Oracle® Communications Policy Management

Configuration Management Platform Wireless User's Guide

Release 9.7.3

E63618 Revision 01

August 2015

ORACLE®

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

Release 9.7.3

Table of Contents

List of Figures

List of Tables

Chapter 1

About this Guide

Topics:

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

Introduction

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

How This Guide is Organized

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

- *About this Guide* provides general information about the organization of this guide, related documentation, and how to get technical assistance.
- *The Oracle Communications Policy Management Solution* provides an overview of the 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 configure the advanced setting for the policy server.
- *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).
- *Call Clearance* describes how to how to remove an MPE from a PCRF topology.
- *Managing Policy Front End Devices* describes the Multi-Protocol Routing Agent (MRA), a standalone entity that supports MPE devices and is manageable by the CMP system.
- *Managing Message Distribution Function Servers* describes the Message Distribution Function (MDF) server.
- *Managing Subscriber Profile Repositories* describes how to manage subscriber profile repositories (SPRs).
- *Managing Subscribers* describes how to manage subscriber tiers, entitlements, and quota usage within the CMP system.
- *Managing Network Elements* describes how to manage network elements.
- *Managing Policy Front End Devices* describes the Oracle Communications Policy Management Policy Front End (also known as the MRA), a standalone entity that supports MPE devices and is manageable by the CMP system.
- *Managing Message Distribution Function Servers* describes how to define and manage Message Distribution Function (MDF) servers in the CMP system.
- *System-Wide Reports* describes the reports available on the function of Policy Management systems in your network.

- *Upgrade Manager* describes the purpose of the Upgrade Manager GUI page and the elements found on that page.
- *Global Configuration* describes how to configure the global settings for the CMP system.
- *System Administration* describes functions reserved for CMP system administrators.
- The appendix, *CMP Modes*, lists the functions available in the CMP system, as determined by the operating modes and sub-modes selected when the software is installed.

Scope and Audience

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

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

Documentation Admonishments

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

Table 1: Admonishments

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

Related Publications

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

Other Publications

The following documents are useful for reference:

- Internet Engineering Task Force (IETF) Diameter-related RFCs:
  - RFC 3539: "Authentication, Authorization and Accounting (AAA) Transport Profile"
  - RFC 3588: "Diameter Base Protocol"
- 3rd Generation Partnership Project (3GPP) technical specifications:
  - 3GPP TS 23.203: "Policy and charging control architecture (Release 8)"
  - 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows (Release 6)"
  - 3GPP TS 29.209: "Policy control over Gq interface (Release 6)"
  - 3GPP TS 29.211: "Rx Interface and Rx/Gx signalling flows (Release 6)"
  - 3GPP TS 29.212: "Policy and Charging Control over Gx/Sd reference point (Release 11)"
  - 3GPP TS 29.213: "Policy and Charging Control signalling flows and QoS parameter mapping (Release 11.4)"
  - 3GPP TS 29.214: "Policy and Charging Control over Rx reference point (Release 8)"
  - 3GPP TS 29.219: "Policy and Charging Control: Spending limit reporting over Sy reference point (Release 11.3)"
  - 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 8)"
  - 3GPP TS 32.240: "Charging architecture and principles (Release 8)"
  - 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications (Release 8)"
- 3rd Generation Partnership Project 2 (3GPP2) technical specifications:
  - 3GPP2 X.S0013-012-0: "Service Based Bearer Control — Stage 2"
  - 3GPP2 X.S0013-013-0: "Service Based Bearer Control — Tx Interface Stage 3"
  - 3GPP2 X.S0013-014-0: "Service Based Bearer Control — Ty Interface Stage 3"

Locate Product Documentation on the Oracle Technology Network Site

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

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

2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
   The Oracle Communications Documentation page appears with Tekelec shown near the top.
4. Click the **Oracle Communications Documentation for Tekelec Products** link.
5. Navigate to your Product and then the Release Number, and click the **View** link (the Download link will retrieve the entire documentation set).
   A list of the entire documentation set for the selected product and release appears.
6. To download a file to your location, right-click the **PDF** link, select **Save target as**, and save to a local folder.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Chapter

2

The Oracle Communications Policy Management Solution

Topics:

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

Note: The Policy Management Release 9.7 Solution interfaces with a third-party Policy and Charging Enforcement Function (PCEF). Therefore, some of the features and capabilities described in this document may not be available in this release. For additional clarification, please contact your local representative.

