status Report

The connection status report provides an aggregate view of connections maintained by managed Policy Management systems. The display is refreshed every ten seconds.
To view the connection status report.

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **Connection Status**

Figure 15-5 shows a sample connection status report.

Figure 15-5 Sample Connection Status Report



Connection Status (Stats Reset: Interval / Last Refresh: 06/10/2017 17:31:46)

Display results per page: 50
[First/Prev]1[Next/Last] Total 1 pages

Server	Server Type	Remote Identity	Type	Status	Up/Down Since	# Total Connect	# Active Connect	Msgs Sent	Msgs Received	Errors Sent	Errors Received
mpe17-79	MPE	mra17-38.camiant	Diameter AF	normal	06/10/2017 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter PCEF	normal	06/10/2017 10:34:03 EDT	15	1	872	872	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter BBERF	normal	06/10/2017 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter TDF	normal	06/10/2017 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter CTF	normal	06/10/2017 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	ggsn1	---	down	N/A	---	---	---	---	---	---

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The available columns are the following:

- **Server**
  Name of the associated system.
- **Server Type**
  MPE (Multimedia Policy Engine) or **MRA**.
- **Remote Identity**
  The Diameter ID (if known) or IP address of the remote system.
- **Type**
  The type of connection
- **Status**
  The status of the connection (the possible values are protocol-specific).
- **Up/Down Since**
  The timestamp when the connection reached its current state (N/A if the connection has never been established).
- **# Total Connect**
  The number of times that the connection has been re-established.

  > **Note:**
  >
  > This counter is reset if the cluster is restarted.

- **# Active Connect**
  The number of active connections.

  > **Note:**
  >
  > This counter is reset if the cluster is restarted.

- **Msgs Sent**

The number of Diameter or RADIUS protocol messages that have been sent to the remote system.

- **Msgs Received**
  The number of protocol messages that have been received from the remote system.
- **Errors Sent**
  The number of protocol error messages that have been sent to the remote system.
- **Errors Received**
  The number of protocol error messages that have been received from the remote system.

If a connection is in a non-functional state, the row is displayed in red; if a connection is in a transitional state between functional and non-functional (including when a connection is being established), the row is displayed in yellow.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server**
  Filter in all servers (default) or one specific server.
- **Server Type**
  Filter in all server types (default), totals only, MPE devices only, or MRA devices only.
- **Remote Identity**
  Filter in all remote devices (default) or one specific device.
- **Type**
  Filter in all remote device types (default) or one specific device type: **Diameter AF**, **Diameter PCEF**, **Diameter BBERF**, **Diameter TDF**, **Diameter SH**, **Diameter CTF**, or **Diameter DRMA**.
- **Status**
  Filter in all remote device status values (default) or one specific status: **down**, **normal**, or **reopen**.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a Connection Status Report window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

Viewing the Protocol Errors Report

The protocol errors report provides an aggregate view of connection errors, with one row for each distinct error code or sub-code. The display is refreshed every ten seconds.
To view the protocol errors report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **Protocol Errors**.

From the report page you can do the following:

- To sort the report on any column, click the column title.

- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The following columns are available:

- **Server**
  Name of the associated system.
- **Server Type**
  MPE or **MRA**.
- **Remote Identity**
  The Diameter ID (if known) or IP address of the remote system.
- **Error**
  The protocol error.
- **# Received**
  The number of protocol errors received from the remote system.
- **# Sent**
  The number of protocol errors sent to the remote system.

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

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

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a Connection Status Report window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

Viewing the Policy Statistics Report

The policy statistics report provides an aggregate view of policy statistics, with one row for each policy, letting you gauge the performance of individual policies. The display is refreshed every ten seconds.
To view the policy statistics report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.

   The list of available reports displays in the navigation pane.

2. Select **Policy Statistics Report**.

   The Policy Statistics report opens.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The following columns are available:

- **Server Name**
  Name of the associated system
- **Server Type**
  Either **MPE** or **MRA**
- **Policy Name**
  The name of each policy defined and active on the displayed server
- **Evaluated**
  The number of times the displayed policy was evaluated for the displayed server
- **Executed**
  The number of times the displayed policy was executed for the displayed server
- **Ignored**
  The number of times the displayed policy was ignored by the displayed server
- **Total Execution Time (ms)**
  The total execution time for each policy, in milliseconds
- **Average Execution Time (ms)**
  The average amount of time it takes a policy to execute, in milliseconds
- **Maximum Execution Time (ms)**
  The maximum execution time for each policy, in milliseconds

You can filter results by controlling which table rows appear, using the **Filters** list. You can define filtering criteria using the following fields:

- **Server Name**
  Filter in all servers (default) or one specific server.
- **Policy Name**
  Filter in all policies (default) or one specific policy.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a Policy Statistics Report window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

Viewing the MPE/MRA Replication Statistics Report

The MPE/MRABoD replication statistics report provides a view of database replication statistics, with one row for each replication path in an MPE or MRABoD 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**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To save the any formatting changes in the page, click **Save Layout**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** list. The following columns are available:

- **Cluster Name**
  The name of the cluster and the blades participating in replication as well as their high availability (HA) states.
- **Server Type**
  The type of cluster being utilized (MPE or MRABoD).
- **Blade State**
  Displays the state of the blade replicating with the current active blade.

Table 15-27 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 15-28 Sync State Values in MPE/MRAReplication 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

Table 15-28 (Cont.) Sync State Values in MPE/MRAReplication Stats Report

Sync Status	Description	Value Displayed on the CMP	Icon Used in the User Interface
DownRejected	The link is down because a connect attempt was rejected in the handshake phase.	Critical	⊗ Red X
DownHandshake	The link is connected but not ready for application use (so it is down logically). The links is being validated in a handshake as legitimate.	Critical	⊗ Red X
Connected	Connected and ready for use.	Critical	⊗ Red X
ConnectedReinit	Connected and ready for use, but after an application error where the recovery is start over without either a link drop or a complete application restart.	Critical	⊗ Red X
Connected Incompat	Connected but the schema are incompatible and replication cannot run until (1) the schema has the needed upgrade information or (2) problematic tables are excluded from replication.	Critical	⊗ Red X
RegisterSent	RegisterSent means the link is exchanging application level credentials and information (such as data dictionary information). In this state, registration has been sent from one side and it is being awaited from the other side.	Critical	⊗ Red X
RegisterAcked	In this state, registration has been sent acknowledged from the other side. In most configurations, it is a 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 a message that is is OK tor 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 databases with a normal and acceptable delay.	OK	✓ Green Check Mark
ActiveBehind	ActiveBehind is the same as Active but the slave database is unacceptably behind for whatever reasons. After an audit, it would be typical to be in the ActiveBehind state until any queued updates are applied to the slave database.	Major	❗ Red Exclamation Mark
ActiveSwitch	A switchover is being attempted without an audit if the states of the databases allow it.	Major	❗ Red Exclamation Mark
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 Sync State columns. The value for the Cluster State is selected based on the maximum severity.

Table 15-29 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** list. You can define filtering criteria using the following fields:

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

You can display the report in a format suitable for printing. Click **Printable Format**. The MPE/MRA Rep Status Report window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

Viewing the SGW Failure Report

The SGW failure report provides a list of the last 10 AN-GWs that failed and the corresponding time stamps.

To view the failure report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **SGW Failure Reports**.

   The SGW Failure Reports page opens.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To save the any formatting changes in the page, click **Save Layout**.
- To display another page of the report, click the page number.

You can customize the the table by controlling which columns appear, using the **Columns** list. The following columns are available:

- **SGW IP**
  The IP address for the SGW.
- **Last Failure Time**
  The UTC date and time the specified SGW failed.
- **Status**
  The current status for the specified SGW (that is, up or down).

You can customize the information displayed by using the **Filter** list to display information by **SGW IP** address and by **Status**.

You can display the report in a format suitable for printing. Click **Printable Format**; an SGW Failure Reports window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard File Download window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard File Download window opens, so you can save or open the file.

16

Upgrade Functions

This chapter describes the functions under the **Upgrade** menu in the CMP system.

For detailed instructions on upgrading your system, download the *Upgrade Guide* for your release from the Oracle Help Center (see Locate Product Documentation on the Oracle Help Center Site for more information).

Overview of Upgrade Functions

> **Note:**
>
> Access to the Upgrade functions may be restricted by user role. See About User Roles for more information.

The ISO Maintenance page lets you manage ISO files for the Policy Management servers. Using the **Operations** menu, you can push scripts, upload ISO files to selected servers or clusters, and delete uploaded ISO files from selected servers or clusters. See Viewing the ISO Maintenance Page for more information.

The Upgrade Manager page lets you upgrade software on clusters in the Policy Management network, or roll back an upgrade. An upgrade or rollback automatically processes a multi-server cluster or a georedundant site in the proper order to minimize data loss and downtime. During the process, the Upgrade Manager page displays progress information. The Upgrade Manager page also lets you view an upgrade log to review operations. See Viewing the Upgrade Manager Page for more information.

Viewing the ISO Maintenance Page

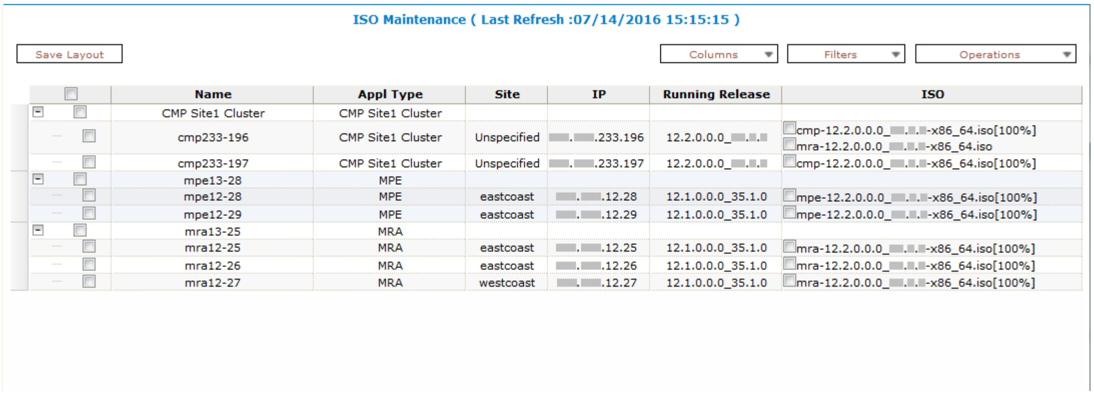
To view the ISO Maintenance page:

- From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.

  The ISO Maintenance page opens.

The ISO Maintenance page lists the clusters and servers in the Policy Management system. Also listed are application type, site, IP address, current release, and any ISO files available for upgrading the server or cluster.

Figure 16-1   ISO Maintenance Page



ISO Maintenance (Last Refresh :07/14/2016 15:15:15)

	☐	Name	Appl Type	Site	IP	Running Release	ISO
⊟	☐	CMP Site1 Cluster	CMP Site1 Cluster				
	☐	cmp233-196	CMP Site1 Cluster	Unspecified	[redacted].233.196	12.2.0.0.0_[redacted]	☐cmp-12.2.0.0.0_[redacted]-x86_64.iso[100%] ☐mra-12.2.0.0.0_[redacted]-x86_64.iso
	☐	cmp233-197	CMP Site1 Cluster	Unspecified	[redacted].233.197	12.2.0.0.0_[redacted]	☐cmp-12.2.0.0.0_[redacted]-x86_64.iso[100%]
⊟	☐	mpe13-28	MPE				
	☐	mpe12-28	MPE	eastcoast	[redacted].12.28	12.1.0.0.0_35.1.0	☐mpe-12.2.0.0.0_[redacted]-x86_64.iso[100%]
	☐	mpe12-29	MPE	eastcoast	[redacted].12.29	12.1.0.0.0_35.1.0	☐mpe-12.2.0.0.0_[redacted]-x86_64.iso[100%]
⊟	☐	mra13-25	MRA				
	☐	mra12-25	MRA	eastcoast	[redacted].12.25	12.1.0.0.0_35.1.0	☐mra-12.2.0.0.0_[redacted]-x86_64.iso[100%]
	☐	mra12-26	MRA	eastcoast	[redacted].12.26	12.1.0.0.0_35.1.0	☐mra-12.2.0.0.0_[redacted]-x86_64.iso[100%]
	☐	mra12-27	MRA	westcoast	[redacted].12.27	12.1.0.0.0_35.1.0	☐mra-12.2.0.0.0_[redacted]-x86_64.iso[100%]

Viewing the Upgrade Manager Page

> **Note:**
>
> For detailed instructions on upgrading your system, download the *Upgrade Guide* for your release from the Oracle Help Center (see #unique_447 for detailed information).

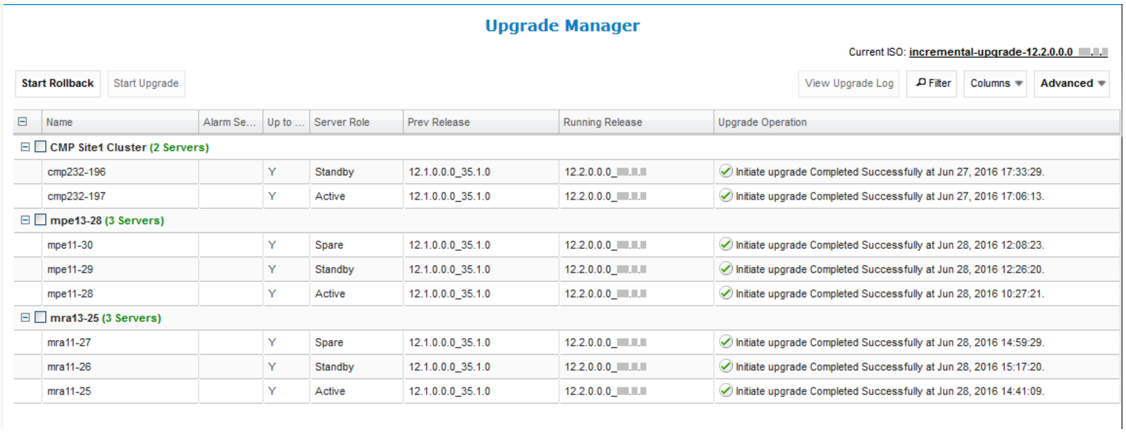
To view the Upgrade Manager page:

- From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

  The Upgrade Manager page opens.

The Upgrade Manager page lists the clusters and servers in the Policy Management system. Also listed are the current server alarm state, server role, previous release, current release, and the date, time, and result of the last upgrade operation performed on the server. You can display an upgrade log, which records timestamped upgrade events.

Figure 16-2   Upgrade Manager Page



Upgrade Manager

Current ISO: incremental-upgrade-12.2.0.0.0 [redacted]

⊟	Name	Alarm Se...	Up to ...	Server Role	Prev Release	Running Release	Upgrade Operation
⊟ ☐	CMP Site1 Cluster (2 Servers)						
	cmp232-196		Y	Standby	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 27, 2016 17:33:29.
	cmp232-197		Y	Active	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 27, 2016 17:06:13.
⊟ ☐	mpe13-28 (3 Servers)						
	mpe11-30		Y	Spare	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 28, 2016 12:08:23.
	mpe11-29		Y	Standby	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 28, 2016 12:26:20.
	mpe11-28		Y	Active	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 28, 2016 10:27:21.
⊟ ☐	mra13-25 (3 Servers)						
	mra11-27		Y	Spare	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 28, 2016 14:59:29.
	mra11-26		Y	Standby	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 28, 2016 15:17:20.
	mra11-25		Y	Active	12.1.0.0.0_35.1.0	12.2.0.0.0_[redacted]	✓ Initiate upgrade Completed Successfully at Jun 28, 2016 14:41:09.

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 contain both upgrade software and files that direct the upgrade process. When upgrading the Policy Management software, you can automatically distribute the files using the CMP interface or manually distribute the ISO files to the servers and clusters.

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

> **Note:**
>
> When patching the Policy Management software, do not use the ISO Maintenance page. You must manually distribute the ISO files to the CMP servers. See Preparing to Install a Patch or Patch Set for more information.

Adding an ISO File to a Server

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

To add an ISO file to a server:

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

   The ISO Maintenance page opens.
2. Select the clusters or servers to receive the ISO file.
3. Click the **Operations** list and select **Upload ISO**.

   The Upload ISO window opens.
4. Enter the following information for the ISO file (all fields are required):
   a. **Mode** — Mode used to transfer the ISO file to remote servers. Currently, **SCP** (Secure CoPy) 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 of the ISO file to be added to the remote server.
5. Click **Add**.

   The Upload ISO window closes, and the transfer process begins to the selected servers. A download icon appears in the **Name** column for the servers receiving the ISO file during the file transfer process. A progress bar displays during the operation. When the process completes, the icon disappears.

The ISO file is added to the servers.

Deleting ISO Files from the Servers

Before you start a new upgrade, it is recommended that any ISO file from past upgrades are removed from the servers.

To delete ISO files from the server:

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

   The ISO Maintenance page opens.
2. Select the clusters or servers.
3. Select the ISO file to be removed.
4. Click the **Operations** list and select **Delete ISO**.

   A confirmation message opens.
5. Click **OK**.

   A progress bar displays the progress of this operation.

The ISO files are deleted from the servers.

Manually Adding ISO Files to the Servers

You must add the upgrade file to all servers in the Policy Management system before performing an upgrade. This procedure describes the how to manually add the ISO files to the servers. To add the ISO files using the CMP interface, see Preparing for an Upgrade.

> **Note:**
>
> Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

> **Caution:**
>
> After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

If you are installing a patch or patch set, use the procedure described in Preparing to Install a Patch or Patch Set.

To manually add the ISO files to the servers:

1. Log in to the active server of the primary-site CMP cluster as `root`.

   The system displays the root-level prompt (`#`).
2. Ensure that the directory `/var/camiant/iso/` is empty.
3. Enter the command `cp /var/TKLC/upgrade/* /var/camiant/iso`.

   Upgrade files are copied to the target directory on the active server.

4. Enter the command `logout`.

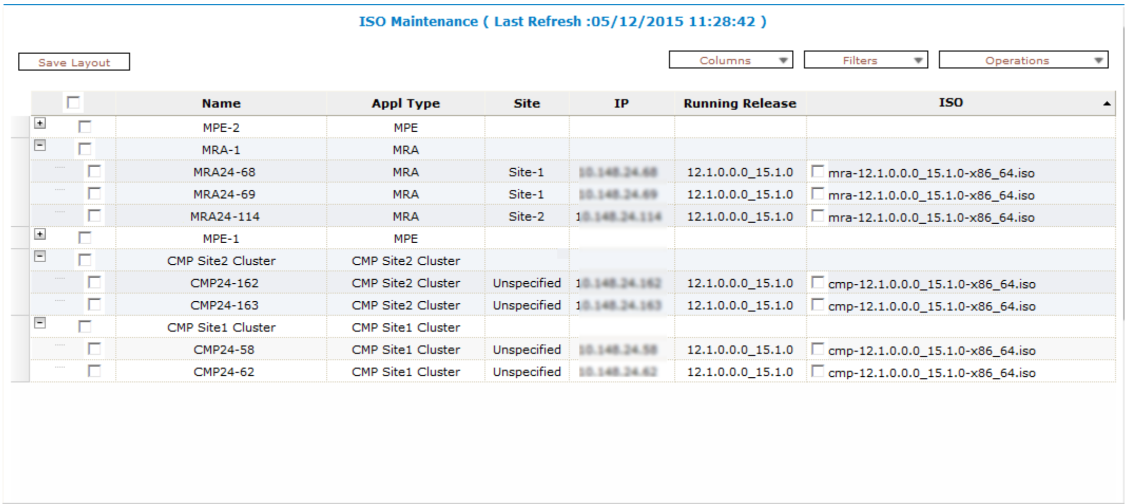
   You are logged out of the active server.

The servers now contain the ISO file and are ready for upgrading.