The Multimedia Policy Engine

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

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

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

- MPE devices — Provide policy control decisions and flow-based charging control. When a request for a policy decision is received for a subscriber session, the MPE device obtains subscriber information, evaluates the applicable policies, and directs the enforcement device to handle the session based on policy rules. MPE devices can communicate with an online charging system (OCS) indirectly using a Gy interface. MPE devices can send Short Message Service (SMS) or Simple Mail Transfer Protocol (SMTP) notifications to subscribers, and analytics data stream (ADS) information, as a series of policy event records (PERs), to third-party systems for analysis.
- Subscriber Profile Repository (SPR) — Contains subscriber or subscription information. MPE devices can operate with the following SPR systems:
  - Oracle Communications Subscriber Database Management (SDM)
  - Oracle Communications User Data Repository (UDR)
  - Third-party SPR

  The communication protocol can be Sh or Lightweight Directory Access Protocol (LDAP). The SDM and UDR supports a RESTful application programming interface (API) to provisioning and OCS systems.
- Diameter Routing Application — Depending on the size of the Policy Management network, a combination of stateful and dynamic Multi-Protocol Routing Agent (MRA) or Diameter Signaling Router (DSR) systems. MRA systems distribute the load between multiple MPE devices. DSR systems are multi-application Diameter agents that support segmented Policy Management networks.
- Configuration Management Platform (CMP) — Provides the policy console. The contains a centralized database of policy rules, policy objects, and network objects. Carriers can exchange database information in eXtensible Markup Language (XML) format with office support or back-office support systems (OSS/BSS). A system can communicate Policy Management network management information with network management stations (NMSs) using Simple Network Management Protocol (SNMP).

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

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

The Traffic Detection Function (TDF) can permit, gate, shape, or redirect service traffic.

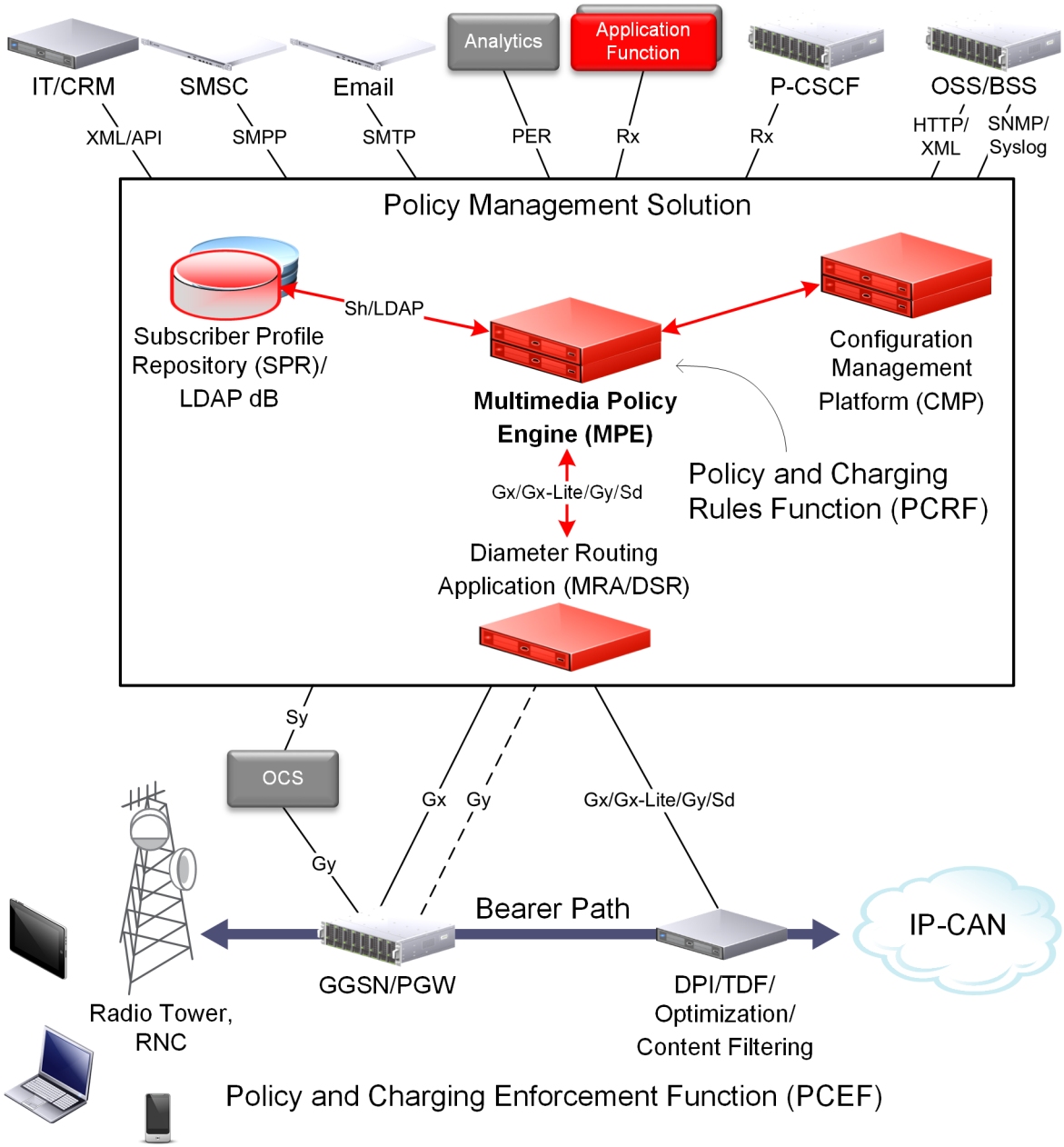


Figure 1: The Policy Management Solution and MPE Devices

Policy Front End Overview

The Policy Front End product (referred to in this document as the Multi-Protocol Routing Agent [MRA]) is a product deployed in a Policy Management network that maintains bindings that link subscribers to Multimedia Policy Engine (MPE) devices. An MPE is a Policy Charging and Rules Function (PCRF) device. An MRA ensures that all of a subscriber's Diameter sessions established over the Gx, Gxx, Gx Lite, Rx and Sd reference points reach the same MPE device when multiple and separately addressable MPE clusters are deployed in a Diameter realm.

An MRA device implements the proxy (PA1 variant) DRA functionality defined in the 3GP TS 29.203 [1] and 3GPP TS 29.213 [2] specifications, whereby all Diameter Policy and Charging Control (PCC) application messages are proxied through the MRA device.