ISO Maintenance Page Elements

On the **Upgrade** section of the navigation pane, **ISO Maintenance** is an option. All clusters and their constituent servers in the Policy Management network are in the table on this page. You can collapse or expand the display of servers by clicking the [-] or [+] icons in the first column of the table. The display is updated every ten seconds. Figure 16-3 shows a sample ISO Maintenance page.

Figure 16-3 Sample ISO Maintenance Page



ISO Maintenance (Last Refresh :05/12/2015 11:28:42)

	□	Name	Appl Type	Site	IP	Running Release	ISO ▲
+	□	MPE-2	MPE				
−	□	MRA-1	MRA				
	□	MRA24-68	MRA	Site-1	[redacted]	12.1.0.0.0_15.1.0	□ mra-12.1.0.0.0_15.1.0-x86_64.iso
	□	MRA24-69	MRA	Site-1	[redacted]	12.1.0.0.0_15.1.0	□ mra-12.1.0.0.0_15.1.0-x86_64.iso
	□	MRA24-114	MRA	Site-2	[redacted]	12.1.0.0.0_15.1.0	□ mra-12.1.0.0.0_15.1.0-x86_64.iso
+	□	MPE-1	MPE				
−	□	CMP Site2 Cluster	CMP Site2 Cluster				
	□	CMP24-162	CMP Site2 Cluster	Unspecified	[redacted]	12.1.0.0.0_15.1.0	□ cmp-12.1.0.0.0_15.1.0-x86_64.iso
	□	CMP24-163	CMP Site2 Cluster	Unspecified	[redacted]	12.1.0.0.0_15.1.0	□ cmp-12.1.0.0.0_15.1.0-x86_64.iso
−	□	CMP Site1 Cluster	CMP Site1 Cluster				
	□	CMP24-58	CMP Site1 Cluster	Unspecified	[redacted]	12.1.0.0.0_15.1.0	□ cmp-12.1.0.0.0_15.1.0-x86_64.iso
	□	CMP24-62	CMP Site1 Cluster	Unspecified	[redacted]	12.1.0.0.0_15.1.0	□ cmp-12.1.0.0.0_15.1.0-x86_64.iso

The following types of elements display on the ISO Maintenance page:

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

Table 16-1 describes the elements on the ISO Maintenance page.

Table 16-1 ISO Maintenance Page Elements

Element	Description
□ (checkbox)	Use this column to select the clusters or servers on which an operation is to be performed. If you select a cluster, all servers in that cluster are selected. **Note:** At least one cluster or server must be selected before you can select an operation from the **Operations** menu.
Name	Displays the names of all filtered clusters and servers. When a server is receiving an ISO file, a download icon displays next to the name. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Appl Type	Displays the type of application running on each server. The **Filters** list lets you select the application type: • **CMP Site1 Cluster** • **CMP Site2 Cluster** • **MPE** • **MRA** • **All** You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Site	Displays the site name, if any, that is associated with each server. The **Filters** list also lets you display **Unspecified** or **All** sites. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column. **Note:** This column is only shown for a georedundant Policy Management network.
IP	Displays the OAM server IP address of each server. The **Filters** list lets you filter on only a server with a specific IP address or display **All** servers. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Running Release	Displays the current Policy Management software release of each server. The **Filters** list lets you filter on only a specific major release only or display **All** releases. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
ISO	Displays the ISO files available on each server. Use the checkbox to select the ISO file to delete during the **Delete ISO** operation. You can click on the column heading to reverse the sort order, or drag the edge of the heading to resize the column.
Columns	Use the **Columns** list to change the columns that are shown in this table. The **Name** column is mandatory. By default, all columns display. To change which columns display, uncheck the columns to be removed from the page.
Save Layout	Use the **Save Layout** button to save formatting changes to this page.

Table 16-1 (Cont.) ISO Maintenance Page Elements

Element	Description
Filters	Use the **Filters** list to select a subset of clusters and servers to display on this page. On this menu are the following pulldown filter submenus: **Appl Type**, **Site**, **IP**, and **Running Release**. By default, the filters are set to **All**, and all servers are listed. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	Use the **Operations** list to select an ISO operation to perform. **Note:** You must select (in the first column of the table) the cluster(s) or server(s) on which the operation is being performed before you can select an operation. The operations listed are dependent on the state of the selected servers; that is, if you select more than one server, only the operations that are valid for all the selected servers display. Possible operations are **Push Script**, **Upload ISO**, and **Delete ISO**. As a protective feature, before **Push Script** or **Delete ISO** are executed, you are prompted whether you sure you want to execute the operation. If you click **OK**, the operation is performed. A progress bar displaying the status of the command execution displays in a window. **Note:** After an operation is confirmed, it cannot be cancelled.

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.

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

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

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

During an upgrade, the Upgrade Manager asserts (that is, generates) and displays appropriate alarms, such as when servers go into forced standby, and clears the alarms when appropriate, such as when server upgrades are complete. The Upgrade Manager will also assert an alarm if an unexpected error prevents it from continuing the upgrade.

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

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

You must upgrade the CMP cluster (or, in a georedundant topology, the primary-site CMP cluster and then the secondary-site CMP cluster) before upgrading any other Policy Management systems.

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

Preparing for an Upgrade

You must add the upgrade file to all servers in the Policy Management system before performing an upgrade. This procedure describes the how to add the file to the servers using the user interface. To add the files manually see Manually Adding ISO Files to the Servers.

> **Note:**
>
> Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

> **Caution:**
>
> After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

If you are installing a patch or patch set, use the procedure described in Preparing to Install a Patch or Patch Set.

To prepare for an upgrade:

1. Use **Delete ISO** to remove any old upgrade files from all servers in the Policy Management network. See Deleting ISO Files from the Servers.

   The servers are now ready for the new upgrade file.
2. Use **Upload ISO** to distribute the upgrade ISO file to all servers in the Policy Management network. See Adding an ISO File to a Server.

The servers are now ready for upgrade.

The servers now contain the upgrade package and are ready for upgrading.

Preparing to Install a Patch or Patch Set

Patch software is available for electronic download on My Oracle Support. See the release notes for the patch to determine the servers that require the patch installation. If there is an order requirement, the Upgrade Director manages that process.

To prepare to install a patch or patch set:

1. Copy the ISO file to all CMP servers.
   a. Ensure that the directory `/var/camiant/iso` is empty.
   b. Use the secure copy command, `scp`, to copy the ISO file to the `/var/camiant/iso` directory.
2. Open the CMP interface.
3. View the active alarms.

   Identify the cause of any existing active alarms, and determine if the alarms have an impact on the patch or patch set. Export the current alarms and save to a file.

   > **Note:**
   >
   > If there are alarms present that could impact the patch or patch set, it is recommended that you contact Oracle Consulting services prior to adding the patch.

4. View the KPI stats. Verify that the system is running within expected parameters and export current KPI stats to a file.
5. Check the checksum file:
   a. Transfer the md5sum.out file to the `/var/camiant/tmp` directory.
   b. Use the catenate command, `cat`, to see the value of the checksum.

      For example:

      ```
      [root@CMP-JB-126 tmp]# cat md5sum.out
      cca84e669c8db680f3264a93fe83aab7/home/build/build/PLATFORM-70/iso/
      patch-12.1.1.1.x_x.x.x.iso
      [root@CMP-JB-126 tmp]#
      ```

   c. Verify that the checksum value is the same as the value in the md5sum.out file.

      For example:

      ```
      [root@CMP-JB-126 iso]# md5sum patch-12.1.1.1.x_x.x.x.iso
      cca84e669c8db680f3264a93fe83aab7 patch-12.1.1.1.x_x.x.x.iso
      [root@CMP-JB-126 iso]#
      ```

6. Using the CMP interface, select the ISO file containing the patch or patch set. See Selecting an ISO for Upgrade.

7. Continue with Upgrading a Primary-site CMP Cluster.

Selecting an ISO for Upgrade

You must distribute an ISO file beforehand to all servers that will use it (see Adding an ISO File to a Server). When the distribution is complete, you must select the ISO file to use in an upgrade before beginning the process. If you have multiple ISO files available for an upgrade (for example, if you have a major release and an update release, or an update release and a patch), you can select which one to use. If you have multiple clusters to upgrade, you only have to select the ISO file for the CMP system.

To select an ISO:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

   The Upgrade Manager page appears.

2. Click on the name of the file listed as the current ISO (which may appear as **Install Kit**).

   The Select ISOs window opens, listing the available ISO files.

3. (Optional) You can click on a column heading to sort the rows on that column. You can click **Filter** list to filter out rows based on the data in one or more columns. You can click the **Columns** list to select which columns are displayed (by default, all columns are displayed). You can resize columns.

4. Select which ISO file to use and click the **Select** button at the bottom of the window.

   You are prompted: `Loading this ISO will cause the upgrade manager to abandon the current upgrade and start a new one. Are you sure you want to continue loading this ISO?`

5. Click **OK**.

   The Select ISOs window closes, and the selected ISO file is listed as the current ISO.

The ISO is selected for upgrade. The data in the Up to date column changes from **n/a** to either **Y** (which means that the server is running up-to-date software) or **N** (which means that the server needs upgrading).

Upgrading a Primary-site CMP Cluster

You must upgrade the primary-site CMP cluster first in any Policy Management topology. This procedure describes the normal upgrade process.

Note:

Contact My Oracle Support and inform them of your upgrade plans prior to beginning this or any upgrade procedure. Before upgrading any system, please read the upgrade procedure, the *Release Notice* for this release, and any *Network Impact Report*. Also, go to the My Oracle Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

Caution:

After you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost.

If you are installing a patch or patch set, use the procedure described in Preparing to Install a Patch or Patch Set.

If you are installing an upgrade to the current release, see Preparing for an Upgrade before starting this procedure.

To upgrade the primary-site CMP cluster:

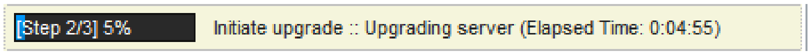
1. Log in to the active CMP server as an administrator with upgrade privileges.
2. Click **Upgrade** in the navigation pane and then click **Upgrade Manager**.

   The **Upgrade Manager** page opens.
3. Select an ISO file to use for the upgrade.

   For more information, see Selecting an ISO for Upgrade.
4. Select the primary CMP (Site1) cluster and click **Start Upgrade**.

   You are prompted: `Are you sure that you want to perform this action? Initiate upgrade` *`server_name`* `(next)`
5. Click **OK** to continue.

   The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the standby server. The **Upgrade Operation** column displays the progress of the action; for example:

   [Step 2/3] 5% Initiate upgrade :: Upgrading server (Elapsed Time: 0:04:55)

   > **Note:**
   >
   > The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

   When the standby server is upgraded, the **Upgrade Operation** column displays the message: `Initiate upgrade Completed Successfully at` *`date_time`*. and the following alarms are reported:

   - 70500-System Mixed Version
   - 70501-Cluster Mixed Version
   - 70502-Cluster Replication Inhibited
   - 70503-Server Forced Standby
   - 70506-Upgrade Operation Failed
   - 70507-Upgrade In Progress
   - 70508-Server Is Zombie

   > **Tip:**
   >
   > Review alarms associated with each action before proceeding with the next action.

6. Log in to the active server of the primary-site CMP cluster as `root`.

   The system displays the root-level prompt (`#`).

7. Enter the command `ls -l /var/camiant/iso` to verify that the correct CMP ISO is in the directory.

   If the ISO is not present, enter the following commands:

   ```
   rm -f /var/camiant/iso/*
   ```

   ```
   cp /var/TKLC/upgrade/* /var/camiant/iso
   ```

   Upgrade files are copied to the target directory on the active server.

8. Enter the command `logout`.

   You are logged out of the active server.

9. Log in to the active CMP server as an administrator with upgrade privileges.

   You have access to the **Upgrade** menu in the navigation pane.

10. Select the cluster again and click **Continue Upgrade**.

    You are prompted: `Are you sure that you want to perform this action? Failover to new version` *`cluster_name`* `(next).`

11. Click **OK** to continue.

    If you stop an upgrade at a point of operator intervention, you can resume it later, or roll it back from there.

    The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.

12. Select the cluster again and click **Continue Upgrade**.

    You are prompted: `Are you sure that you want to perform this action? Initiate upgrade` *`server_name`* `(next).`

13. Click **OK**.

    The remaining CMP server in the cluster is upgraded. When the Cluster Mixed Version alarm clears, the upgrade is complete.

    > **Tip:**
    >
    > You do not have to wait for the primary CMP cluster to be upgraded before beginning to upgrade the secondary CMP cluster.

The primary-site CMP cluster is upgraded. You must now upgrade the secondary (Site2) CMP cluster, if present, before you can upgrade any other Policy Management clusters. When all the CMP clusters are upgraded, you can upgrade the remaining clusters of the Policy Management network.

Upgrading a Georedundant Cluster

Before upgrading a cluster, see Preparing for an Upgrade.

If you are adding a patch or patch set, see Preparing to Install a Patch or Patch Set.

If you are upgrading an entire Policy Management network, you must upgrade the primary-site CMP cluster first, then the secondary-site CMP cluster (if present).

The required sequence followed by the Upgrade Manager to upgrade a two-server cluster (including a CMP cluster) is as follows:

1. Upgrade the standby server.
2. Fail over to the standby server.
3. Reapply the configuration to the cluster.
4. Upgrade the remaining server.

The default, preferred sequence followed by the Upgrade Manager to upgrade a georedundant (three-server) cluster is as follows:

1. Upgrade the standby server.
2. Fail over to the standby server.
3. Reapply the configuration to the cluster.
4. Upgrade the remaining server in the primary site.
5. Upgrade the spare server.

An optional action lets you change this order if required. You can also upgrade the second and third server in the cluster simultaneously.

You can upgrade up to four MPE or MRA clusters in parallel. (This is the best practice.) You must manually start the process for each cluster.

You can roll back from an upgrade from any point of operator intervention. Whenever the action **Continue Upgrade** is available, the action **Start Rollback** is also available.

> **Caution:**
>
> Use only the upgrade procedure provided by the Oracle Customer Care Center. Before upgrading any system, please go to the Oracle Customer Support website and review any Technical Service Bulletins (TSBs) that relate to this upgrade. After you begin an upgrade, any changes to the configuration (such as creating or editing network elements or policies) may be lost.

To upgrade a georedundant cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

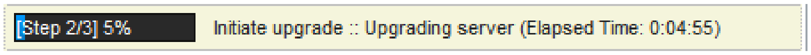
   The Upgrade Manager page opens.

2. Select the cluster to be upgraded and click **Start Upgrade**.

   You are prompted: `Are you sure that you want to perform this action? Initiate upgrade` *`server_name`* `(next)`

3. Click **OK** to continue.

   The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the standby server, in the primary site. The **Upgrade Operation** column displays the progress of the action; for example:

   [Step 2/3] 5%

   Initiate upgrade :: Upgrading server (Elapsed Time: 0:04:55)

> **Note:**
>
> The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

When the standby server is upgraded, the **Upgrade Operation** column displays the message `Initiate upgrade Completed Successfully at` *`date_time`* and Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

> **Tip:**
>
> Review alarms associated with each action before proceeding with the next action.

4. Select the cluster again and click **Continue Upgrade**.

   You are prompted: `Are you sure that you want to perform this action? Failover to new version` *`cluster_name`* `(next).`

5. Click **OK** to continue.

   If you stop an upgrade at a point of operator intervention, you can resume it later, or roll it back from there.

   The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.

6. Reapply the configuration to the cluster:

   - (For an MPE cluster) From the **Policy Server** section of the navigation pane, select **Configuration**, select the cluster, and in the Policy Server Administration page, click **Reapply Configuration**.
   - (For an MRA cluster) From the **MRA** section of the navigation pane, select **Configuration**, select the cluster, and in the MRA Administration page, click **Reapply Configuration**.

   The configuration information is synchronized.

7. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

   The Upgrade Manager page opens.

8. Select the cluster again and click **Continue Upgrade**.

   You are prompted: `Are you sure that you want to perform this action? Initiate upgrade` *`server_name`* `(next).`

9. Click **OK** to continue.

   The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the second server in the primary site. The **Upgrade Operation** column displays the progress of the current action.

   When the second server is upgraded, the **Upgrade Operation** column displays the message: `Initiate upgrade Completed Successfully at` *`date_time`*.

10. Select the cluster again and click **Continue Upgrade**.

    You are prompted: `Are you sure that you want to perform this action? Initiate upgrade` *`server_name`* `(next).`

11. Click **OK** to continue.

    The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then upgrades the spare server, in the secondary site. The **Upgrade Operation** column displays the progress of the current action.

    When the spare server is upgraded, the **Upgrade Operation** column displays the message: `Initiate upgrade Completed Successfully at` *`date_time`* and Alarm 70501 is cleared.

The georedundant cluster is upgraded. For each server, the **Prev Release** column displays the release installed before the upgrade, and the **Up to Date** column displays `Y` (yes).

If the upgrade fails, a diagnostic message describes the problem. Try the upgrade again; if it fails again, contact My Oracle Support.

> **Note:**
>
> If the upgrade fails and also leaves the 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.

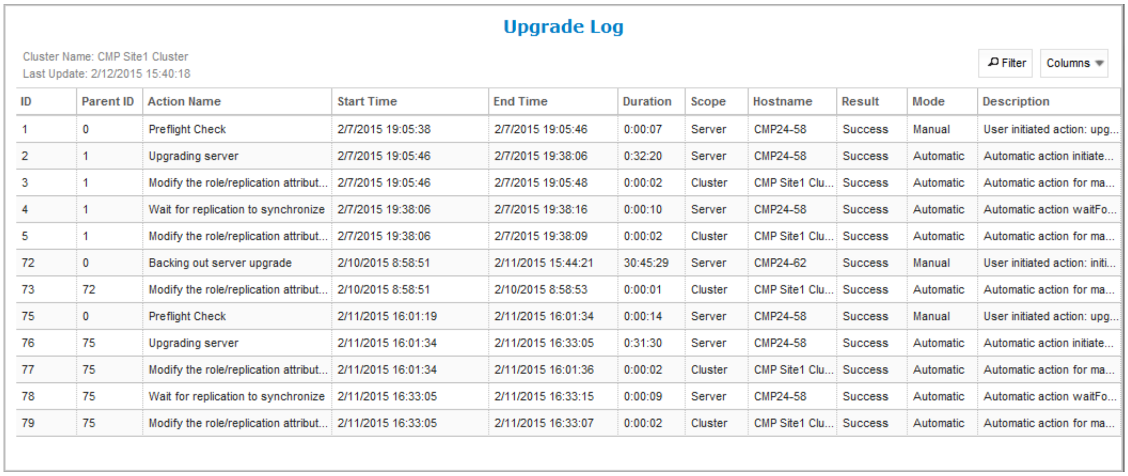
2. Select the cluster and then click **View Upgrade Log**.

   The Upgrade Log window opens.

The upgrade log is displayed. Figure 16-4 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.