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

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

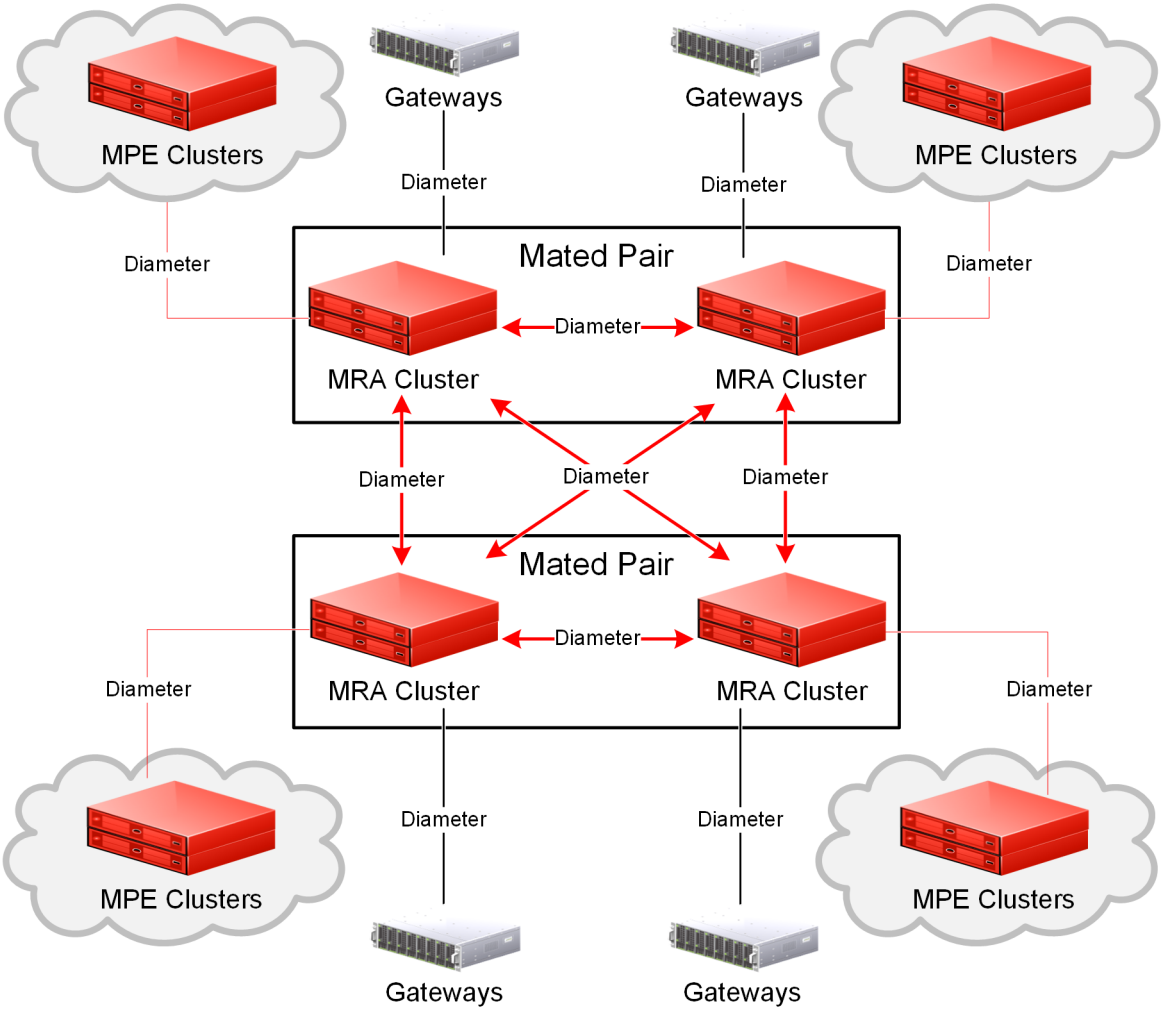


Figure 2: Typical Front End (MRA) Network

The Oracle Communications User Data Repository

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

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

The Oracle Communications Policy Management Configuration Management Platform

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

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

Specifications for Using the GUI

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

Web Browsers

- Mozilla Firefox® release 10.0 or higher
- Microsoft Internet Explorer® 10.0 or higher
- Google Chrome version 20.0 or higher

Monitor Use a resolution of 1024 x 768 or higher

Note: When using the CMP system for the first time, Oracle recommends that you change the default username and password to a self-assigned value. See *Changing a Password* for details.

Logging In

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

Before logging in, you need to know the following:

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

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

To log in:

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

You are logged in.

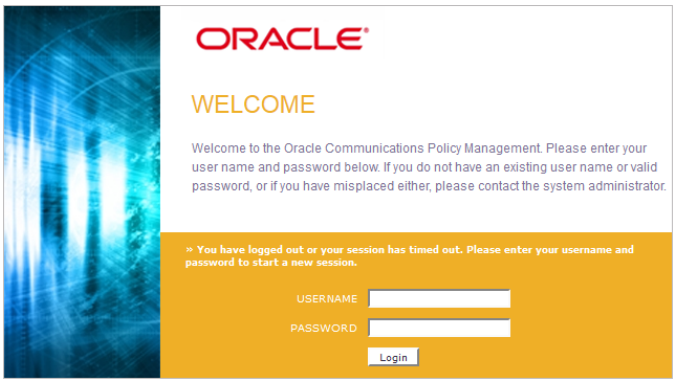


Figure 3: CMP Login Page

GUI Overview

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

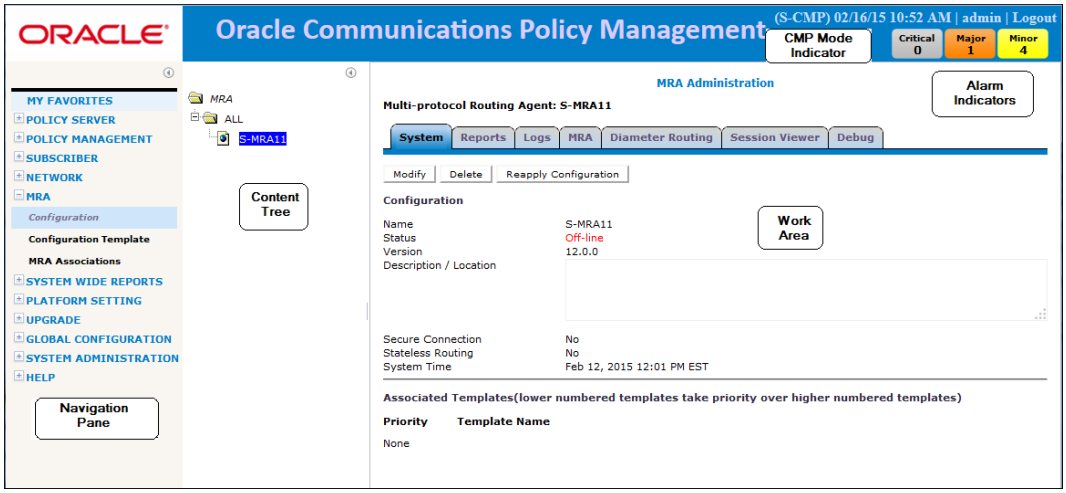


Figure 4: Structure of the CMP Wireless GUI

Navigation Pane	Provides access to the various available options configured within the CMP system. You can bookmark options in the navigation pane by right-clicking the option and selecting **Add to Favorite**. Access the bookmarks 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. The content tree section is not visible with all navigation selections. You can collapse the content tree to make more room by clicking the button in the top right corner of the pane ( ). Click the button again to expand the tree. You can also resize the content tree relative to the work area.
Work Area	Contains information that relates to choices in both the navigation pane and the content tree. This is the area where you perform all work.
Alarm Indicators	Provides visual indicators that show the number of active alarms.
CMP Mode Indicator	Indicates the current CMP mode. **NW-CMP** for Network mode or **S-CMP** for System mode. If there is not a mode indicated, the mode is **CMP**.

GUI Icons

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

Add	Use this icon to add an item to a list.
Calendar	Use this icon to select a date and, in some cases, time.
Clone	Use this icon to duplicate a selection in a list.
Critical error	Displays in reports to indicate a critical error during the blade replication process.
Delete	When visible in the work area, selecting the Delete icon deletes an item, removing it from the MPE device. **Note:** Deleting an item from the **ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.
× **Delete**	When visible in the work area, selecting the Delete icon deletes an item, removing it from the MPE device. **Note:** Deleting an item from the **ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.

Details	The binoculars icon displays when there is more details for an item.
Edit	Use this icon to modify a selection in a list.
External Connection	When visible in the work area, indicates which server currently has the external connection (the active server).
Gear	The gear icon displays when a policy references another policy or policy group.
Hide	When visible in the work area, selecting the hide icon removes the item from the current view but does not delete the item. **Note:** The item is only hidden during the current session. The item will be visible the next time a user logs into the CMP system.
Manual	Displays when a field is configured by the user. Hover over this icon to see the name of the device.
Major error	Displays in reports to indicate a major error during the blade replication process.
Minor error	Displays in reports to indicate a minor error during the blade replication process.
Up/Down	The up and down arrow icons are displayed when you can change the sequential order of items in a list.
Left/Right	The left and right arrow icons are displayed when it is possible to move an item from one list to another.
OK status	Displays in reports to indicate a that the blade replication process completed without error.
Remove	Removes an item from the group. The item is still listed in the ALL group and any other group that has an association with the item. For example, if you remove MPE device PS_1 from policy server group PS_Group2, PS_1 still displays in the ALL group.
Selection	This icon is in the Policy Wizard. The icon is used to select conditions and actions to add to the policy rule.
Synch broken	When visible in the Upgrade Manager, indicates that the CMP system does not have current information on a server.
Template	Displays when a field is configured by template. Hover over this icon to see the name of the template. Click the icon to view the template.

Overview of Main Tasks

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

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

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

The element and profile definition tasks you need to perform depend on what exists on your network. They can be defined in any order at any time as needed. The full set of tasks is as follows:

- Create network element profiles, including protocol options, for each network element with which Policy Management devices interact. This task is described in *Managing Network Elements*.
- Specify which Policy Management device will interact with which network element(s). 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 Subscriber Profile Repositories* and *Managing Subscribers*.

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

- View reports on the function of the Policy Management systems in your network. This task is described in *System-Wide Reports*.
- Manage CMP users, accounts, access, authorization, and operation. These tasks are described in *System Administration*.
- Upgrade software using the Upgrade Manager. These tasks are described in *Upgrade Manager*.

Chapter 3

Configuring the Policy Management Topology

Topics:

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

About the Policy Management Topology

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

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

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

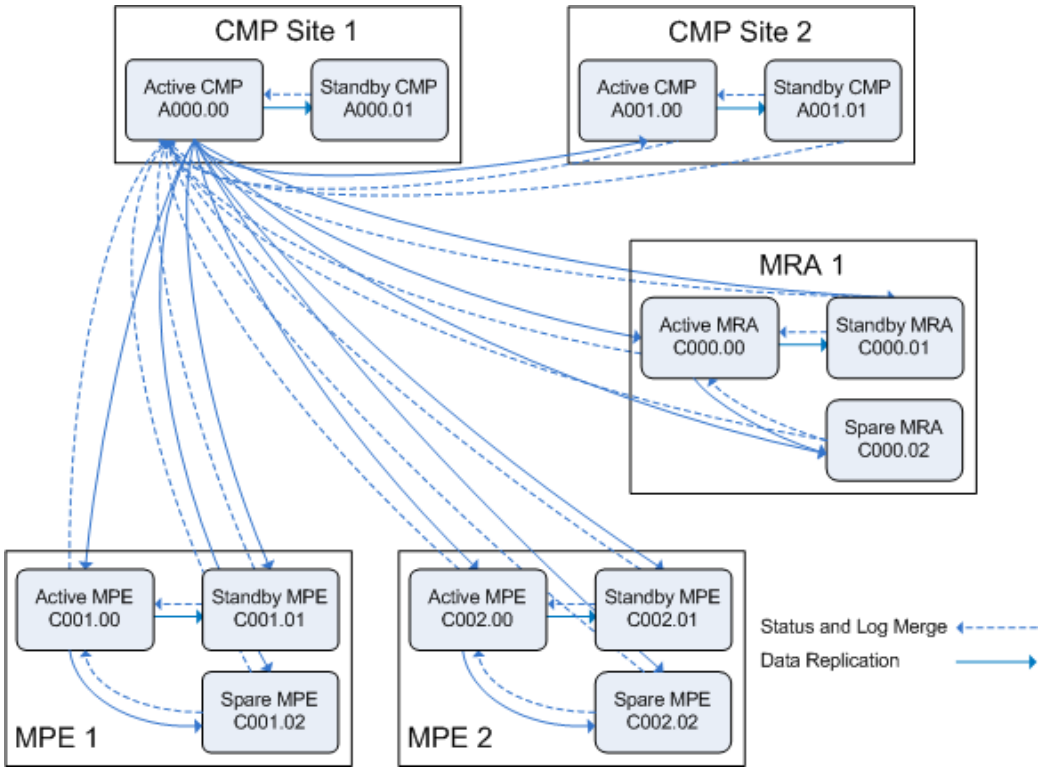


Figure 5: Policy Management Topology

High Availability

High Availability (HA) is provided for all Policy Management cluster configurations. HA is accomplished by using two servers per cluster, an active server and a standby server. Servers are continually monitored by the Communications Core Object Library (COMCOL) in-memory database. As shown in *Figure 6: High Availability*, the active server processes network traffic and is accessible and connected to external devices, clients, gateways, and so forth. Only one server in a cluster can be the active server.

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

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

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

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

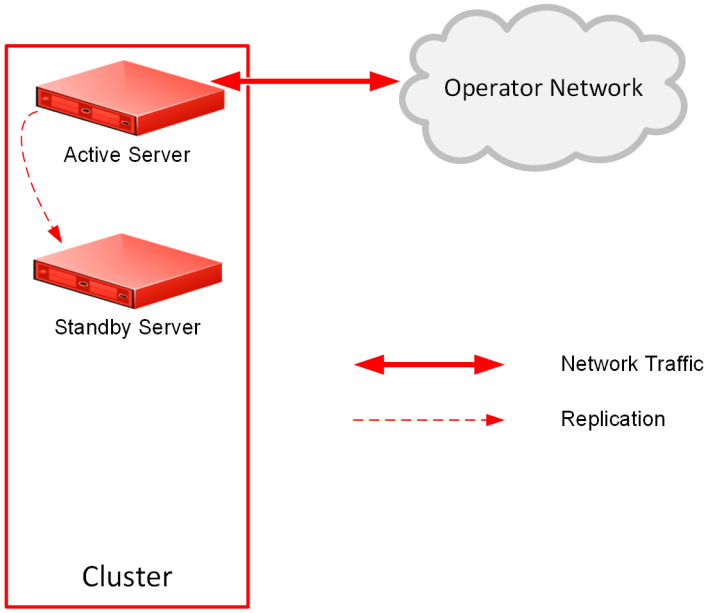


Figure 6: High Availability

Server Status

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

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

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

The status values are as follows:

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

Setting Up the Topology

Topology configuration consists of defining Policy Management sites and clusters, including their addresses and hierarchy. You can add C-level clusters to the topology before configuring the individual servers themselves. You can define all the servers in a cluster in the same operation.

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

1. Configure the primary CMP cluster — You start to build a topology by logging in to the active CMP server at the primary site. Configure the CMP cluster settings. The settings are replicated (pushed) to the standby CMP server. Together, the two servers form a primary, or Site 1, CMP cluster. This is the primary CMP site for the whole topology network. The primary site cannot be deleted from the topology.