Figure 16-4   Sample Upgrade Log



Upgrade Log

Cluster Name: CMP Site1 Cluster
Last Update: 2/12/2015 15:40:18

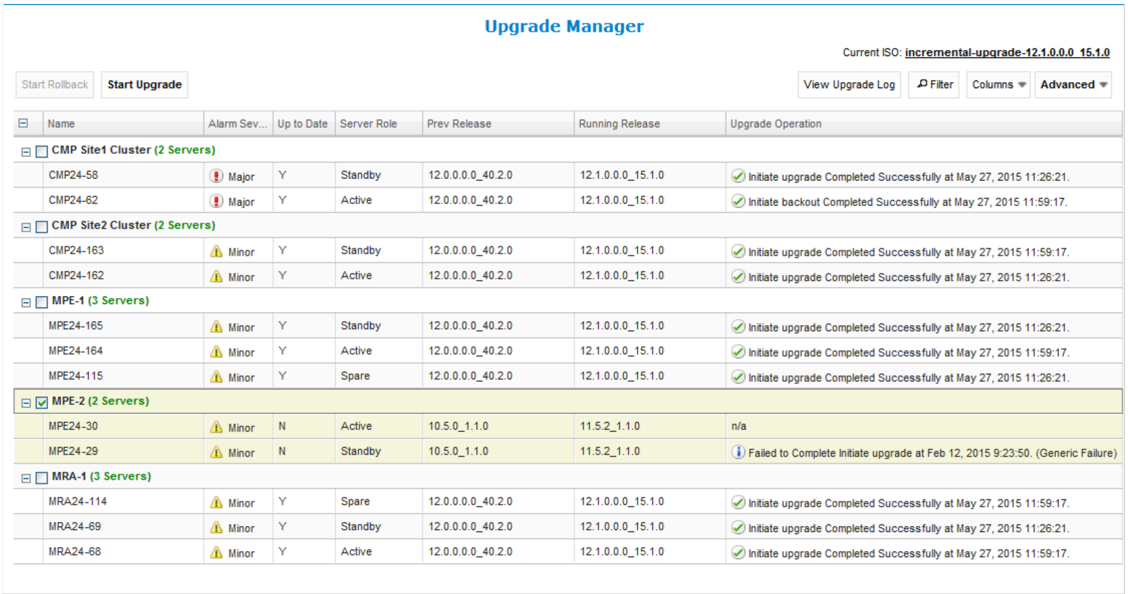
ID	Parent ID	Action Name	Start Time	End Time	Duration	Scope	Hostname	Result	Mode	Description
1	0	Preflight Check	2/7/2015 19:05:38	2/7/2015 19:05:46	0:00:07	Server	CMP24-58	Success	Manual	User initiated action: upg...
2	1	Upgrading server	2/7/2015 19:05:46	2/7/2015 19:38:06	0:32:20	Server	CMP24-58	Success	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...

Upgrade Manager Page Elements

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

Figure 16-5 shows a sample.

Figure 16-5 Sample Upgrade Manager Page



Upgrade Manager

Current ISO: incremental-upgrade-12.1.0.0.0_15.1.0

⊟	Name	Alarm Sev...	Up to Date	Server Role	Prev Release	Running Release	Upgrade Operation
⊟ □	CMP Site1 Cluster (2 Servers)						
	CMP24-58	Major	Y	Standby	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
	CMP24-62	Major	Y	Active	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate backout Completed Successfully at May 27, 2015 11:59:17.
⊟ □	CMP Site2 Cluster (2 Servers)						
	CMP24-163	Minor	Y	Standby	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.
	CMP24-162	Minor	Y	Active	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
⊟ □	MPE-1 (3 Servers)						
	MPE24-165	Minor	Y	Standby	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
	MPE24-164	Minor	Y	Active	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.
	MPE24-115	Minor	Y	Spare	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
⊟ ☑	MPE-2 (2 Servers)						
	MPE24-30	Minor	N	Active	10.5.0_1.1.0	11.5.2_1.1.0	n/a
	MPE24-29	Minor	N	Standby	10.5.0_1.1.0	11.5.2_1.1.0	ⓘ Failed to Complete Initiate upgrade at Feb 12, 2015 9:23:50. (Generic Failure)
⊟ □	MRA-1 (3 Servers)						
	MRA24-114	Minor	Y	Spare	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.
	MRA24-69	Minor	Y	Standby	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:26:21.
	MRA24-68	Minor	Y	Active	12.0.0.0.0_40.2.0	12.1.0.0.0_15.1.0	✓ Initiate upgrade Completed Successfully at May 27, 2015 11:59:17.

The Upgrade Manager page contains the following elements:

- □ (check boxes) to select clusters to upgrade or roll back
- Buttons (context-sensitive actions such as **Start Rollback** or **Start Upgrade**); **View Upgrade Log**; **Filter**; and the name of the current ISO
- The table of filtered clusters and servers
- Lists (**Columns** and **Advanced**) for changing what columns are in the table and for selecting optional advanced operations

Table 16-2 describes these elements.

Table 16-2   Upgrade Manager Page Elements

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

Table 16-2 (Cont.) Upgrade Manager Page Elements

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

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 16-5, **Start Upgrade** is a valid action for the selected cluster, but **Start Rollback** is not.

Common actions include the following:

- **Start Upgrade** (after a new ISO file is available)

- **Continue Upgrade** (when the upgrade process has reached a point of user intervention)
- **Start Rollback** (after a system is upgraded)
- **Continue Rollback** (when the rollback process has reached a point of user intervention)

You should normally be able to complete an upgrade by clicking only **Start Upgrade** and **Continue Upgrade**.

About Rolling Back an Upgrade

It is possible to roll back, or back out, the Policy Management software to the previous release in a production environment. The overall sequence is the reverse of the upgrade sequence:

1. Roll back MPE and MRA clusters.
2. Roll back all CMP systems except for the last CMP server. (You cannot begin this operation until all MPE andMRA clusters are rolled back.)
3. If you are rolling back to Release 11.5, use the System Maintenance page to roll back the last CMP server.

In the same way that you can roll back from an upgrade from any point of operator intervention, you can also upgrade from a rollback from any point of operator intervention. Whenever the action **Continue Rollback** is available, the action **Resume Upgrade** is also available.

Rolling Back an Upgrade

The default, preferred sequence followed by the Upgrade Manager to roll back a georedundant (three-server) cluster is as follows:

1. Roll back the standby server.
2. Roll back the spare server.
3. Fail over to the standby server.
4. Reapply the configuration to the cluster.
5. Roll back the remaining server.

An optional advanced action lets you change this order if required. You can also roll back the second and third server in the cluster simultaneously.

The default, preferred sequence followed by the Upgrade Manager to roll back a two-server cluster is as follows:

1. Roll back the standby server.
2. Fail over to the standby server.
3. Reapply the configuration to the cluster.
4. Roll back the remaining server.

You can roll back up to four MPE or MRA clusters in parallel. (You must manually start the process for each cluster.)

To roll back a georedundant cluster:

1. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

   The Upgrade Manager page opens.

2. Select the cluster to be rolled back and click **Start Rollback**.

   You are prompted: `Are you sure that you want to perform this action? Initiate backout` *`server_name`* `(back).`

3. Click **OK** to continue.

   The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the standby server, in the primary site. The **Upgrade Operation** column displays the progress of the current action.

   > **Note:**
   >
   > The number of steps in any given action is determined outside of the Upgrade Manager and may vary from release to release.

   When the standby server is rolled back, the **Upgrade Operation** column displays the message `Initiate backout Completed Successfully at` *`date_time`* and Alarm 70501 (CLUSTER_MIXED_VERSION) is asserted.

   > **Tip:**
   >
   > Review alarms associated with each action before proceeding with the next action.

4. Select the cluster again and click **Continue Rollback**.

   You are prompted: `Are you sure that you want to perform this action? Initiate backout` *`server_name`* `(back).`

5. Click **OK** to continue.

   If you stop a rollback at a point of operator intervention, you can continue it later, or resume upgrading it from there.

   The confirmation window closes and the Upgrade Manager performs pre-rollback checks and then rolls back the spare server, in the secondary site. The **Upgrade Operation** column displays the progress of the current action. When the spare server is rolled back, the **Upgrade Operation** column displays the message `Initiate backout Completed Successfully at` *`date_time`*.

6. Select the cluster again and click **Continue Rollback**.

   You are prompted.: `Are you sure that you want to perform this action? Failover to old version` *`cluster_name`* `(next).`

7. Click **OK** to continue.

   The confirmation window closes and the cluster fails over to the standby server, which becomes the active server.

8. Reapply the configuration to the cluster:

   - (For an MPE cluster) From the **Policy Server** section of the navigation pane, select **Configuration**, select the cluster, and in the Policy Server Administration page, click **Reapply Configuration**.
   - (For an MRA cluster) From the **MRA** section of the navigation pane, select **Configuration**, select the cluster, and in the MRA Administration page, click **Reapply Configuration**.

The configuration information is synchronized.

9. From the **Upgrade** section of the navigation pane, select **Upgrade Manager**.

   The Upgrade Manager page opens.

10. Select the cluster again and click **Continue Rollback**.

    You are prompted: `Are you sure that you want to perform this action? Initiate backout` *`server_name`* `(back)`

11. Click **OK** to continue.

    The confirmation window closes and the Upgrade Manager performs pre-upgrade checks and then rolls back the remaining server, in the primary site. The **Upgrade Operation** column displays the progress of the current action.

    When the remaining server is rolled back, the **Upgrade Operation** column displays the message `Initiate backout Completed Successfully at` *`date_time`* and Alarm 70501 is cleared.

The cluster is rolled back to the previous release. For each server, the **Running Release** column displays the release to which you rolled the system back, and the **Up to Date** column displays `N` (no).

If the rollback fails, a diagnostic message describes the problem. Try the rollback again; if it fails again, contact My Oracle Support.

> **Note:**
>
> If the rollback fails and also leaves the 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.

17 Global Configuration

This section describes how to configure the global settings in the CMP system.

Setting the Precedence Range

When overlapping policy and charging control (PCC) quality of service (QoS) rules apply to the same Gx or Gxx Diameter session, precedence is applied to determine which rule is installed on the gateway. In the case of an overlap, the rule with the lower precedence value is installed. Some vendor gateways require unique precedence, or else reject rules. You can configure MPE devices to maximize the probability that all rules have unique PCC rule precedences. This is a global configuration setting that affects all MPE devices managed by this CMP system.

> **Note:**
>
> This does not guarantee rule precedence uniqueness. Operator-defined rules are not validated to ensure precedence uniqueness; if you define such rules, you must track their precedence values yourself.

To set the precedence range:

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

   The content tree displays a list of global configuration settings.
2. From the content tree, select the **Precedence Range** group.

   The Precedence Range Configuration page opens in the work area.
3. Click **Modify**.

   The fields become editable.
4. Enter values for the configuration attributes:
   a. **AF-Triggered** — Enter the minimum and maximum values for rules triggered by Rx requests. The default range is 400 to 899.
   b. **UE-Triggered** — Enter the minimum and maximum values for rules triggered by user equipment-initiated resource requests. This range cannot overlap with the AF range. The default range is 1000 to 1999.
   c. **Default Session** — If no other rules are installed when a Gx eHRPD, E-UTRAN, or GPRS session is established, a default rule is installed. Enter the default session precedence. The default precedence is 3000.
5. Click **Save**.

The reserved precedence ranges are configured.
Precedence values not set aside here are available for your use in defining rules. By default, you can use:

- 0–399
- 900–999
- 2000–2999
- 301–4,294,967,295

> **Note:**
>
> Range changes do not automatically redeploy rule with new precedence values. Also, range changes do not automatically cause the validation of defined traffic profiles.

When traffic profiles are imported, they are imported regardless of their configured precedence values. The CMP system displays a message reminding you to check the precedence values of the imported traffic profiles.

Setting UE-Initiated Procedures

When enabled, this feature allows an MPE device to trap UE-Init resource modification requests and reject them using the specified parameters. This feature applies to Gx and Gxx (Gxa, Gxc) interfaces.
To enable or disable processing of UE-Initiated procedures or to change configuration attributes:

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

   The content tree displays a list of global configuration settings.
2. From the content tree, select the **UE-Initiated Procedures**.

   The UE-Initiated Procedures page opens in the work area group.
3. Click **Modify**.

   The Modify UE-Initiated Procedures page opens.
4. Enter values for the configuration attributes:
   a. **Reject UE-Initiating Request** — Select to enable this feature to reject UE-Initiated resource modification requests gracefully, or leave unchecked to process normally with no impact (by ignoring specific AVPs relevant to the UE-Initiated procedure request). The default is unchecked (disabled).
   b. **Experimental Result Code** — Enter the numeric value that is returned in the Experimental-Result-Code AVP as part of the CCA message (if no configured code exists). Enter an integer between 0 and 2,147,483,647. The default value is 5144.
   c. **Experimental Result Code Name** — Enter the description of the error that is returned in the Experimental-Result-Code AVP as part of the CCA message. Enter a string value up to 255 characters in length. The default name is DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED.
   d. **Experimental Result Code Vender Id** — Enter the vender ID that is included in the Experimental-Result-Code AVP as part of the CCA message. Enter an integer between 0 and 2,147,483,647. The default ID is 10415.

   e. **Experimental Result Code Vendor Name** — Enter the vender name that is included in the Experimental-Result-Code AVP as part of the CCA message. Enter a string value up to 255 characters in length. The default name is 3GPP.

5. Click **Save**.

The UE-initiated attributes are configured.

Setting Stats Settings

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

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

To change stats settings:

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

   The content tree displays a list of global configuration settings.

2. From the content tree, select the **Stats Settings** folder.

   The Stats Settings page opens in the work area.

3. Click **Modify**.

   The fields become editable.

4. Set the **Stats Collection Period**. When **Stats Reset Configuration** is set to Interval, specify the time interval after which stats are written to the Policy Management devices from the list. Options are minutes.

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

5. Click **Save**.

The Stats Settings attributes are configured.

Setting Quota Settings

This feature defines the quota pools.
To enable or disable processing of the Quota Settings procedures or to change configuration attributes, do the following:

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

   The content tree displays a list of global configuration settings.

2. From the content tree, select the **Quota Settings** folder.

   The Quota Settings page opens in the work area.

3. Click **Modify**.

   The Quota Settings page refreshes with pooled quota settings editable.

4. Enter values for the configuration attributes:

   a. **Enable subscriber pools**—The global configuration setting for a pooled quota is enabled if the box is checked.

   b. **Enable pooled quota usage tracking**—This allows both individual quota usage tracking and pool quota usage tracking to occur simultaneously.

   c. **Enable pooled entity state**—A defined policy which allows you to update individual entity states or pool entity states or both.

   > **Note:**
   >
   > A subscriber can only be associated with one pool.

   d. **Enable pooled dynamic quota**—Enables pooled dynamic quotas for passes. The default is disabled.

   e. **Enable Pass Expiration Extension**—Allows the expiration date and time value of a pass to be extended to match a later expiration date and time value of a pass that has the same name or is in the same pass group.

5. Click **Save**.

The Quota Setting attributes are configured.

Setting eMPS ARP Settings

The Enhanced Multimedia Priority Service (eMPS) feature allows prioritization of IMS-based calls. The feature allows National Security/Emergency Preparedness users to make calls over the public network when the network is congested by giving those calls/sessions priority in the network over other traffic.
The values configured through the CMP system, using the process below, are used as the default Allocation and Retention Policy (ARP) values for all MPE devices associated with the CMP system when a session is identified as Priority and the ARP values are not defined through policy.

To enable or disable prioritization of IMS-based calls:

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

   The content tree displays a list of global configuration settings.

2. From the content tree, select the **eMPS ARP Settings** folder.

   The Priority Value page opens in the work area.

3. Click **Modify**.

   The eMPS ARP Settings page opens.

4. Enter values for the configuration attributes:

   a. **Priority Value**—Defines the relative importance of a resource request. Enter a value from 1 to 15. The default is 1.

   b. **Preemption Capability**—Defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. Select **Enable** or **Disable** from the list. The default is **Enable**.
   c. **Preemption Vulnerability**—Defines whether a service data flow can lose the resources assigned to it so that a service data flow with a higher priority level can be admitted. Select **Enable** or **Disable** from the list. The default is **Disable**.
5. Click **Save**.

The eMPS ARP Settings attributes are configured.

Setting GCS ARP Settings

The Group Communication Service (GCS) feature allows you to prioritize group communication sessions from an Application Function acting as a Group Communication Service application server. Prioritizing traffic from GCS application servers allows public safety groups, like police and emergency medical services, to communicate over the public network when the network is congested.
The values configured through the CMP system, using the process below, are used as the default GCS Allocation and Retention Policy (ARP) values for all MPE devices associated with the CMP system when a session is identified as a group communication session and the ARP values are not defined through policy.

To enable or disable prioritization of group communication sessions:

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 **GCS ARP Settings** folder.

   The Priority Value page opens in the work area.
3. Click **Modify**.

   The GCS ARP Settings page opens.
4. Enter values for the configuration attributes:
   a. **Priority Value**—Defines the relative importance of a resource request. Enter a value from 1 to 15. The default is 1.
   b. **Preemption Capability**—Defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. Select **Enable** or **Disable** from the list. The default is **Enable**.
   c. **Preemption Vulnerability**—Defines whether a service data flow can lose the resources assigned to it so that a service data flow with a higher priority level can be admitted. Select **Enable** or **Disable** from the list. The default is **Disable**.
5. Click **Save**.

The GCS ARP Settings attributes are configured.

Setting PDN APN Prefixes

Access point name (APN) prefix matching on the MPE device is performed by reading the APN prefixes configured on the CMP system. An APN is considered a match based on the longest prefix 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 prefix match for a PDN connection. After it is created, each new PDN connection for that APN updates the current object. If a stats object has not been created for an APN prefix, the stats object is not displayed in the APN reports page.

If the MPE device receives a PDN connection without a configured APN prefix match, then the connection is added to a stats object called OtherAPN.

PDN connections per APN prefix are shown in the PDN APN prefix report. See prefix for more information.

Up to 25 different APN prefixes can be configured. Each prefix is limited to 64 characters.

To configure PDN APN prefixes:

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 Prefixes** folder.

   The PDN APN Prefix Administration page opens in the work area, listing the configured PDN APN prefixes.
3. Click **Create PDN APN Prefix**.
4. Enter the following values:
   a. **Name**— Enter the name of the APN prefix.
   b. **Value**—Enter a value for the APN prefix.
   c. **Description**—Enter descriptive text.
5. Click **Save**.

The PDN APN prefix is created.

Configuring the Activity Log

The Activity Log allows the real-time tracing activity of Gx and Rx protocol messages to be performed for a specific subscriber from multiple MPE devices.

After activation, traces for subscriber protocol messages are merged from all MPE devices in the network to the CMP system. Messages are selected for tracing based on subscriber identification.

Up to 100 subscriber IDs can be configured in the subscriber configuration window with tracing enabled or disabled. Tracing can be enabled for up to 20 subscribers.

After tracing is enabled, the following associated tasks can be performed:

- Modify subscriber tracing configuration settings and add subscribers for tracing
- Activate and deactivate trace log backup
- View and export historical trace log data
- View and export real-time trace data for up to 10 subscribers

See Subscriber Activity Log for information on performing these tasks.

To enable subscriber tracing, do the following:

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

   The content tree displays a list of global configuration settings.
2. From the content tree, select **Activity Log Configuration**.

   The Activity Log Configuration page opens in the work area.
3. Click **Modify**

   The fields become editable.
4. Enter the number of subscribers for which tracing can be performed in the **Max Subscriber Trace Count** field. The subscriber trace count can be a value of 1 to 100. The default is 100.
5. Enter the number of active subscribers for which tracing can be performed in the **Max Active Subscriber Trace Count** field. The default is 20. Up to 20 subscribers can be enabled for tracing.
6. Click **Save**.

Subscriber tracing is enabled.

Configuring Custom APNs

Custom Access point name (APN) configuration on the MPE device, when the setting is set to true, overrides the behavior of the DIAMETER.ENF.AFDirectReply setting on a per APN basis.

When the DIAMETER.ENF.AFDirectReply setting is set to true, all Rx processing can be synchronous for specific APNs.

The Custom APNs Configuration display has three screens:

- Synchronous APNs
- Session Recovery APNs—Allows a session recovery.
- Session Synch APNs—Allows you to enable or disable Gx Session-Sync on a per APN per MPE basis.

To configure custom APNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Custom APNs Configuration** folder.
3. Click **Modify**.
4. To configure Synchronous APNs:
   a. On the Custom APNs Configuration page, select the **Synchronous APNs** section.
   b. Enter a **Synchronous APN** (for example, `xyz1.oracle.com`).
   c. Click **Add** to add the new Synchronous APN to the list.
   d. To delete an APN, select the APN in the list and click **Delete**.
   e. Click **Save**.
5. To configure Session Recovery APNs:
   a. On the Custom APNs Configuration page, select the **Session Recovery APNs**section.
   b. Enter the name of the **Session Recovery APN**.

   c. Click **Add** to add the Session Recovery APN.
   d. To delete a Session Recovery APN, select the APN in the list and click **Delete**.
   e. Click **Save**.
6. To configure a Session Synch APN:
   a. On the Custom APNs Configuration page, select the **Session Synch APNs**section.
   b. Enter a **Session Synch APN**.
   c. Click **Add** to add the Session Synch APN.
   d. To delete a Session Synch APN, select the APN in the list and click **Delete**.
   e. Click **Save**.

The custom APNs are configured.

About Emergency APNs Settings

The MPE determines if an IP-CAN Session requires an IMS emergency session based on the PDN-id. The MPE device stores a configurable list of Emergency APNs that are valid for the the MPE device. For emergency APNs, the IMSI cannot be present. The MPE device supports requests for PCC and QoS Rules that do not include an IMSI. See Viewing the Audit Log.

The MPE device verifies the Service-URN if the IMS service information is associated with a UE IP address belonging to an emergency APN. The MPE device stores a configurable list of Service-URNs designated for emergency services. If the IMS service information does not contain an emergency-related indication and the UE IP address is associated with an emergency APN, the MPE rejects the IMS service information provided by the AF.

The Emergency APNs Settings display has two tabs:

- **Emergency APNs**
- **Emergency Service-URNs**

Adding Emergency APNs Settings

To add emergency APNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency APNs** section.
5. Enter an emergency APN.
6. Click **Add** to add the emergency APN to the list.
7. Click **Save**.

Deleting Emergency APNs Settings

To delete emergency APNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.

2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency APNs** section.
5. Select the emergency APN in the list.
6. Click **Delete**.
7. Click **Save**.

Adding Emergency Service-URNs Settings

To add emergency Service-URNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency Service-URNs** section.
5. Enter an emergency service-URNs.
6. Click **Add** to add the new emergency service-URN to the list.
7. Click **Save**.

Deleting Emergency Service-URNs

To delete emergency Service-URNs:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Emergency APNs Settings** folder.
3. Click **Modify**.
4. Select the **Emergency Service-URNs** section.
5. Select the emergency service-URN in the list.
6. Click **Delete**.
7. Click **Save**.

18

System Administration

This chapter describes functions reserved for CMP system administrators.

> **Note:**
>
> Some options are visible only when you are logged in with administrative rights to the CMP system. However, the **Change Password** option is available to all users.

Configuring System Settings

Within the CMP system you can define the settings that control system behavior.

To define system settings:

1. From the **System Administration** section of the navigation pane, select **System Settings**.

   The System Settings page opens in the work area, displaying the current system settings.

2. Click **Modify**.

   The System Settings page opens.

3. In the Configuration section, define the following:

   a. **Idle Timeout (minutes; 0=never)**—The interval of time, in minutes, that a user login 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 a message indicating that the maximum number of concurrent sessions has been reached.

   d. **Password Expiration Period (days; 0=never)**—The number of days a password can be used before it expires. Enter a value from 7 to 365, or 0 to indicate that the password never expires.

   e. **Password Expiration Warning Period (days; default=3)**—The number of days before a password expires to begin displaying a window to users after login warning that their password is expiring.

f. **Admin User Password Expiration**—By default, the password for the `admin` user never expires.

   If you select this option, the `admin` user is subject to the same password expiration policies as other users.

g. **Block users when password expires**—By default, after a password expires, the user must immediately change it at the next login.

   If you select this option, if their password expires, users cannot log in at all. (If you select **Admin User Password Expiration** and the `admin` user's password expires, the user can still log in but must immediately enter a new password.)

h. **EMS Shared Secret**—Field provided to support third-party single sign-on architectures.

i. **Minimum Password Length**—The minimum allowable length in characters for a password, from 6 to 64 characters.

   The default is six characters.

j. **Login Banner Title**—The banner that displays on the login page. The default is "Welcome." You can enter up to 30 characters.

k. **Login Banner Text**—The text that displays on the login page. You can enter up to 10,000 characters.

l. **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.

m. **Allow policy checkpoint and restore (copies; 0=disallow)**—The number of checkpoints allowed in the system. Valid value range is 0 to 10. If set to 0, the Policy Checkpoint/Restore option is turned off and is no longer visible under the Policy Management heading on the navigation panel. The default value is 0.

n. **Object's "name" attribute validation rule** (Debug mode only)—Defines the valid characters in manageable object names in the CMP database; specified as a regular expression. By default, names can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). Changing characters could allow users to create names that are not accepted by external systems.

4. In the Invalid Login Threshold Settings section, define the following:

   a. **Enable**—Enables login threshold control.

      By default, this feature is enabled; deselect the check box to disable this feature.

   b. **Invalid Login Threshold Value**—Defines the maximum number of consecutive failed logins after which action is taken.

      Enter a value from 1 through 500; the default is 3 attempts.

   c. **Action(s) upon Crossing Threshold**—The system action to take if a user reaches the invalid login threshold:

      - **Lock user account**—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 from which the login attempts was made. The default level is **Warning**; to change the event level, select a different level from the list.

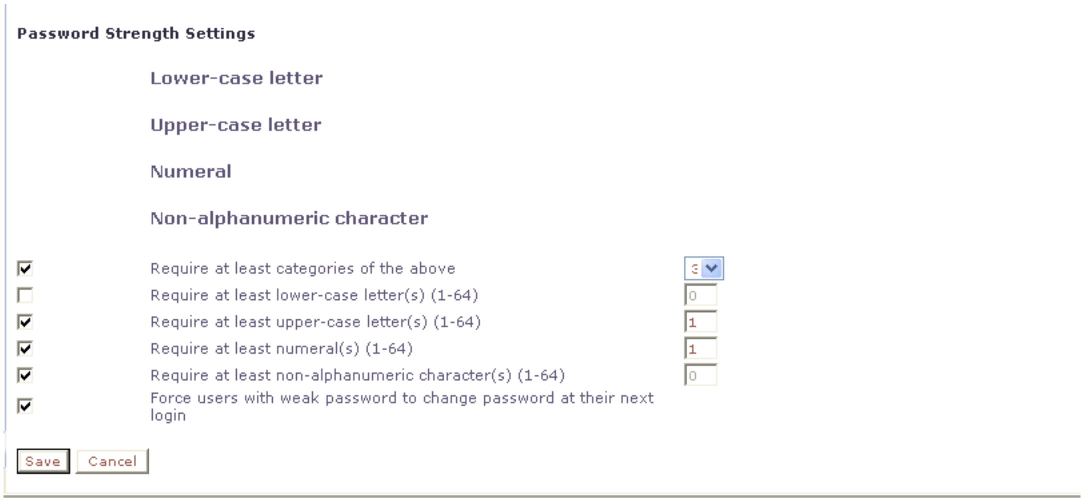
5. The Password Strength Settings section lists four character categories: lowercase letters, uppercase letters, numerals, and non-alphabetic characters. You can specify a password strength policy that requires users to create passwords by drawing from these categories:

- **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-alphanumeric character(s) (1-64)**—By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 non-alphabetic characters in their passwords.
- **Force users with weak password to change password at their next login**—By default, this setting is disabled. Select it to require users to conform to a new password policy effective the next time they log in.

6. Click **Save**.
7. To refresh the CMP system, log out and log back in.

The system settings are configured.
Figure 18-1 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 18-1   Sample Password Strength Policy



Password Strength Settings

Lower-case letter

Upper-case letter

Numeral

Non-alphanumeric character

☑	Require at least categories of the above	3
☐	Require at least lower-case letter(s) (1-64)	0
☑	Require at least upper-case letter(s) (1-64)	1
☑	Require at least numeral(s) (1-64)	1
☑	Require at least non-alphanumeric character(s) (1-64)	0
☑	Force users with weak password to change password at their next login	

Importing and Exporting Configurable Objects

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

You can export configuration information as a single ZIP file. This ZIP file contains an inner ZIP file of XML files, an MD5 checksum file for data verification, and an `exportResults.txt` file containing export result messages. You can use these exported XML or ZIP files to update configurable objects in a CMP system or to configure a new system.

> **Note:**
>
> For CMP systems within NW-CMP manager, the **Import/Export** action is only available for NW-CMP servers. S-CMP servers do not show this action.

User Privileges and Import/Export

To use the **Import/Export** action, you must have a role that includes the **System Administrator Privileges Import / Export** privilege.

> **Note:**
>
> If the you have a role with the **Import / Export** privilege, then top-level objects are available for importing and exporting even though you may not have specific privileges to view the objects (that is, the specific object is hidden to your role).

See Creating a Role for details on roles and privileges.

If you are expected to perform checkpoint operations during an import action, you must have a role that includes **Policy Management Privileges** with **Read-Write** access to **Policy Checkpoint**. See Checkpoint and Importing Objects for more information.

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.
- **Subscriber Interface**
  Allows you to manage and query quota profiles, conventions, subscriber accounts and tiers.
- **Identity Management**
  Allows you to configure user names, passwords, and roles.
- **Policy Tables**
  Allows you to export policy tables, and import them to add, edit, replace or delete a table.

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

About Importing Configuration Objects

The CMP system exports configurable objects to a ZIP file. This ZIP file consists of an inner ZIP file, `export.zip`, containing XML files of configuration data (by object type), an MD5 checksum file (`md5.txt`), and an `exportResults.txt` message file. By default, during an import, the CMP system uses the MD5 file to verify the integrity of the import file.

The Import function provides a method for importing either XML or ZIP configuration data files. In this way, the CMP configurable objects in a system can be restored to a prior configuration or a new CMP system created and configured.

Another import option allows the CMP system to use the Checkpoint function to save a snapshot of all existing configuration objects. If necessary, this snapshot can be used to restore the system to its previous configuration. See Checkpoint and Importing Objects for more information. Refer to the *Policy Wizard Reference* for details on managing policy checkpoints.

See About Adding Objects for Export for details on exporting configuration objects.

Checkpoint and Importing Objects

> **NOT_SUPPORTED:**
>
> To use the checkpoint option, the **Allow policy checkpoint and restore** setting must be configured in **System Settings**. See Configuring System Settings.

During an import action, the CMP system includes the **Perform checkpoint before importing** option. This is a protective measure that uses the Checkpoint function to save a snapshot of all the configuration objects that exist in the system. See the *Policy Wizard Reference* for more checkpoint details. Included in the checkpoint output file are:

- Configurable objects such as policies, policy groups, policy templates, policy tables, traffic profiles, match lists, retry profiles, applications, policy counter IDs, MPE configuration templates, and traffic profile groups, RADIUS CoA templates
- All MPE templates
- Associations between virtual MPE templates and real MPE templates
- Associations between MPEs and virtual MPE templates
- Associations between virtual MPE templates and other configuration objects (for example, policies)

Enabling the checkpoint option ensures that if a newly reconfigured system fails to function as expected, a checkpoint XML file exists that returns the system to the state prior to the import action. An additional benefit is that the checkpoint output file is saved in the CMP database and is accessible using **Policy Checkpoint/Restore** under the **Policy Management** section. Refer to the *Policy Wizard Reference* for details on managing checkpoint files.

In a networked CMP system, the checkpoint function is limited to the NW-CMP server. The **Perform checkpoint before importing** option is not available for S-CMP servers. After a restoration from a checkpoint onto a NW-CMP server, the NW-CMP server pushes the restoration data to all S-CMP servers. The MPE and virtual MPE templates are not updated.

Real MPE templates and related associations are restored on the S-CMP servers, so that the policies can be restored to MPE through the virtual template.

The **Checkpoint** function differs from the **Export All** function in the following ways:

- The output file is an XML file that is saved in the CMP database.
- MPE template associations are saved.

See #unique_483 for details on exporting all configurable objects.

Importing Configuration Object Files

To import XML or ZIP files, use the following file naming conventions:

- If you are importing a ZIP file, the filename for the inner ZIP file must be `export.zip`.
- If you are importing a series of XML files, Oracle recommends the file naming convention `obj_type + Export[sequence_number] + *.xml`. For example:
  - `networkelementExport1_20150501.xml`
  - `networkelementExport2_20150501.xml`
  - `networkelementExport3_20150501.xml`

> **Note:**
>
> If there are multiple files of one type, the sequence number is necessary. Any object groups for import should be included in the last file of the sequence.

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Import**.

   The import file upload form and options appear.
3. Click **Browse** to locate the file to be imported.
4. Select a processing option to use to **Handle collisions between imported items and existing items**:
   - **Delete all before importing**
     The CMP system deletes all objects for each object type matching the import file before importing the object type XML file.

     > **NOT_SUPPORTED:**
     >
     > This import strategy can result in object inconsistency. For example, if you import a ZIP file that only contains traffic profiles, all the traffic profiles are deleted first. However, if existing policies depend on the existing traffic profiles, and the import file does not contain them, the policies can become invalid.

   - **Overwrite with imported version**
     For each object in the import file, if the object exists in the CMP system, the import updates the object with the configuration contained in the import file. If an object does not exist, the CMP system adds the object to the system.
   - **Reject any that already exist**

For objects that already exist in CMP system, the import action does nothing. For objects that do not exist in the CMP system, the import adds the objects to the system.

- **Any collisions prevent all importing**
  The CMP system compares all objects in the import file with objects in the system. If any object exists, the entire import is canceled.
- **Validate without importing**
  If an MD5 file (part of the ZIP file) is present, the CMP system performs an MD5 checksum on the ZIP file and compares the hash value with that in the MD5 file. If the hash values match, the system validates each XML file contained in the inner ZIP file. The CMP system then performs a collision check between the system and the XML files and indicates if any exists.

5. Select one or more **Options**:
   - **Skip checksum**
     If unselected and an MD5 file (part of the ZIP file) is present, the CMP system performs a checksum on the inner ZIP file and compares the hash value with that of the MD5 file from the ZIP file. If the values do not match, the import action is canceled.

     If selected, the CMP system does not perform a checksum and proceeds with the import.
   - **Perform checkpoint before importing**
     If selected, the CMP system uses the **Checkpoint** function to save a file with all the configuration objects that exist in the system. The checkpoint file is saved in the CMP database. See Checkpoint and Importing Objects for more information.
6. Click **Import**.

The configuration objects and their configuration settings are imported into the CMP database. After the import is complete, the window reports the results for each XML file contained in the ZIP file. Results include whether a file was successfully imported or the number of objects successfully updated. Any problems during the import action appear in red text.

> **Note:**
>
> As the result of memory limitations, the CMP system only displays the first 2000 characters for each import type file.

The checkpoint file and the checkpoint management functions are accessed using **Policy Checkpoint/Restore** under the **Policy Management** section. Refer to the *Policy Wizard Reference* for details on managing policy checkpoint files.

About Exporting Configuration Objects

The Export action provides a method for exporting CMP configuration information as a ZIP file. Using this file, the configurable objects can be restored to a prior configuration or a new system can be created and configured.

As part of the export action, the CMP system performs the following actions:

1. Exports the configuration objects as individual XML files by object type.

> **Note:**
>
> Network Element, Policy, and Policy Counter ID objects will be exported into multiple XML files. Network Element files contain a maximum of 500 objects per file. Policy files contain a maximum of 10000 objects per file. Policy Counter ID files contain a maximum of 10000 objects per file.

2. Compresses the XML files into a ZIP file named `export.zip`.
3. Creates the `exportResults.txt` file containing export result messages.
4. Calculates MD5 checksum number for `export.zip` and creates an `md5.txt` file containing the MD5 number.
5. Compresses the `md5.txt`, `exportResults.txt`, and `export.zip` files into another ZIP file named `CMP_export__`*yyyyMMddhhmmss*`.zip`.
6. Downloads the `CMP_export`ZIP file to the local computer.

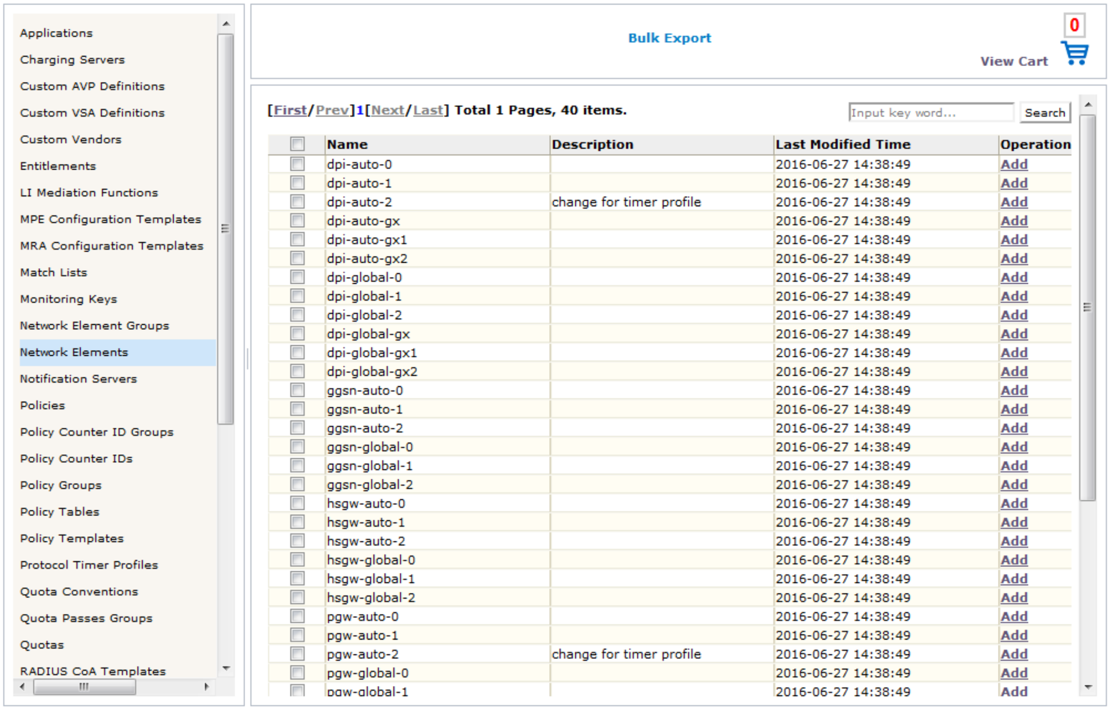
To restore or configure a CMP system, see Importing Configuration Object Files.

Export Window Overview

The Bulk Export window is divided into three areas.

- Object List
  The left pane lists all of the configurable object types in CMP that are available for export. The top pane contains the **View Cart** link and a counter for the total number of objects in the cart.
- Work Area
  The work area lists all of the configured objects for the selected object type. Objects are listed by Name in ascending alphabetical order. A maximum of 50 objects per page are shown.
- Navigation Area
  Page navigation links appear at the top left of the work area. A **Search** text box appears at the top right of the work area. You can search the entire list of objects for specific strings and numbers. The **Search** text box accepts the wildcard (%) and underscore (_) characters.

Figure 18-2 Bulk Export Window



[First/Prev]1[Next/Last] Total 1 Pages, 40 items.

□	Name	Description	Last Modified Time	Operation
□	dpi-auto-0		2016-06-27 14:38:49	Add
□	dpi-auto-1		2016-06-27 14:38:49	Add
□	dpi-auto-2	change for timer profile	2016-06-27 14:38:49	Add
□	dpi-auto-gx		2016-06-27 14:38:49	Add
□	dpi-auto-gx1		2016-06-27 14:38:49	Add
□	dpi-auto-gx2		2016-06-27 14:38:49	Add
□	dpi-global-0		2016-06-27 14:38:49	Add
□	dpi-global-1		2016-06-27 14:38:49	Add
□	dpi-global-2		2016-06-27 14:38:49	Add
□	dpi-global-gx		2016-06-27 14:38:49	Add
□	dpi-global-gx1		2016-06-27 14:38:49	Add
□	dpi-global-gx2		2016-06-27 14:38:49	Add
□	ggsn-auto-0		2016-06-27 14:38:49	Add
□	ggsn-auto-1		2016-06-27 14:38:49	Add
□	ggsn-auto-2		2016-06-27 14:38:49	Add
□	ggsn-global-0		2016-06-27 14:38:49	Add
□	ggsn-global-1		2016-06-27 14:38:49	Add
□	ggsn-global-2		2016-06-27 14:38:49	Add
□	hsgw-auto-0		2016-06-27 14:38:49	Add
□	hsgw-auto-1		2016-06-27 14:38:49	Add
□	hsgw-auto-2		2016-06-27 14:38:49	Add
□	hsgw-global-0		2016-06-27 14:38:49	Add
□	hsgw-global-1		2016-06-27 14:38:49	Add
□	hsgw-global-2		2016-06-27 14:38:49	Add
□	pgw-auto-0		2016-06-27 14:38:49	Add
□	pgw-auto-1		2016-06-27 14:38:49	Add
□	pgw-auto-2	change for timer profile	2016-06-27 14:38:49	Add
□	pgw-global-0		2016-06-27 14:38:49	Add
□	pgw-global-1		2016-06-27 14:38:49	Add

When operating in Debug mode, the Accounts and Tiers objects are included in the Object List.