2. Configure the secondary CMP cluster (optional) — Use the primary CMP cluster to configure a secondary, or Site 2, CMP cluster.
3. Configure C-level clusters — Enter C-level cluster settings on the active CMP server on the primary site. You can define the topology before defining the servers themselves. After the cluster is defined, the configuration information is replicated as follows:
   a. The active and standby servers communicate using several TCP connections over the OAM network. The topology configuration, including the cluster settings, is replicated to both servers. These servers form an MPE, MDF, or MRA cluster based on the topology configuration.
   b. The servers share a virtual IP (VIP) cluster address to support automatic failover.
   c. The COMCOL database runtime process constantly monitors the status of the servers in each cluster. If an active server fails, it instructs the standby server to take over and become the active server.

After you define the topology, go to the **System** tab for each server to determine if there are any topology mismatches. If there are any mismatches, make the necessary changes and reapply the configuration. See *Reapplying the Configuration to Policy Management Devices* for more information.

Setting Up a CMP Cluster

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

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

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

To set up the primary CMP cluster:

1. Log in to the CMP server.
2. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens. If a primary cluster is not yet defined, you are prompted, `Initial Configuration Detected. Please add CMP Site 1 Cluster`.
3. From the content tree, select the **All Clusters** group.
4. Click **Add CMP Site1 Cluster**.
   The **Cluster Settings** page opens. The cluster name and application type are fixed.
5. Enter the following information (*Figure 7: Cluster Settings Page for CMP Cluster* shows an example):
   a) **HW Type** — Select the type of hardware:
      - **C-Class** (default)
      - **C-Class(Segregated Traffic)** (for a configuration where Signaling and other networks are separated onto physically separate equipment)
      - **RMS** (for a rack-mounted server)
   b) **Network VLAN IDs** (appears if you selected **C-Class**, **C-Class(Segregated Traffic)**, or) — Enter the Operation, Administration, and Management (OAM), SIG-A, and (optionally) SIG-B

virtual LAN (VLAN) IDs, in the range 1–4095. The defaults are 3 for the OAM Virtual IP (VIP) and server IP, 5 for the SIG-A VIP, and 6 for the SIG-B VIP.

c) **OAM VIP** (required) — The OAM VIP is the IP address the CMP uses to communicate with a Policy Management cluster. Enter up to two OAM VIP addresses (one IPv4 and one IPv6) and their masks. Enter the address in the standard dot format and the subnet mask in CIDR notation from 0–32 (IPv4), or standard 8-part colon-separated hexadecimal string format and the subnet mask in CIDR notation from 0–128 (IPv6).

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

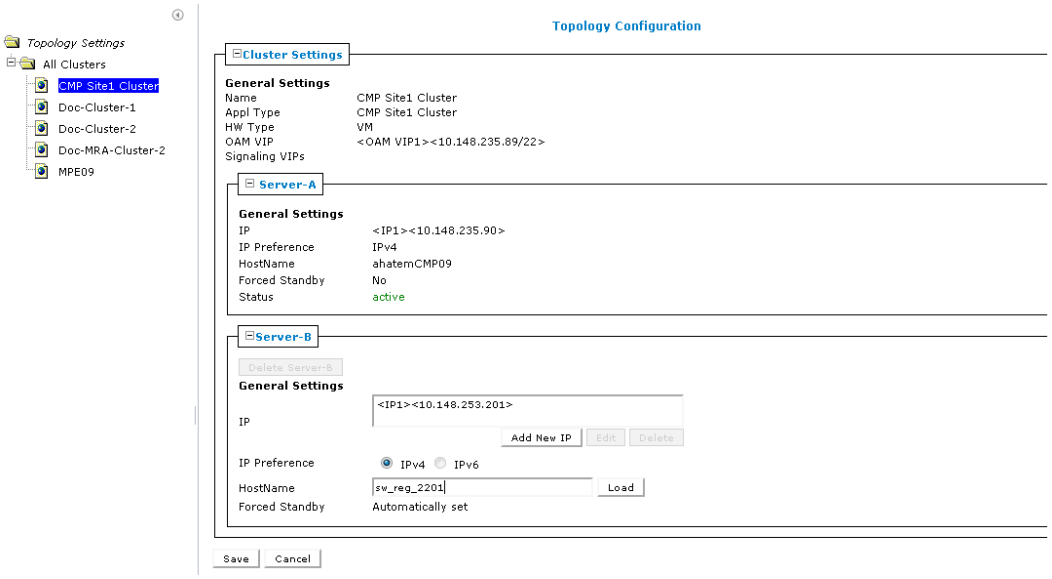


Figure 7: Cluster Settings Page for CMP Cluster

6. Select **Server-A** and enter the following information for the first server of the cluster (which will be the initial active server):

   a) **IP** (required) — The IP address of the server. Up to two IP addresses can be entered (one IPv4 and one IPv6). Use the standard dot-formatted IP address string for an IPv4 address, and the standard 8-part colon-separated hexadecimal string format for an IPv6 address.