> **Note:**
>
> The Accounts object depends on Network Elements and Tiers objects.

About Adding Objects for Export

The Export action has different methods for selecting export objects:

- **Add**
  Adds a single object to the export cart. See Exporting a Configuration Object.
- **Add selected items**
  Adds selected objects to the export cart. See Exporting Multiple Selected Objects.
- **Add filtered items**
  Adds the results of a search to the export cart. See Exporting Multiple Filtered Objects.

After configuration objects have been added to the export cart, they are ready for export.

See Exporting All Configuration Objects for details on exporting all configurable objects.

Exporting a Configuration Object

To export a configuration object:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export**.

The Bulk Export page opens with a listing of exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the object type from the left pane (for example, **Users**).

   A list of configured objects for the specified type displays in the work area.

4. To include dependent objects in the export file, select **Include Dependencies**.

   Any object dependencies for the selected objects will also be selected for export.

5. Use the pagination links at the top left of the work area to locate the object for export.

6. Click **Add** for the object to export.

   A message displays indicating the named object has been successfully added to the cart.

7. Click X to close the message.

   > **Note:**
   >
   > If **Include Dependencies** is checked, the total number of items in the export cart may exceed the number of items checked in the list.

8. Click **View Cart** or 🛒 to continue with the export.

   The Check out Page opens.

9. To remove an object from the listing, use any of the following methods:

   - Click **Remove** next to the named object.
   - Select the check box next to the named object and click **Remove selected items**.
   - Use the **Search** tool to search the list for a specific string to remove and click **Remove filtered items**.

10. After the export list of objects is complete, click **Export Cart**.

    A warning message displays verifying that you want to export the select item in the shopping cart.

11. Click **OK** to proceed with the export.

12. Click **Clear Cart**.

    The contents of the export cart are removed.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention: `CMP_export_`*`yyyyMMddhhmmss`*`.zip`.

Exporting Multiple Selected Objects

To export multiple selected objects:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.

2. Select **Export**.

   The Bulk Export page opens with a list of the exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the object type from the left pane (for example, **Users**).

   A list of configured objects of the specified type displays in the work area.

4. To select all objects on the page for export:

a. Select the check box next to the Name heading of the table.

   All objects listed on the page are selected.

   > **Note:**
   >
   > Your selections only apply to the current page. Objects on other pages are not selected.

b. Click **Add selected items** to add all objects in the filtered list to the export cart.

A message displays indicating the selected objects have been successfully added to the export cart.

5. To select several objects from multiple pages for export:

   a. Use the pagination links at the top left of the work area to locate the first page of objects for export.

   b. Select the check box next to the name of each of the objects to be exported.

   c. Click **Add selected items** to add the selected objects to the export cart.

   d. Use the pagination links at the top left of the work area to locate the next page of objects for export.

   e. Select the check box next to the name of each of the objects to be exported.

   f. Click **Add selected items** to add the selected objects to the export cart.

   A message displays indicating the selected objects have been successfully added to the export cart.

6. Click the X to the right of the message to close the message.

7. Click **View Cart** or 🛒 to continue with the export.

   The Check out Page opens.

8. Review the listing of objects.

9. To remove an object from the listing, use one of the following methods:

   - Click **Remove** next to the named object.
   - Select the check box next to the named object and click **Remove selected items**.
   - Use the **Search** tool to search the list for a specific string and click **Remove filtered items**.

   > **Note:**
   >
   > Any checked items will become unchecked if you change pages.

10. To view a filtered list of export objects by object type:

    a. Click the **Type** list and select the object types.

    b. Click **Search**.

    All of the selected object types display in the list.

> **Note:**
>
> The remaining object types are still in the export cart. To view the entire contents, select **All** from the **Type** list and click **Search**.

11. When the list of objects is ready, click **Export Cart**.

    A warning message displays verifying that you want to export the select items in the shopping cart.

12. Click **OK** to proceed with the export.
13. Click **Clear Cart**.

    The contents of the export cart are removed and you can proceed with another export.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention: `CMP_export_`*`yyyyMMddhhmmss`*`.zip`.

Exporting Multiple Filtered Objects

To export multiple filtered objects:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export**.

   The Bulk Export page opens with a listing of exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the object type from the left pane (for example, **Users**).

   A list of configured objects of the specified type displays in the work area.

4. To include dependent objects in the export file, select **Include Dependencies**.

   Any object dependencies for selected objects will also be selected for export.

5. To export a subset of objects, use the **Search** tool to search the list.

   > **Note:**
   >
   > The text box accepts the wildcard (%) and underscore (_) characters.

   The list of objects is filtered to a subset of objects matching the search criteria.

6. Click **Add filtered items** to add all objects in the filtered list to the export cart.

   A message displays indicating the objects has been successfully added to the export cart.

7. Repeat the search for other filter criteria.
8. Click the X to the right of the message to close the message.
9. Click **View Cart** or 🛒 to continue with the export.

   The Check out Page opens.

10. Review the listing of objects.
11. To remove an object from the listing, use one of the following methods:
    - Click **Remove** next to the named object.

- Select the check box next to the named object and click **Remove selected items**.
- Use the **Search** tool to search the list for a specific string and click **Remove filtered items**.

> **Note:**
>
> Any checked items will become unchecked if you change pages.

12. To view a filtered list of export objects by object type, click the **Type** list, select the object types, and click **Search**.

    All of the selected object types are shown in the list.

    > **Note:**
    >
    > The remaining object types are still in the export cart. To view the entire contents, select **All** from the **Type** list and click **Search**.

13. After the export list of objects is complete, click **Export Cart**.

    A warning message displays verifying that you want to export the select items in the shopping cart.

14. Click **OK** to proceed with the export.
15. Click **Clear Cart**.

    The contents of the export cart are removed and you can proceed with another export.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention: `CMP_export_`*`yyyyMMddhhmmss`*`.zip`.

Exporting Configuration Object Groups

To export configuration object groups:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export**.

   The Bulk Export page opens with a listing of exportable CMP object types in the left pane and a work area for selecting objects for export on the right.

3. Select the group object type from the left pane (for example, **Network Element Groups**).

   A list of object groups are shown in the work area.

4. To include dependent objects in the export file, select **Include Dependencies**.

   Any object dependencies for the selected group will also be selected for export.

5. For each group you want to export, click the check box next to the group Name.
6. Click **Add selected items** to add the selected groups to the export cart.

   A message displays indicating the objects has been successfully added to the export cart.

7. Click the X to the right of the message to close the message.

> **Note:**
>
> If **Include Dependencies** is checked, the total number of items in the export cart may exceed the number of items checked in the list.

8. Click **View Cart** or 🛒 to continue with the export.

   The Check out Page opens.

9. Review the listing of objects.

10. To remove an object from the listing, use one of the following methods:

    - Click **Remove** next to the named object.
    - Select the check box next to the named object and click **Remove selected items**.
    - Use the **Search** tool to search the list for a specific string and click **Remove filtered items**.

11. To view a filtered list of export objects by object type, click the **Type** list, select the object types, and click **Search**.

    All of the selected object types are shown in the list.

    > **Note:**
    >
    > The remaining object types are still in the export cart. To view the entire contents, select **All** from the **Type** list and click **Search**.

12. After the list of objects is ready, click **Export Cart**.

    A warning message displays verifying that you want to export the select items in the shopping cart.

13. Click **OK** to proceed with the export.

14. Click **Clear Cart**.

    The contents of the export cart are removed and you can proceed with another export.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention: `CMP_export_`*`yyyyMMddhhmmss`*`.zip`.

Exporting All Configuration Objects

The **Export All** function exports a ZIP file to the local computer that contains all of the exportable types of configuration objects.

> **Note:**
>
> **Export All** does not include associations between policies and MPE templates.

To export all configuration objects:

1. From the **System Administration** section of the navigation pane, expand **Import/Export**.
2. Select **Export All**.

The Bulk Export page appears.

3. Click **Export All**.

A ZIP file is downloaded to your local computer. The filename uses the following naming convention: `CMP_export_`*`yyyyMMddhhmmss`*`.zip`.

About the Manager Reports

The Manager Reports function provides information about the CMP cluster itself. This information is similar to the Cluster Information Report for MPE and MRA clusters. The display is refreshed every ten seconds.

Viewing Manager Reports

To view Manager Reports:

1. From the **System Administration** section of the navigation pane, select **Reports**.

   The Manager Reports page opens in the work area.

2. To manage the reports:

   - To pause refreshing the display, click **Pause**.
     The report does not update.
   - To resume refreshing the display, click **Resume**.
     The report refreshes every 10 seconds.
   - To reset the display counters, such as the number of blade failures, click **Reset Counters**.
     The counters in the report are reset to zero.

   The fields that are displayed in the Manager Reports include the following:

   - **Cluster Name and Designation**
     The name of the cluster and whether it is the primary **(P)** or secondary **(S)** site.
   - **Mode**
     The status of the cluster:
     – **Active**
       The cluster is managing the Policy Management network.
     – **Standby**
       The cluster is not currently managing the Policy Management network.
     – **Paused**
       The report is paused. Click **Resume** to return the **Mode** to **Active**.
   - **Cluster Status**
     The status of the servers within the cluster:
     – **On-line**
       If one server, it is active; if two servers, one is active and one is standby.
     – **Degraded**
       One server is active, but the other server is not available.
     – **Out-Of-Service**
       Neither server is active.
     – **No Data**
       The CMP system cannot reach the server.

Also within the Manager Reports is a listing of the **Blades** (that is, the servers) contained within the cluster. A symbol (🔌) indicates which server currently has the external connection (that is, which server is the active server). The report also lists the following server-specific information:

- **Overall** section
  Displays the current topology:
  - **State**
    Active, Standby, or Forced Standby
  - **Blade Failures**
    Counters
  - **Uptime**
    The time providing active or standby service

    For the definitions of these states, see Server Status.
- **Utilization**
  Displays the current usage statistics:
  - **Disk**
    Percentage utilization of disk (of the `/var/camiant` file system)
  - **CPU**
    Average value for the CPU utilization
  - **Memory**
    Average value for Memory use

The **Actions** links let you **Restart** the CMP software on the server or **Reboot** the server.

About the Trace Log

The trace log is part of system administration records notifications for management activity on the CMP system. For information on configuring the cluster-level messages written to the trace log, see Configuring Log Settings for Servers in a Cluster. For information on configuring the system-level messages written to the trace log, see Configuring the Trace Log.

Configuring the Trace Log

You can configure the trace log severity message levels for the CMP system.

> **Note:**
>
> For information on configuring debug logs, see Configuring Debug Logs.

To configure the trace log:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.

   The Trace Log page opens in the work area.
2. Click **Modify**.

   The Modify Trace Log Settings page opens.
3. Select the **Trace Log Level** from the list.

This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:

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

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

4. Click **Save**.

The trace log is configured.

Viewing the Trace Log

To view the Trace Log:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.

   The Trace Log page opens in the work area.

2. Click **View Trace Log**.

   The Trace Log Viewer window opens. While data is being retrieved, the progress message indicating that the trace logs are being scanned appears.

   All events contain the following information:

   - **Date/Time** — Event timestamp. This time is relative to the server time.

- **Code** — The event code. For information about event codes and messages, see the *Troubleshooting Reference*.
- **Severity** — Severity level of the event. Application-level trace log entries are not logged at a higher level than error.
- **Message** — The message associated with the event. If additional information is available, the event entry shows as a link. Click on the link to see additional detail in the frame below.

By default, the window displays 25 events per page. You can change this to 50, 75, or 100 events per page by selecting a value from the **Display results per page** list.

Events that occur after the Trace Log Viewer starts are not visible until you refresh the display. To refresh the display, click one of the following buttons:

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

3. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search.**

   The trace log for the selected server displays.

4. To filter the log, see Filtering the Trace Log.
5. Click **Close**.

Filtering the Trace Log

The Trace Log can contain a large number of messages. To reduce the number, the log can be filtered using several criteria.
To filter the trace log information:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.

   The Trace Log page opens in the work area.

2. Click **View Trace Log**.

   The Trace Log Viewer window opens. While the data is being retrieved, the a progress message displays.

3. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search.**

   The trace log for the selected server displays.

4. Specify the filtering parameters using any of the following fields.

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

- **Trace Codes**
  Enter one or a comma-separated list of trace code IDs. Trace code IDs are integers up to 10 digits long.
- **Use timezone of remote server for Start Date/Time**
  Select to use the time of a remote server (if it is in a different time zone) instead of the time of the CMP server.
- **Severity**
  Filter by severity level. Events with the selected severity and higher are displayed. For example, if the severity selected is **Warning**, the trace log displays events with the severity level Warning.
- **Contains**
  Enter a text string to search. For example, if you enter `connection`, all events containing the word `connection` display. This field does not use wildcards and is not case specific.

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

5. Click **Search**.

   The filtered log displays.
6. Click **Close**.

   The Trace Log Viewer window closes.

Modifying the Trace Log Configuration

To configure the trace log display:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.

   The Trace Log page opens in the work area, displaying the current trace log configuration.
2. Click **Modify**.

   The Modify Trace Log Settings page opens.
3. Define the settings.

   For a description of the settings, see Configuring Log Settings for Servers in a Cluster.
4. Click **Save**.

The trace log configuration is modified.

About the Audit Log

The audit log lets you track and view activity and changes within the Policy Management system. Using the audit log, you can track and monitor each event, providing you better system control. The audit log is stored in the CMP database, so it is backed up and can be restored.

You can view the entire audit log, search for individual entries, export entries to a text file, or purge entries.

Note:

Audit log data is kept until you choose to purge it.

Viewing the Audit Log

To view the audit log:

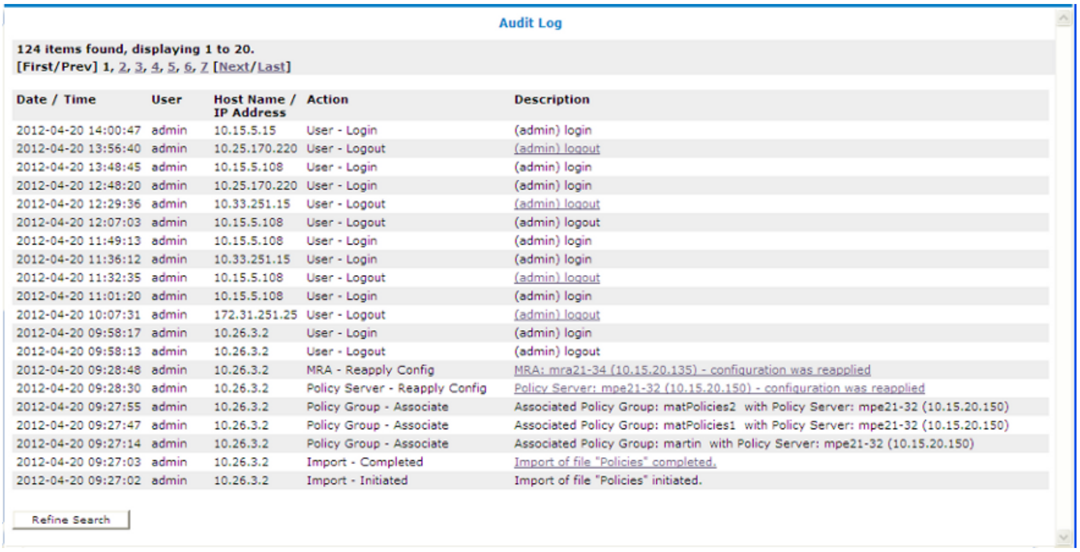
1. From the **System Administration** section of the navigation pane, select **Audit Log**.

   The Audit Log page opens in the work area.

2. On the Audit Log page, click **Show All**.

   The **Audit Log** opens. Figure 18-3 shows an example.

Figure 18-3 Audit Log



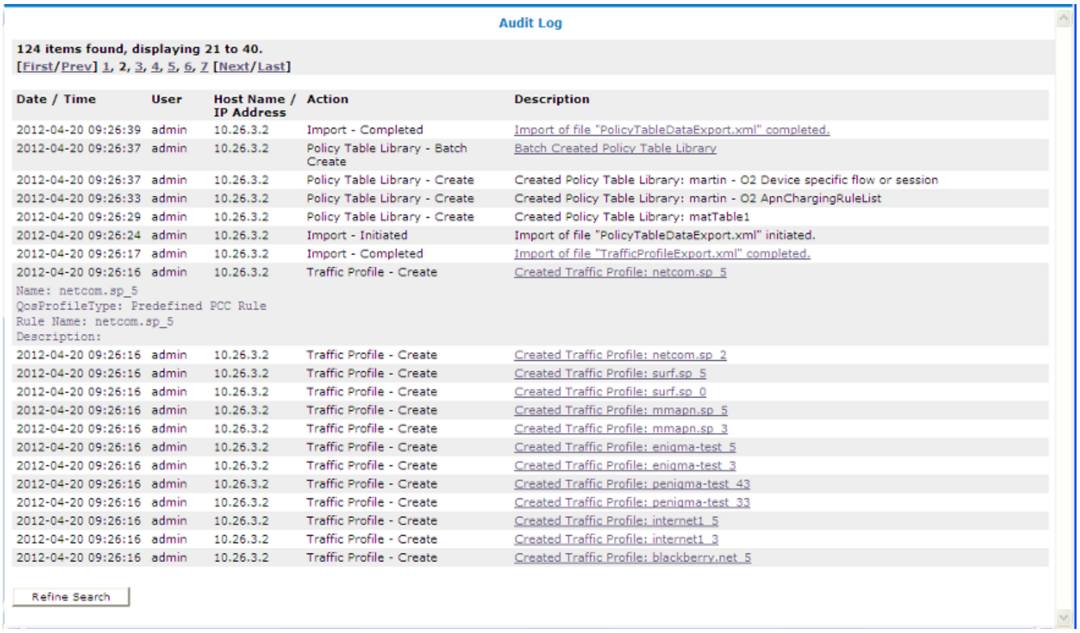
Audit Log

124 items found, displaying 1 to 20.
[First/Prev] 1, 2, 3, 4, 5, 6, 7 [Next/Last]

Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 14:00:47	admin	10.15.5.15	User - Login	(admin) login
2012-04-20 13:56:40	admin	10.25.170.220	User - Logout	(admin) logout
2012-04-20 13:48:45	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 12:48:20	admin	10.25.170.220	User - Login	(admin) login
2012-04-20 12:29:36	admin	10.33.251.15	User - Logout	(admin) logout
2012-04-20 12:07:03	admin	10.15.5.108	User - Logout	(admin) logout
2012-04-20 11:49:13	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 11:36:12	admin	10.33.251.15	User - Login	(admin) login
2012-04-20 11:32:35	admin	10.15.5.108	User - Logout	(admin) logout
2012-04-20 11:01:20	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 10:07:31	admin	172.31.251.25	User - Logout	(admin) logout
2012-04-20 09:58:17	admin	10.26.3.2	User - Login	(admin) login
2012-04-20 09:58:13	admin	10.26.3.2	User - Logout	(admin) logout
2012-04-20 09:28:48	admin	10.26.3.2	MRA - Reapply Config	MRA: mra21-34 (10.15.20.135) - configuration was reapplied
2012-04-20 09:28:30	admin	10.26.3.2	Policy Server - Reapply Config	Policy Server: mpe21-32 (10.15.20.150) - configuration was reapplied
2012-04-20 09:27:55	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: matPolicies2 with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:47	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: matPolicies1 with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:14	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: martin with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:03	admin	10.26.3.2	Import - Completed	Import of file "Policies" completed.
2012-04-20 09:27:02	admin	10.26.3.2	Import - Initiated	Import of file "Policies" initiated.

For a detailed description of an item, click the underlined description. The details of the event display. (Figure 18-4 shows an example.)
To filter search results, click **Refine Search**, located at the bottom of the page. (See Searching for Audit Log Entries.)

Figure 18-4 Audit Log Details



Audit Log

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

Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 09:26:39	admin	10.26.3.2	Import - Completed	Import of file "PolicyTableDataExport.xml" completed.
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Batch Create	Batch Created Policy Table Library
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 Device specific flow or session
2012-04-20 09:26:33	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 ApnChargingRuleList
2012-04-20 09:26:29	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: matTable1
2012-04-20 09:26:24	admin	10.26.3.2	Import - Initiated	Import of file "PolicyTableDataExport.xml" initiated.
2012-04-20 09:26:17	admin	10.26.3.2	Import - Completed	Import of file "TrafficProfileExport.xml" completed.
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: netcom.sp_5
Name: netcom.sp_5 QosProfileType: Predefined PCC Rule Rule Name: netcom.sp_5 Description:				
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: netcom.sp_2
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: surf.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: surf.sp_0
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmapn.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmapn.sp_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: penigma-test_43
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: penigma-test_33
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: internet1_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: internet1_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: blackberry.net_5

Searching for Audit Log Entries

To search for the Audit Log entries:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.

   The Audit Log page opens in the work area.

2. Click **Search**.

   The Audit Log Search Restrictions page opens.

3. Define the following items, depending on how restrictive you want the audit log search to be:

   - **From/To** — Click 📅 (calendar icon), specify a date and time then click **Enter**.
   - **Action by User Name(s)** — Enter the **User Name** of the user or users to audit.
   - **Action on Policy Server(s)** — Enter the name of the Policy Management device to audit.
   - **Audit Log Items to Show** — Specifies the category of items to audit:

     a. When you select some categories, a **Name** field displays, which lets you enter a search string.

     b. Leave the **Name** field blank to include all items.

     c. When you select a category, an **Actions** link displays, which lets you select individual audit log items within the category.
     By default all items in the category are selected, but you can select individual items instead.

     By default you can specify three item categories. Click **More Lines** to add an additional audit log item category.

   - **Results Forms** — Specifies the number of items per page to display, including which data to display (most recent or oldest items).

4. Click **Search**.

   The Audit Log displays search results.

Exporting Audit Log Data

You can export audit log data to a text file. The default file name is `AuditLogExport.txt`. To export audit log data:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.

   The Audit Log page opens in the work area.
2. Click **Export/Purge**.

   The Export and Purge Audit Log Items page opens.
3. In the **Items to Export** section, select one of the following options:
   a. **Export All Items** — Writes all audit log entries.

   b. **Export Through Date** — Click 📅 (calendar icon), and select a date.
4. Click **Export**.

   A standard File Download window opens; you can open or save the export file.

The audit log is exported.

Purging Audit Log Data

To purge data from the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.

   The Audit Log page opens in the work area.
2. Click **Export/Purge**.

   The Export and Purge Audit Log Items page opens.
3. In the **Items to Purge** section, click 📅 (calendar icon) and select a date.
4. Click **Purge**.

   You are prompted with a confirmation message.
5. Click **OK**.

The data is purged from the audit log.

About the Manager Log

The Manager log is a series of files that records information about the operation of CMP components and subcomponents. Log data is appended to component and subcomponent logs (for example, tomcat.log and HTTP.log). When the maximum file size is reached a new file is started. When the maximum number of files is reached the oldest file is deleted.

The Manager Log page is available when the CMP system operates in debug mode. Contact My Oracle Support for more information about enabling debug mode. The Manager Log page lets you configure system-wide default values for the available debug logs for Policy Management components and subcomponents.

Configuring the Manager Log

> **Note:**
>
> To view the **Manager Log** menu in the navigation pane, you must enable **Debug Mode**. Contact My Oracle Support for more information.

You can use the Manager Log to configure the default debug logs severity message levels for the CMP system subcomponents.

> **Note:**
>
> For information on configuring debug logs, see Configuring Debug Logs.

To configure the Manager Log:

1. From the **System Administration** section of the navigation pane, select **Manager Log**.

   The Manager Log page opens in the work area.
2. Click **Modify**.

   The Manager Log page becomes editable.
3. In the **Tomcat Log Configuration** section of the page:
   a. Enter the **Scan Period (Seconds)**.

      The default value is 20 seconds.
   b. Select the **Root Log Level**:

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

> **Caution:**
>
> Before changing any default logging level, consider the implications. Lowering the log level setting from its default value (for example, from **WARN** to **INFO**) causes more notifications to be recorded in the log and can adversely affect performance. Similarly, raising the log level setting (for example, from **WARN** to **ERROR**) causes fewer notifications to be recorded in the log and may cause you to miss important notifications.

4. In the **File Apppender Configuration** section of the page, for each appender file listed:
   a. Enter the **Maximum File Size**.

      The file size is in megabytes.
   b. Enter the **Maximum File Count**.
5. In the **DC Log Configuration** section of the page:
   a. Enter the **Scan Period (Seconds)**.

      The default value is 20 seconds.
   b. Select the **Root Log Level**.
6. In the **File Apppender Configuration** section of the page, for each appender file listed:
   a. Enter the **Maximum File Size**.

      The file size is in megabytes.
   b. Enter the **Maximum File Count**.
7. Click **Save**.

The Manager Log is configured.

Managing Scheduled Tasks

The CMP system runs batch jobs to complete certain operations. These tasks are scheduled to run at regular intervals, with some tasks scheduled to run in a certain order. You can change the scheduling, reschedule, enable or disable these tasks to better manage network load or to propagate a network element change to the Policy Management devices on demand. You can also abort a running task.

> **Caution:**
>
> Oracle recommends that you follow the order in which scheduled tasks are listed. Serious system problems can occur if the order is changed. Consult My Oracle Support before changing the order of task execution.

The tasks include:

Alert Aging
Ensures that alerts age out and are eventually removed from the CMP database. (The valid range is 1 to 365 days.)

Stats Files Synchronization #1, 2, 3, 4
Synchronizes stats files to defined remote server. Up to four synchronization tasks can be defined, and they are scheduled independently. Statistics files are generated and synchronized to external systems only from the active CMP system. This task retries when the remote server is unreachable. The default number of retries is three times in each one minute interval. The maximum number of retries in one minute is five times. If a transfer period is missed, the next time the remote server is reached any files from the missed transfer periods are transferred. Remote server information that must be defined before this task runs is: Host Name/IP address, Remote repository path, and SSH user login and password.

> **Note:**
>
> An external system must be configured before beginning this task. If no external system is configured in any of the Stats File Synchronization tasks, no stats files are generated.

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

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

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

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

> **Note:**
>
> This task depends on the SMS Relay configuration. See #unique_504 for details.

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

> **Note:**
>
> CMPP and Wireless-C mode must be enabled and the CMPP log level must be set to INFO. See the following for detailed information: #unique_505 and #unique_506.

OM Statistics
Periodically retrieves Operational Measurement (OM) statistics from all Policy Management devices.

The Operational Measurements XML interface retrieves operational counters from the system. The OM interface requires that the OM Statistics scheduled task be running on the CMP system. After the specified Stats Collection Period, this task collects the operational counters from the Policy Management devices in the network and records them in the CMP database; the data is then available for query via the OM XML interface. You can configure the task to poll at intervals between 5 minutes and 24 hours, with a default value of 15 minutes; the system keeps the data available for query for 1 to 30 days, with a default value of 7 days. The recommended settings for this task will vary depending on the volume of data you are collecting.

When you request OM statistics, the data for the response is taken from the information that has been collected by this task. You must gather data using the OM Statistics scheduled task if you want data available for subsequent OM queries.

Most values returned as part of the response are presented as the positive change between the start time and end time. To calculate a response, you must have a minimum of two recorded values available; thus you must run the OM Statistics task at least twice in a given time period before you can obtain any statistical data from the OSSI XML interface. *OSSI XML Interface Definitions Reference* describes the OM Interface and the OM Statistics in detail.

> **Stats File Generator**
> Generates statistics files by extracting the data from the CMP database using the OSSI XML interface. This task is also responsible for cleaning up the statistics files. The available settings for this task are: Local Repository directory (the default is `/var/camiant/stats_export`); Maximum age to keep files, in hours (default is 72 hours); File Format, either XML (default) or CSV; and Stats Type, which lets you select the statistics groups to extract. For information on the individual statistics in each available group, see *OSSI XML Interface Definitions Reference*.

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

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

Legacy OM Statistics
Periodically retrieves OM statistics from MPE devices executing the previous release of Policy Management software. This task should be run only during migration between software releases.

Subscriber Distributor
Reads subscriber data from the CMP database and then distributes it to the appropriate Policy Management devices within the system.

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 #unique_507.

Configuring a Scheduled Task

To configure an individual task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.

   The Scheduled Task Administration page opens showing the settings for the available scheduled tasks.
2. Click **Refresh** to update the page.
3. To configure a scheduled task, click the task name.

   The page displays the current settings and status for the selected scheduled task.
4. Click **Settings**.

   > **Note:**
   >
   > The **Health Checker** task has no configurable settings.

5. To configure a **Stats File Synchronizations** task (maximum of 4) for CMP to store copies of stats files to a remote external system:
   a. Enter the **Host Name / IP Address** for the remote server.

      You can use either the FQDN or IP address (either IPv4 or IPv6 format).
   b. Enter the SSH **User Name** required to access the remote server.
   c. Enter the SSH **Password**.
   d. Enter the **Path of Remote Repository** for storing the stats files.
   e. Enter the **Retry Limit** for the number of times to retry synchronizing the stats files (default is 3 with a maximum of 5) if the remote server is unreachable.
6. To configure the **OM Statistics** or **Replication Statistics** task:
   - Enter the **Number of days to keep statistical data**.

     This is the number of days to retain the specified statistics file. The valid range is from 1 to 30 days with a default of seven days.
7. To configure the **Stats Files Generator**:
   a. Enter the path for the **Local Repository**.

      This is the path on the external server where stats files are replicated. The default root directory for the repository is `/var/camiant/stats_export`. Two levels of subdirectories will be created under this root directory. An MPE or MRA cluster will have a corresponding first level subdirectory. Each stats file type will have its own subdirectory under the cluster-level directory. All the stats files will be created under the stats type subdirectory.

b. Enter the **Maximum age to keep files (hours)**.

   The default is 72 hours.

c. Select the **File Format** from the list.

   Available formats are **CSV** or **XML** (default).

d. Select the **Stats Type** from the list:

   See Generated Statistics for a list of available statistics.

   - Click **Select All** to have the generator collect statistics for all stats types.
   - Click **Inverse All** to deselect any selected stats types and select any unselected stats types.
   - Select each individual stats types.

8. If **Wireless-C** and **CMPP** modes are enabled, to configure the **PM Statistics** task:

   a. Enter the **Number of days to keep statistical data**.

      This is the number of days to retain the specified statistics file. The valid range is from 1 to 7 days with a default of seven days.

   b. Enter the **Number of Max TPS Capacity**.

      This is the maximum transactions per second. The default value is 5000

9. If **Wireless-C** and **CMPP** modes are enabled, to configure the **PM Statistics Files Uploading** task:

   a. Enter the **Host Name / IP Address** for the remote server.

      You can use either the FQDN or IP address (either IPv4 or IPv6 format).

   b. Enter the FTP **User Name** required to access the remote server.

   c. Enter the FTP **Password**.

   d. Enter the **Path of Remote Repository** for storing the stats files.

   e. Enter the **Retry Limit** for the number of times to retry synchronizing the stats files (default is 3 with a maximum of 5) if the remote server is unreachable.

   f. Select to enable **Security FTP**.

10. If **Wireless-C** and **CMPP** modes are enabled, to configure the **SMS Statistics Files Uploading** task:

   a. Enter the **Host Name / IP Address** for the remote server.

      You can use either the FQDN or IP address (either IPv4 or IPv6 format).

   b. Enter the FTP **User Name** required to access the remote server.

   c. Enter the FTP **Password**.

   d. Enter the **Path of Remote Repository** for storing the stats files.

   e. Enter the **Retry Limit** for the number of times to retry synchronizing the stats files (default is 3 with a maximum of 5) if the remote server is unreachable.

   f. Select to enable **Security FTP**.

11. Click **Save**.

   - Click **Save**.

The scheduled task is configured.

Rescheduling a Task

To reschedule a scheduled task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.

   The Scheduled Task Administration page opens showing the settings for the available scheduled tasks.

2. To configure a scheduled task, click the task name.

   The page displays the current settings and status for the selected scheduled task.

3. Click **Reschedule**.

   The reschedule configuration settings appear.

4. To **Schedule by Interval**:

   a. Select the date and time for the **Next Run Time**.

   b. For the Run Interval, select the **Hours** or **Minutes**.

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

5. To schedule the task **Following Another Task**, select the **Task to Follow** from the list.

6. Click **Save**.

The scheduled task is rescheduled.

Enabling or Disabling a Scheduled Task

To enable or disable an individual task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.

   The Scheduled Task Administration page opens showing the settings for the available scheduled tasks.

2. To configure a scheduled task, click the task name.

   The page displays the current settings and status for the selected scheduled task.

3. To disable an enabled task, click **Disable**.

   The scheduled task is disabled and the button text changes to **Enable**.

4. To enable a disabled task, click **Enable**.

   The scheduled task is enabled and statistics files will be generated based on the task's configuration settings. The button text changes to **Disable**.

5. Click **OK** to acknowledge the change.

The specified task is disabled or enabled.

About Managing Users

The CMP system lets you configure the following user attributes:

Roles
Determines the actions (and the access level) a user can perform within the CMP system. See About User Roles for details.

Scopes
Determines the network element groups and Policy Management device groups a user can perform actions on and providing a context for a role. See About User Scopes for details.

Users
After you define roles and scopes, you can assign them to user profiles. See About User Profiles for details.

External Authentication
Enables the CMP system to authenticate users using either RADIUS or SANE Authentication. These users must match the RADIUS Server account information before access is permitted. See About External Authentication for details.

About User Roles

The CMP system uses roles to configure what a user can do within the CMP system. Assigning roles to the various users that access the CMP system lets you control who can configure and access features within the CMP system. The default roles are:

Administrator
Permits full read/write access to all functions. You cannot delete the **Administrator** role.

Operator
Permits full read/write access to all Policy Management server management and configuration functions. Access is also permitted to all system administration functions except **User Management**.

Viewer
Permits read-only access to functions associated with Policy Management server management and configuration. Full access is also permitted to some of the system administration functions, such as **Change Password**.

> **Note:**
>
> When you create a new role, ensure that it has appropriate access to all functions you intend the role to use. For example, if you create a role for third-party access to OSSI functions, but it does not have the system administration privilege **Import/Export** set to **Show**, a user given that role cannot perform OSSI queries.

The CMP system lets you perform the following role management actions:

- Creating a Role
- Modifying a Role
- Deleting a Role

Creating a Role

To create a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

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

   The Role Administration page opens in the work area.

3. Click **Create Role**.

   By default, all access for privileges are set to either **Hide** (that is, the functions do not appear to users of the role, so access must be explicitly granted) or **Read-Only** (that is, information can be displayed but not changed).

   The New Role page opens.

4. Enter the **Name** for the new role.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

5. Enter a **Description/Location** (optional).

   Free-form text.

6. **Policy Server Privileges**—Defines access to the following MPE device management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):

   - **Configuration**
   - **Configuration Template**
   - **Applications**
   - **Match Lists**
   - **Quota Profiles & Conventions**
   - **Services & Rating Groups**
   - **Policy Counter ID**
   - **PRA Lists**
   - **Traffic Profiles**
   - **Roaming Profile**
   - **Protocol Timer Profile**
   - **Retry Profiles**
   - **Charging Servers**
   - **Time Periods**
   - **Monitoring Key**
   - **Serving Gateway/MCC-MNC Mapping**
   - **Custom AVP Definitions**
   - **AVP Definitions**
   - **Custom VSA Definitions**
   - **Customer Vendor**
   - **Notification Server**
   - **SMS Gateway**

   - **Global Configuration Settings**
   - **Presence Reporting Area Lists**
   - **Bulk Operation**

7. **Subscriber Privileges**—Defines access to the subscriber functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Entitlements**
   - **Tiers**
   - **Quota Usage**
8. **SPR Privileges**—Defines access to the SPR functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Subscriber Data**
9. **Network Privileges**—Defines access to the network management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Network Elements**
   - **Topology** (not supported)
10. **MRA Privileges**—Defines access to the MRA Configuration functions:
    - **Configuration** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Bulk Operations** (with the access **Hide** or **Show**)
    - **Configuration Template**
11. **Policy Management Privileges**—Defines access to the policy management functions:
    - **Policy Library** (with the access **Hide**, **Read-Only**, **Read and Deploy**, or **Read, Deploy, and Write**)
    - **Template Library** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Policy Table Library** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Policy Checkpoint** (with the access **Hide**, **Read-Only**, or **Read-Write**)
12. **System Wide Reports Privileges**—Defines access to the system-wide reports functions:
    - **System Wide Reports Configuration** (with the access **Hide**, **Read-Only**, or **Read-Write**)
13. **Platform Setting Privileges**—Defines access to the platform setting functions:
    - **Platform Configuration Setting** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Topology Settings** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **SNMP Settings** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Server Operation** (with the access **Hide** or **Read-Write**)
14. **Upgrade Manager Privileges**—Defines access to software upgrade functions:
    - **ISO Maintenance** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Upgrade Manager** (with the access **Hide**, **Read-Only**, or **Read-Write**)
15. **System Administration Privileges**—Defines access to system administration functions:
    - **Import / Export** (with the access **Hide** or **Show**)
    - **Operational Measurements** (with the access **Hide** or **Read-Only**)

- **User Management** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Scheduled Tasks** (with the access **Hide** or **Read-Write**)
- **Trace Log of CMP** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Subscriber Activity Log** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Audit Log** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Audit Log User Info** (with the access **Hide** or **Show**)
- **Alarms** (with the access **Hide**, **Read-Only**, or **Read-Write**)
- **Password Strength** (with the access **Read-Only** or **Read-Write**)
- **Push Method for Statistics** (with the access **Read-Only** or **Read-Write**)
  If set to **Read-Only**, the following fields are displayed for the **Stats File Generator** (see Managing Scheduled Tasks) setting:
  - **Name**
  - **Description**
  - **Last Exit Status**
  - **Current State**
  - **Last Start Time**
  - **Last End Time**
  - **Follows Task**

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

> **Note:**
>
> By default, the **Read-Write** privilege for this is only available for members of the Administrator role. Other roles have **Read-Only** access by default.

New tasks are created to synchronize stats files. These tasks perform a retry if a remote server is unreachable. The following fields are displayed for the Stats Files Synchronization setting:

- **Remove Server Information**
  - **Host Name/IP Address**
  - **User Name**
  - **Password**
  - **Path of Remote Repository**
- **Retry Limit**—You have a limit of three retries in one-minute intervals.

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

16. Click **Save**.

The role is created.

Modifying a Role

To modify a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

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

   The Role Administration page opens in the work area.

3. Select the role to modify.

   The Role Administration page displays the configuration of the role.

4. Click **Modify**.

   The Modify Role page opens.

5. Modify role information as necessary.

   See Creating a Role for a description of the fields on this page.

6. Click **Save**.

The role is modified.

Deleting a Role

> **Note:**
>
> You can delete any role except the **Administrator** role.

You cannot delete a role that is in use. You must remove any users assigned to the role before deleting it.

To delete a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

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

   The Role Administration page opens in the work area.

3. Delete the role using one of the following methods:

   - From the work area, click the 🗑 (Delete icon) located next to the role to delete.

- From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

  A confirmation message displays.

4. Click **OK**.

The role’s information is deleted from the CMP database.

About User Scopes

The CMP system uses scopes to define the network element groups and Policy Management device groups that a user can access, which provides operational context for a role.

> **Note:**
>
> You can assign a user more than one scope.

The CMP system allows you to perform the following scope management actions:

- Creating a Scope for CMP Servers
- Creating a Scope for Multilevel CMP Servers
- Modifying a Scope
- Deleting a Scope

Creating a Scope for CMP Servers

> **Note:**
>
> This procedure applies to non-tiered CMP servers. See Creating a Scope for Multilevel CMP Servers.

Scopes allow you to control what areas or devices in a network a user can manage. The default scope, **Global**, contains all items defined within the CMP database. After you define a scope you can assign it to users.

To create a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
2. In the content tree, select **Scopes**.

   The Scope Administration page opens in the work area.
3. Click **Create Scope**.

   The New Scope page opens.
4. Enter the **Name** for the new scope.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

5. Enter the **Description/Location** (optional).

   Free-form text.

6. Select the **Policy Server Group**s included in this scope.
7. Select the **Network Element Groups** included in this scope.
8. Select the **MRA Groups** included in this scope.
9. Click **Save**.

The scope is created.

Creating a Scope for Multilevel CMP Servers

Scopes allow you to control what areas or devices in a network a user can manage. The default scope, **Global**, contains all items defined within the CMP database. After you define a scope you can assign it to users.

> **Note:**
>
> Network Element Groups can only be created at the NW-CMP level. MPE Groups and MRA Groups can only be created at the S-CMP level.

To create a scope on an NW-CMP server:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

2. In the content tree, select **Scopes**.

   The Scope Administration page opens in the work area.

3. Click **Create Scope**.

   The New Scope page opens.

4. Enter the **Name** for the new scope.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

5. Enter the **Description/Location** (optional).

   Free-form text.

6. Select the **Policy Server Groups** included in this scope.
7. Select the **Network Element Groups** included in this scope.
8. Select the **MRA Groups** included in this scope.
9. Click **Save**.

The scope is created.

Modifying a Scope

To modify a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

2. In the content tree, select **Scopes**.

   The Scope Administration page opens in the work area.

3. Select the scope you want to modify.

   The scope configuration appears.

4. Click **Modify**.

   The Modify Scope page opens.

   > **Note:**
   >
   > See Creating a Scope for CMP Servers for descriptions of the fields on this page.

5. Modify the scope as needed.

6. Click **Save**.

The scope is modified.

Deleting a Scope

> **Note:**
>
> You cannot delete the **Global** scope.

To delete a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

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

   The Scope Administration page opens in the work area.

3. Delete the scope using one of the following methods:

   - From the work area, click 🗑 (Delete icon) located to the right of the scope you want to delete.
   - From the content tree, select the scope to delete and click **Delete**.

   A confirmation message appears.

4. Click **OK**.

The scope is deleted.

About User Profiles

User Management includes functions to create, modify, or delete user profiles. A user profile defines a user with a role and one or more scopes.

The CMP system is configured initially with the following default user profiles and passwords:

- `admin` (you cannot delete this profile)

  > **Note:**
  >
  > Oracle recommends changing the password after your first log in to the CMP system.

- `operator`
- `viewer`

The `admin` user is the only profile that cannot be deleted or have its username modified. The `admin` user is the only user that can create, modify, or delete other users, as well as log off all users.

> **Note:**
>
> When logging in, the username is not case sensitive; however, the password is case sensitive.

The CMP system lets you perform the following user management actions:

- Creating a User Profile
- Modifying a User Profile
- Deleting a User Profile

Creating a User Profile

To create a user profile:

1. Log in to the CMP system as `admin`.
2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. In the content tree, select **Users**.

   The User Administration page opens in the work area.

   > **Note:**
   >
   > The **Log Out All Users** button is visible only to the `admin` user.
4. Click **Create User**.

   The New User page opens.
5. Enter the **Username**.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

> **Note:**
>
> This value is not case sensitive.

6. Enter a **Description/Location** (optional).

   Free-form text.

7. Enter the **Password**.

   This value is case sensitive and must contain at least six characters; alphabetic, numeric, and special characters are allowed. This value must conform to the password strength rules. See Changing a Password for details on configuring password strength rules.

8. Enter to **Confirm Password** the **Password**.

9. Enter the number of days for the **Password Expiration Period(days; 0=never)**.

   Enter a value from `7` to `365`, or `0` to indicate that the password never expires. The default value is the system setting.

   > **Note:**
   >
   > This setting overrides the system setting. For details on configuring password system settings, see Configuring System Settings.

10. Select to **Force to Change Password**.

    If selected, this user must change passwords during the next log in. The default value is enabled.

11. Select a **Role** from the list.

12. Select one or more **Scopes** to assign to the user profile.

13. Click **Save**.

The user profile is created.

Creating a Customer User Management System Profile

To support identity management (IDM), the CMP system can accept HTTP or HTTPS connection requests from an external Customer User Management system to create, update, query, and delete user profiles. Requests and responses consist of XML documents.
For more information on the XML application programming interface, see *OSSI XML Interface Definitions Reference*.

To create a user profile for an external Customer User Management system:

1. Create a user profile as described in Creating a User Profile.
2. Assign the user profile a **Role** that includes the following privileges:
   - **Show** access for **Import/Export** privilege
   - **Read-Write** access for **User Management** privilege
3. Assign the user profile to the default **Global** scope.
4. Click **Save**.

   - Click **Save**.

The user profile for the Customer User Management System is saved.

Modifying a User Profile

To modify a user profile:

1. Log in to the CMP system as `admin`.
2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. In the content tree, select **Users**.

   The User Administration page opens in the work area.
4. Select the user profile from the content tree.

   The profile information page opens.
5. Click **Modify**.

   The Modify User page opens.
6. Modify the user profile.

   For field descriptions, see Creating a User Profile.
7. Click **Save**.

The user profile is modified.

Deleting a User Profile

> **Note:**
>
> You cannot delete the `admin` user profile.

To delete a user profile:

1. Log in to the CMP system as `admin`.
2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. In the content tree, select **Users**.

   The User Administration page opens in the work area.
4. Delete the user profile using one of the following methods:
   - From the work area, select 🗑 (Delete icon) located to the right of the profile.
   - From the content tree, select the user profile and click **Delete**.

   A confirmation message displays.
5. Click **OK**.

The user profile is deleted.

About Locking and Unlocking User Profiles

A user is locked out after exceeding the login failure threshold, or if the `admin` user locks the user out.

A locked-out user sees the following message on the login page when attempting to log in: `"Your account is locked. Please contact the Administrator."`

> **Note:**
>
> The admin user cannot lock the `admin` user account.

The CMP system includes the following functions:

- Locking a User
- Unlocking a User

Locking a User

To lock a user profile:

1. Log in to the CMP system as `admin`.
2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. In the content tree, select **Users**.

   The User Administration page opens in the work area.
4. Select the user profile from the content tree.

   The User Administration page displays configuration information about the user.
5. Click **Lock**.

   A confirmation message appears.
6. Click **OK**.
   - The user profile is locked.
   - The page displays a message indicating the account was locked successfully.
   - The **Lock** button becomes an **Unlock** button.
   - On the User Administration page, the **Locked Status** for the user shows `Locked`.

Unlocking a User

To unlock a user profile:

1. Log in to the CMP system as `admin`.
2. From the System Administration section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. In the content tree, select **Users**.

The User Administration page opens in the work area.

4. Select the user profile from the content tree.

   The User Administration page displays configuration information about the user.

5. Click **Unlock**.

   A confirmation message appears.

6. Click **OK**.

   - The user profile is unlocked.
   - The page displays a message indicating that the user account was unlocked successfully.
   - The **Unlock** button becomes a **Lock** button.
   - On the User Administration page, the **Locked Status** for the user shows `Unlocked by Admin`.

Logging Out All Users

> **Note:**
>
> Only the `admin` user can log out all users that are currently logged in to the CMP system. The `admin` user will not be logged out.

To log out all other users:

1. Log in to the CMP system as `admin`.

2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.

3. In the content tree, select **Users**.

   The User Administration page opens in the work area.

4. Click **Log Out All Users**.

   A confirmation message appears.

5. Click **OK**.

Logged-in users are logged out from the CMP system.

About External Authentication

In addition to the built-in authentication functions, you can configure external authentication, RADIUS authentication, and SANE authentication of CMP users.

In the CMP system, you can manage the RADIUS Authentication and Account or the SANE Authentication external authentication method.

About 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`admin` user 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 the following steps:

1. See About Configuring the RADIUS Server for details on configuring the RADIUS server to accept authentication (and accounting, if used).
2. See About Defining CMP Users to the RADIUS Server for details on defining CMP users in the RADIUS server.
3. See About Associating Roles and Scopes for details on associating CMP users' roles and scopes with users on the CMP system
4. See About Defining the CMP System as a RADIUS Client for details on configuring the CMP system to work with the RADIUS server.

About Configuring the RADIUS Server

The RADIUS servers must be configured to authenticate clients and users on the CMP system. Some of the configuration values must be consistent with configuration parameters on the CMP system. (The RADIUS administrator is aware of the names and locations of the configuration files.)

See Enabling and Configuring RADIUS on the CMP System for details.

About Defining the CMP System as a RADIUS Client

The client file identifies the systems that use the RADIUS server to authenticate user access. A client should be defined as a single device. For example:

```
client 10.0.10.22 {
        secret = example
        shortname = MPE5
}
client 10.0.10.23 {
        secret = example
        shortname = CMP56
}
```

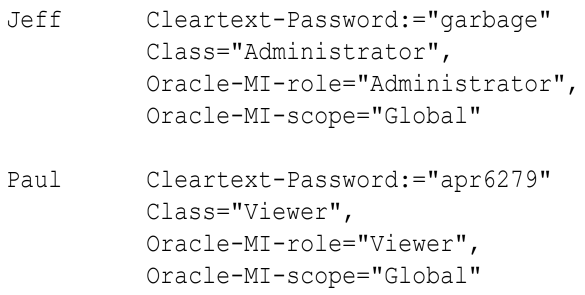
The best practice is to define IP addresses rather than FQDNs. If a netmask is not given, the default is `/32`. The shared `secret` (in this example, `example`) must be defined on both the RADIUS server and entered into the CMP configuration (see Enabling and Configuring RADIUS on the CMP System). The `shortname` is used as an alias.

If multiple IP addresses are configured on the CMP system (such as SIG-A and SIG-B), use the IP address that would be used as the Source IP address of RADIUS requests sent to the RADIUS server.

About Defining CMP Users to the RADIUS Server

The RADIUS server can use either a database or a simple flat file as its repository of user information. The following example uses a flat file to demonstrate a minimum user configuration. The users file contains authentication and configuration information for each user. It begins with the username and the authentication (that is, the password) that is required from the user. The user/password line is followed by indented lines that are attributes to be passed back to the requesting server.

Figure 18-5 Sample RADIUS User Information Flat File



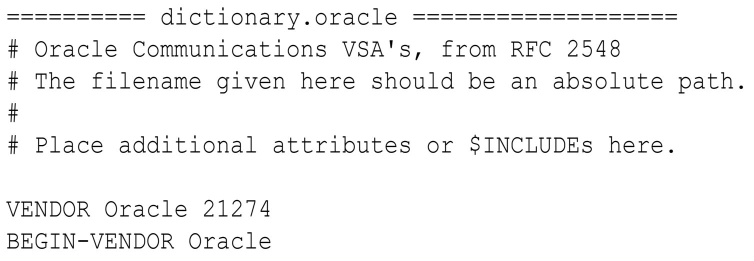
```
Jeff      Cleartext-Password:="garbage"
          Class="Administrator",
          Oracle-MI-role="Administrator",
          Oracle-MI-scope="Global"

Paul      Cleartext-Password:="apr6279"
          Class="Viewer",
          Oracle-MI-role="Viewer",
          Oracle-MI-scope="Global"
```

When the RADIUS server has authenticated a user, it sends back various attributes with the authentication acceptance message. The CMP system uses these attributes to determine what actions the user can perform.

The best practice is to use a vendor-specific attribute (VSA) dictionary file to define what attributes to send back to the client. Figure 18-6 shows a sample file. The local RADIUS administrator is responsible for incorporating the VSA dictionary file onto the RADIUS server.

Figure 18-6 Sample VSA Dictionary File For RADIUS



```
========== 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
======================
```

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.

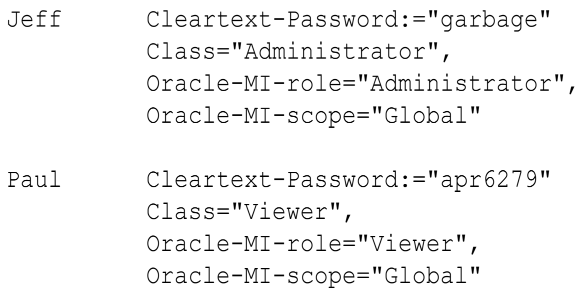
About Associating Roles and Scopes

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.

The best practice is 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 the RADIUS server if the VSA dictionary is integrated.

The following example defines users who have access at different role levels:

Figure 18-7 Sample RADIUS User Information



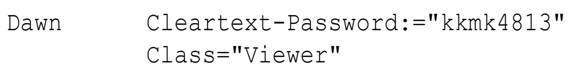
```
Jeff      Cleartext-Password:="garbage"
          Class="Administrator",
          Oracle-MI-role="Administrator",
          Oracle-MI-scope="Global"

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 of the required role and scope credentials. For example, consider this user defined in the RADIUS server:

Figure 18-8   Sample RADIUS User Information - No Role or Scope



```
Dawn      Cleartext-Password:="kkmk4813"
          Class="Viewer"
```

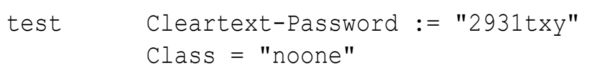
`Dawn` can get access to the CMP system if you have defined both a role named `Viewer` and a scope named `Viewer`; the user interface matches the one returned `Class` value to both of the required role and scope credentials.

Enabling and Configuring RADIUS on the CMP System

By default, RADIUS Authentication is disabled in the CMP system. Enabling authentication requires admin privileges. The `admin` user is always authenticated against the local database record; thus, the `admin` user is best suited to setting up RADIUS authentication (see Creating a User Profile).
Two configuration parameters must match with the configuration that was put on the RADIUS server:

- **Source of User Credentials** must match up with the user configuration in the RADIUS server, but this will also depend on what is configured in the next parameter.
- If **Action if missing credentials** is set to **Use following defaults**, then a user will be authenticated as long as the password is correct. This user could log in even though the `Class` is not valid:

  Figure 18-9   Sample User for RADIUS Server

  ```
  test      Cleartext-Password := "2931txy"
            Class = "noone"
  ```

  – If **Action if missing credentials** is set to **Reject**, then the configuration of the user will depend on the configuration of **Source of User Credentials**.

To enable RADIUS authentication and accounting:

1. Log in to the CMP system as `admin`.
2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. From the content tree, select **External Authentication**.

   The External Authentication page opens. By default, external authentication is disabled.
4. Click **Modify**.

   The External Authentication page becomes editable.
5. In the **Configuration** section, select **Enable RADIUS Authentication**.

   Configuration and RADIUS Services configuration fields appear.

6. Select to **Enable RADIUS Accounting**.

   This feature is disabled by default. When enabled, the CMP system sends an Accounting-Start message to the accounting server when a user logs in, and an Accounting-Stop message when the user logs out. These messages contain a session ID attribute that uniquely identifies the user session so that it can be matched between Start and Stop.

7. Select the **Destination for Accounting Messages** from the list.

   Available options include:

   - **Both Primary and Secondary** (default)
     Specifies that accounting messages generated for each user session are sent to both the primary and (when configured) secondary RADIUS servers.
   - **Primary (Secondary on error)**
     Accounting messages are sent only to the primary server, as long as it is reachable. If the primary accounting server is unreachable, messages are sent to the secondary accounting server.

8. Enter the **NAS IP Address** (required).

   The IP address, in IPv4 or IPv6 format, of the network access server. By default, this is the local host address.

9. Select when to **Use local authentication** from the list.

   Available options include:

   - **When RADIUS servers timeout** (default)
   - **When both RADIUS servers timeout or reject**
   - **Never**

   > **Note:**
   >
   > Fallback to local authentication is never used. However, the `admin` user is always authenticated locally.

10. Select the **Source of User Credentials** from the list.

    Available options include:

    - **RADIUS Class**
      The value of the `Class` attribute returned by the server determines both the role and scope.
    - **Oracle VSAs**
      The value of Oracle VSAs returned by the server determines the role and scope.

11. Select an **Action if Missing Credentials**.

    Available options include:

    - **Reject**
      If you select this option, a user whose login credentials are missing is not logged in.
    - **Use following defaults**
      Select a setting for each of the following attributes:
      - **Default Role**
        The role assigned if the user credentials are missing or mismatched. The default role is **Viewer**.

  - **Default Scope**
    The scope assigned if the user credentials are missing or mismatched. The default scope is **Global**.

12. In the **RADIUS Services** section, edit the following fields:

    a. Configure the **Primary RADIUS Authentication Server**:

    - **Server**
      The FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary authentication server.

      > **Note:**
      >
      > To disable the primary server, delete its IP address.

    - **Port**
      The IP port number of the primary server. The default value is port 1812.
    - **Timeout (seconds)**
      The length of time the CMP system waits for a response from the server. The default value is 3 seconds.
    - **Retries**
      The number of times the CMP system tries to send a message to the server. The default value is 3 times.
    - **Shared Secret**
      A password-like string that must exactly match between the CMP system and the `secret` attribute configured in the entry for this CMP system in the `clients.conf` file in the RADIUS server.

      > **Note:**
      >
      > If the two values do not match, the server ignores all messages from the CMP system.

    b. Configure the**Secondary RADIUS Authentication Server**:

    If configured, the secondary authentication server uses the same fields as the primary authentication server.

    c. Configure the **Primary RADIUS Accounting Server**:

    - **Server**
      The FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary accounting server.
    - **Port**
      The IP port number of the Primary RADIUS Accounting server. The default value is port 1813.
    - **Timeout (seconds)**
      The length of time the CMP system waits for a response from the server. The default value is 3 seconds.
    - **Retries**
      The number of times the CMP system tries to send a message to the server. The default value is 3 times.

- **Shared Secret**
  A password-like string that must exactly match between the CMP system and the `secret` attribute configured in the entry for this CMP system in the `clients.conf` file in the RADIUS server.

  > **Note:**
  >
  > If the two values do not match, the server ignores all messages from the CMP system.

d. **Secondary RADIUS Accounting Server**

   If configured, the secondary accounting server uses the same fields as the primary accounting server.

13. Click **Save**.

RADIUS Authentication and Accounting is configured.

About 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 so 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.

> **Note:**
>
> Usage of a SANE client is outside the scope of this document.

See Enabling SANE Authentication on the CMP System for details.

The `admin` user profile is treated separately. An `admin` user can log in to the CMP system using any supported browser.

The authentication process is as follows:

1. From a SANE client user interface, the user selects the CMP system in a web browser.
2. An encrypted SANE authentication artifact is sent to the CMP system through the browser.
3. The CMP system forwards the artifact to a SANE server (also called, the SANE responder).

   > **Note:**
   >
   > The `admin` user is always authenticated locally, regardless of SANE configuration settings.

   - 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 to the system.
   - If the SANE server does not verify the artifact, the CMP system rejects the login request.

Enabling SANE Authentication on the CMP System

By default, SANE Authentication is disabled in the CMP system. Enabling authentication requires `admin` privileges. The user `admin` is always authenticated against the local database account; thus, the `admin` user is best suited to setting up SANE authentication (see Creating a User Profile).
To enable SANE authentication:

1. Log in to the CMP system as `admin`.
2. From the **System Administration** section of the navigation pane, select **User Management**.

   The content tree displays the **User Management** group.
3. From the content tree, select **External Authentication**.

   The External Authentication page opens, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**.

   The External Authentication page becomes editable.
5. In the **Configuration** section, select **Enable SANE Authentication**.

   Configuration and SANE Servers configuration fields appear.
6. Enter the **Artifact Parameter Name**.

   The name of the artifact parameter. Enter an alphanumeric string. The default value is `artifact`.
7. Select the **Verification for Account** setting from the list.

   Available options are:

   - **On login only** (default) — The CMP system authenticates the user once on login. The user is considered authenticated until logout.
   - **On each request** — The CMP system authenticates the user on login, and then for each HTTP or HTTPS request. If any request is not authenticated, the user is immediately logged out.
8. Select the **Action if Missing Credentials**.

   The available options are:

   - **Reject** — If you select this option, a user login is rejected even if the authentication is successful.
   - **Use following defaults** — If you select this option, a user with missing credentials is allowed to log in, but the system assigns a default role and scope:
     - **Default Role** — Default role assigned to the user. The default role is **Viewer**.
     - **Default Scope** — Default scope assigned to the user. The default scope is **Global**.
9. In the **SANE Servers** section, enter the **SAML Service Name**.

   The name of the Security Assertion Markup Language service registered with the UDDI server. Enter an alphanumeric string.
10. Enter the **UDDI Inquiry URL**.

The Universal Description, Discovery and Integration URL, in HTTP or HTTPS format, for the inquiry.

11. Click **Save**.

SANE authentication is enabled.

Configuring an SMS Relay

> **Note:**
>
> You must enable **Wireless-C** and **CMPP** modes to configure SMS Relay.

The SMS Relay (SMSR) establishes a connection to the Short Message Service Center (SMSC), which is used when submitting short messages to the subscriber. The SMSR is configured using the SMS Relay option in the System Administration section of the navigation pane. You can also use this option to set the log levels for the SMS and CMPP logs.

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

To configure an SMS relay:

1. From the **System Administration** section of the navigation pane, select **SMS Relay**.

   The current CMPP profile settings and SMS log settings are displayed.

2. Click **Modify**.

   A page that allows you to modify the CMPP configuration and SMS log settings opens.

3. In the **CMPP Configuration** section, define the following:

   a. **CMPP Enabled** — Enables the CMPP client to establish a connection with the SMSC. If this box is not checked, all CMPP messages to the SMSC are dropped. The default is to not enable the field.

   b. **SMSC Host** — The host name of the CMPP client that the SMSC server will connect to. The default value is to leave the field blank.

   c. **SMSC Port** — The port number of the CMPP client that the SMSC server will connect to. The default value is 7890.

   d. **Source Address** — The source address of the CMPP client. The default value is to leave the field blank.

   e. **Shared Secret** — The name of the shared secret, which is used to generate the authenticator source. The default value is to leave the field blank.

   f. **Registered Delivery** — Requests an SMSC delivery receipt or SME originated acknowledgments.

      Valid values are:

      - No Delivery Receipt (default)
      - Delivery Receipt

   g. **Service ID** — The service ID. Enter a string value with a 10-character length. The default value is to leave the field blank.

   h. **Message Format** — The format of the message encoding.

The valid values are:

- ASCII Encoding
- Message Write Card Operation
- Binary Message
- UCS2 Encoding (default)
- GBK Encoding

To support Chinese characters in the message content, the format should be UCS2 or GBK.

4. In the **Modify SMS Log Settings** section, define the following:
   a. **SMS Log Level** — The level at which an SMS log is generated.

      Available levels are:

      - OFF
      - ERROR
      - WARN (default)
      - INFO
      - DEBUG
      - TRACE
      - ALL

   b. **SMS Rotation Cycle** — The interval at which SMS logs are generated. The default value is HOUR, which generates logs hourly.
5. In the **Modify CMPP Log Settings** section, define the following:
   a. Select **CMPP Rotation Cycle**:

      Available options are:

      - MINUTE
      - HOUR (default)
      - DAY
      - MONTH

   b. Select **CMPP Log Level**:

      Available levels are:

      - OFF
      - ERROR
      - WARN (default)
      - INFO
      - DEBUG
      - TRACE
      - ALL
6. In the **Generic Notification Configuration** section, configure the following:
   a. Select to enable Notification

b. Select **HTTP Log Level**:

   Available levels are:

   - OFF
   - ERROR
   - WARN (default)
   - INFO
   - DEBUG
   - TRACE
   - ALL

7. Click **Save**.

The CMPP SMS Relay is configured.

Changing a Password

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

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

If the system administrator has configured your account for password expiration, you will receive a warning when you log in that you must change your password.

> **Note:**
>
> To reset the administrator password, it is recommended to contact My Oracle Support.

To change a password:

1. From the **System Administration** section of the navigation pane, select **Change Password**.

   The Account Management page opens. If your account is set up with a password expiration period, the expiration date is displayed.

2. Enter your **Current Password**.
3. Enter your **New Password**.

   The password is case sensitive. Depending on your system settings, the password must meet the following requirements:

   - Cannot contain the username.
   - Must contain the minimum number of characters (default is six).
   - Must contain characters as specified from the following categories:
     – Must contain at least the specified number of lower case letters.

- Must contain at least the specified number of upper case letters.
- Must contain at least the specified number of numbers.
- Must contain at least the specified number of symbols.

> **Note:**
>
> Consult with your system administrator to obtain the password criteria for your system.

4. Re-enter your new password to **Confirm Password**.

> **Note:**
>
> If your new password does not conform to the password strength rules configured for your system, a validation error message appears that includes valid password criteria. Enter and confirm another password that conforms to the criteria.

5. Click **Change Password**.

Your password is changed.

Changing the MySQL Password

To change the MySQL password:

1. Verify that HA and MySQL servers are master.
2. Log into the CMP GUI.
3. Clear any critical alarms and MySQL alarms.

   MySQL related alarms are:

   - 70020—QP Master database is outdated
   - 70021—QP slave database is unconnected to the master
   - 70022—QP Slave database failed to synchronize
   - 70023—QP Slave database lagging the master
   - 70024—QP Slave database is prevented from synchronizing with the master
   - 70025—QP Slave database is a different version than the master
4. Set any secondary and tertiary servers (server-b or server-c) to forced standby.
5. Locate the master MySQL node.

   The master MySQL node is the active MA or CMP in primary site for. There are two ways to find the master MySQl node:

   - Login into the CMP GUI, and find the active server by selecting **Platform Settings**, and then **Topology Settings**.
   - Use the `wbAccess mysqlState` command in the CLI.
6. Using the CLI , enter `manageMySQL ModifyMySQLRootPWD` to modify the MySQL password.

The password is 1 to 32 characters in length.

Because of MySQL cluster replication, this change is replicated to all slave MySQL servers, then the password in the database of all the MySQL servers is changed synchronously.

7. Remove the forced standby from all secondary and tertiary servers (server-b or server-c).

Your MySQL password is changed.

A

CMP Modes

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
- Tabs on the MRA Administration page
- Protocols supported
- Configuration options
- Policy options available in the policy wizard
- Reports available

The mode selection process is not normally available. At initial configuration, and if it becomes necessary to replace a server or reinstall Policy Management software, the Mode Settings page becomes visible, and you must reset the operating 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 or changing modes inappropriately could result in the loss of network element connectivity, policy function, statistical data, and cluster redundancy.

About Mode Settings

When you use a web browser to connect to a CMP system after the software is first installed, the Mode Settings page opens (Figure A-1). Select the needed modes, functions, and management options for your installation and then click **OK**. The browser page closes and you are automatically logged out. When you next log in, the CMP system reopens in the selected mode.

Restriction

> **Important:**
>
> Options marked as **Restricted** are for use within specific environments and should not be enabled without authorization. For more information about the restricted function or feature, contact My Oracle Support.

Modes and Functions

The following modes and functions are available:

Wireless
Enables support of a wireless carrier environment.

Wireless functions include:

Diameter 3GPP
Supports Diameter 3GPP protocol.

Diameter 3GPP2
Supports Diameter 3GPP2 protocol.

> **Note:**
>
> This function is restricted. See Restriction for more information.

PCC Extensions
Supports Policy and Charging Control functions.

> **Note:**
>
> This function is restricted. See Restriction for more information.

Quotas Gx
Supports a subscriber quota environment using the Diameter Gx protocol. The Gx protocol supports deep packet inspection (DPI) devices.

Quotas Gy
Supports a subscriber quota environment using the Diameter Gy protocol.

> **Note:**
>
> This function is restricted. See Restriction for more information.

LI
Supports Lawful Intercept functions. Described in the *Configuring Lawful Intercept Application Note*.

> **Note:**
>
> This function is restricted. See Restriction for more information.

SCE-Gx
Supports the Cisco Service Control Engine Gx protocol. If this mode is selected, **Diameter 3GPP** and **RADIUS** must also be selected, and other Gx sub-modes must not be selected.

> **Note:**
>
> This function is restricted. See Restriction for more information.

Gx-Lite
Supports the Gx-Lite protocol, a simplified version of 3GPP Gx for use by non-GGSN PCEF vendors that do not have access to network-level information.

> **Note:**
>
> This function is restricted. See Restriction for more information.

Cisco Gx
Supports the Cisco Gx protocol.

> **Note:**
>
> This function is restricted. See Restriction for more information.

DSR
Supports Policy Management network segmentation using a Oracle Communications Diameter Signaling Router (DSR).

> **Note:**
>
> This function is restricted. See Restriction for more information.

Wireless-C
Supports a wireless system supporting a SMS Notification Statistics; and SCTP counters.

> **Note:**
>
> This function is restricted. See Restriction for more information.

SMS
Enables support of SMS servers.

SMS Mode functions include:

SMPP
Supports SMS using SMPP protocol.

CMPP
Supports SMS using CMPP protocol.

> **Note:**
>
> This function is restricted. See Restriction for more information.

XML
Supports SMS using XML.

> **Note:**
>
> This function is restricted. See Restriction for more information.

SPR
Enables support of subscriber database management. Select only one sub-mode. Functions are described in the Subscriber Data Management documentation.

SPR Mode functions include:

Subscriber Profiles
Supports subscriber profile functions.

> **Note:**
>
> This function is restricted. See Restriction for more information.

Quota
Supports subscriber quotas.

> **Note:**
>
> This function is restricted. See Restriction for more information.

Wireline
Enables support of a wireline carrier environment. Functions are described in the *Configuration Management Platform Wireline User's Guide*.

> **Note:**
>
> This function is restricted. See Restriction for more information.

SPC
Enables the COPS Application Manager product, which accepts service provisioning requests from a Session Border Controller over the Common Open Policy Service (COPS) protocol.

Functions are described in the *Service Provisioning over COPS Application Manager User's Guide*.

> **Note:**
>
> This function is restricted. See Restriction for more information.

RADIUS
Enables support of RADIUS Change of Authorization.

> **Note:**
>
> This function is restricted. See Restriction for more information.

PCMM
Supports a network creating PacketCable MultiMedia (PCMM) sessions.

Diameter
Supports a network creating Diameter sessions.

> **Note:**
>
> This function is restricted. See Restriction for more information.

RDR
Supports a network containing Service Control Engine (SCE) devices transmitting Raw Data Records (RDRs).

> **Note:**
>
> This function is restricted. See Restriction for more information.

SCEF
Enables support of Service Capability Exposure Function servers in an Internet of Things (IoT) environment. Functions are described in the *Configuration Management Platform SCEF User's Guide*. For SCEF mode select only this function.

Server Management Options

The management options for servers are:

Manage Policy Servers
Manages MPE devices.

Manage MA Servers
Manages Management Agent servers.

Manage Policies
Enables the Policy Wizard.

Manage MRAs
Manages Multi-Protocol Routing Agent servers.

Manage SPR Subscriber Data
Manages Subscriber Profile Repository servers.

Manage Geo-Redundant
Manages georedundant MPE, MRA, BoD, MDF.

Manager is HA (clustered)
Enables High Availability features.

Manage Analytic Data
Enables output of policy event records.

Manage Direct Link
If enabled, all replication and HA transmissions go through the backplane interface; if disabled, all replication and HA transmissions go through the OAM interface.

> **Note:**
>
> This function is restricted. See Restriction for more information.

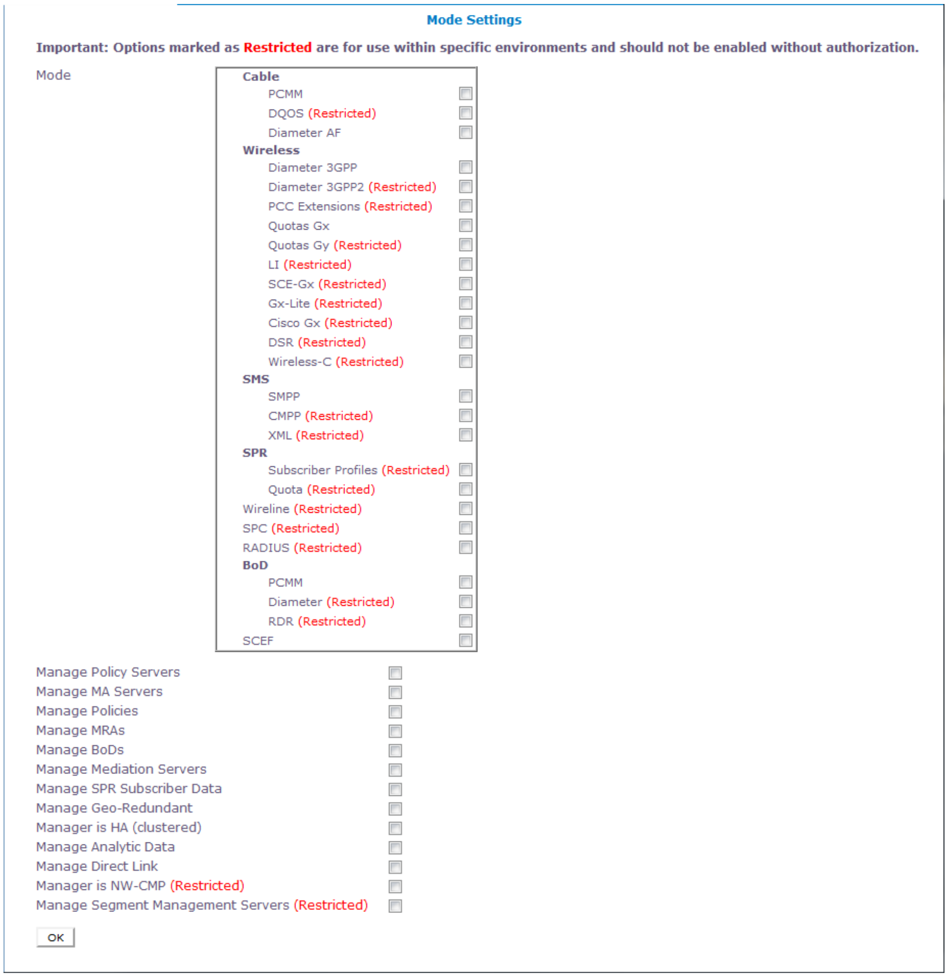
Manager is NW-CMP
Enable Network mode in a tiered CMP system. See #unique_539 for more information.

> **Note:**
>
> This function is restricted. See for more information.

Manage Segment Management Servers
Enable System mode in a tiered CMP system. See #unique_539 for more information.

> **Note:**
>
> This function is restricted. See for more information.

Figure A-1 Mode Settings Page



Mode Settings

Important: Options marked as Restricted are for use within specific environments and should not be enabled without authorization.

Mode

Cable

- PCMM □
- DQOS (Restricted) □
- Diameter AF □

Wireless

- Diameter 3GPP □
- Diameter 3GPP2 (Restricted) □
- PCC Extensions (Restricted) □
- Quotas Gx □
- Quotas Gy (Restricted) □
- LI (Restricted) □
- SCE-Gx (Restricted) □
- Gx-Lite (Restricted) □
- Cisco Gx (Restricted) □
- DSR (Restricted) □
- Wireless-C (Restricted) □

SMS

- SMPP □
- CMPP (Restricted) □
- XML (Restricted) □

SPR

- Subscriber Profiles (Restricted) □
- Quota (Restricted) □

Wireline (Restricted) □

SPC (Restricted) □

RADIUS (Restricted) □

BoD

- PCMM □
- Diameter (Restricted) □
- RDR (Restricted) □

SCEF □

Manage Policy Servers □

Manage MA Servers □

Manage Policies □

Manage MRAs □

Manage BoDs □

Manage Mediation Servers □

Manage SPR Subscriber Data □

Manage Geo-Redundant □

Manager is HA (clustered) □

Manage Analytic Data □

Manage Direct Link □

Manager is NW-CMP (Restricted) □

Manage Segment Management Servers (Restricted) □

B

Generated Statistics

This appendix lists the available statistics for generated scheduled tasks.

List of Generated Statistics

The following is a list of generated statistics available for scheduled tasks:

- DiameterPcefStats
- DiameterPcefPeerStats
- DiameterCTFStats
- DiameterCTFPeerStats
- DiameterBberfStats
- DiameterBberfPeerStats
- DiameterAfStats
- DiameterAfPeerStats
- DiameterShStats
- DiameterShPeerStats
- DiameterSyStats
- DiameterSyPeerStats
- DiameterTdfStats
- DiameterTdfPeerStats
- DiameterDrmaStats
- DiameterDrmaPeerStats
- DiameterPcefLatencyStats
- DiameterPcefPeerLatencyStats
- DiameterBberfLatencyStats
- DiameterBberfPeerLatencyStats
- DiameterAfLatencyStats
- DiameterAfPeerLatencyStats
- DiameterShLatencyStats
- DiameterShPeerLatencyStats
- DiameterSyLatencyStats
- DiameterSyPeerLatencyStats
- DiameterTdfLatencyStats
- DiameterTdfPeerLatencyStats

- DiameterDrmaLatencyStats
- DiameterDrmaPeerLatencyStats
- DiameterVzrStats
- ProtocolErrorStats
- ConnectionErrorStats
- DiameterEventTriggerStats
- DiameterConnectionEventTriggerStats
- IntervalStats
- TrafficProfileStats
- StaleSessionStats
- SyReconciliationStats
- QuotaProfileStats
- SgwFailureStats
- PolicyStats
- TopologyUpdateStats
- PolicyServerStats
- KpiStats
- TpsStats
- LdapDataSourceStats
- ShDataSourceStats
- SprDataSourceStats
- RadiusAccountingStats
- RadiusAccountingNetworkElementStats
- DiameterMraPcefStats
- DiameterMraPcefPeerStats
- DiameterMraAfStats
- DiameterMraAfPeerStats
- DiameterMraBberfStats
- DiameterMraBberfPeerStats
- DiameterMraCtfStats
- DiameterMraCtfPeerStats
- DiameterMraDrmaStats
- DiameterMraDrmaPeerStats
- DiameterMraDraStats
- DiameterMraTdfStats
- DiameterMraTdfPeerStats
- DiameterMraAfLatencyStats
- DiameterMraAfPeerLatencyStats

- DiameterMraPcefLatencyStats
- DiameterMraPcefPeerLatencyStats
- DiameterMraBberfLatencyStats
- DiameterMraBberfPeerLatencyStats
- DiameterMraDrmaLatencyStats
- DiameterMraDrmaPeerLatencyStats
- DiameterMraTdfLatencyStats
- DiameterMraTdfPeerLatencyStats
- DiameterMraVzrStats
- KpiMraStats
- TpsMraStats
- IntervalMraStats
- ProtocolMraErrorStats
- ConnectionMraErrorStats