   b) **IP Preference** — Specify the preferred IP version, either **IPv4** or **IPV6**. If IPv6 is selected, the server will prefer to use the IPv6 address for communication. If neither an IPv6 OAM IP nor a static IP address is defined, the IPv6 radio button cannot be selected here. Similarly, If neither an IPv4 OAM IP nor a static IP address is defined, the IPv4 radio button isn't accessible.

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

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

d) **Forced Standby** — Select to force this server into standby mode. The flag is set automatically when a new server is added to a cluster, or if a server setting is modified and another server already exists in the cluster.

7. When you finish, click **Save**.
   You are prompted, `The VLAN IDs on the page must match the VLAN IDs configured on the server. A mismatch will cause HA to fail. Please confirm that the VLAN IDs are correct before saving.`
8. Click **OK**.
   You are prompted, `Active server will restart and you will be logged out.`
9. Click **OK**.
   The active server restarts.
10. Log back in to the CMP server.
11. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
    The **Cluster Configuration** page opens.
12. From the content tree, select the **CMP Site1 Cluster**.
    The **Topology Configuration** page opens.
13. Select **Modify Server-B**, and enter the appropriate information for the second server of the cluster.
14. When you finish, click **Save**.

The CMP cluster topology is defined.

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

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

Setting Up a C-level Cluster

A C-level cluster is an MPE , MRA, or MDF cluster. Before defining a C-level cluster, ensure the following:

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

To define a C-level cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The **Cluster Configuration** page opens.
2. Click **Add MPE/MRA/Medition Server Cluster**.
   The **Topology Configuration** page opens.
3. Enter the following information. *Figure 8: Cluster Settings Page for MPE Cluster* shows an example:
   a) **Name** (required) — Name of the cluster. Enter up to 255 characters, excluding quotation marks (") and commas (,).
   b) **Appl Type** — Select **MPE** (the default), **MRA**, or **Mediation**.

c) **HW Type** — Select **C-Class** (the default), **C-Class(Segregated Traffic)** (for a configuration in which Signaling and OAM networks are separated onto physically separate equipment), or **RMS** (for a rack-mounted server).

d) **Network VLAN IDs** (appears if you selected **C-Class** or **C-Class(Segregated Traffic)**) — Enter the Operation, Administration, and Management (OAM), SIG-A, and SIG-B virtual LAN IDs, in the range 1–4095. The defaults are 3 for the OAM VIP and server IP, 5 for the SIG-A VIP, and 6 for the SIG-B VIP.

e) **OAM VIP** (optional) — Enter the IPv4 address and mask of the OAM virtual IP (VIP) address. The OAM VIP is the IP address the CMP cluster uses to communicate with the C-level cluster. Enter the address in the standard dot format, and the subnet mask in CIDR notation from 0–32.

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

f) **Signaling VIP 1** through **Signaling VIP 4** — Enter up to four IPv4 or IPv6 addresses and masks of the signaling virtual IP (VIP) addresses. For each address, select **None**, **SIG-A**, or **SIG-B** to indicate whether the cluster will use an external signaling network. The Signaling VIP is the IP address a PCEF device uses to communicate with an C-level cluster. You must enter a Signaling VIP value if you specify either SIG-A or SIG-B.

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

For a CMP cluster, the Signaling VIP is optional, but for a C-level cluster, at least one signaling VIP is required.

4. Select **Server-A** and enter the following information for the first server of the cluster:
   a) **IP** (required) — The IPv4 address of the server. Enter the standard dot-formatted IPv4 address string.
   b) **HostName** (required) — The name of the server. This must exactly match the host name provisioned for this server (that is, the output of the Linux command **`uname -n`**).
5. Once you define Server A, you can optionally click **Add Server-B** and enter the appropriate information for the second server of the cluster.
6. When you finish, click **Save**.
7. You are prompted with a confirmation message. Click **OK**.
8. If you are setting up multiple C-level clusters, repeat the above steps as often as necessary.

The C-level cluster is defined.

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

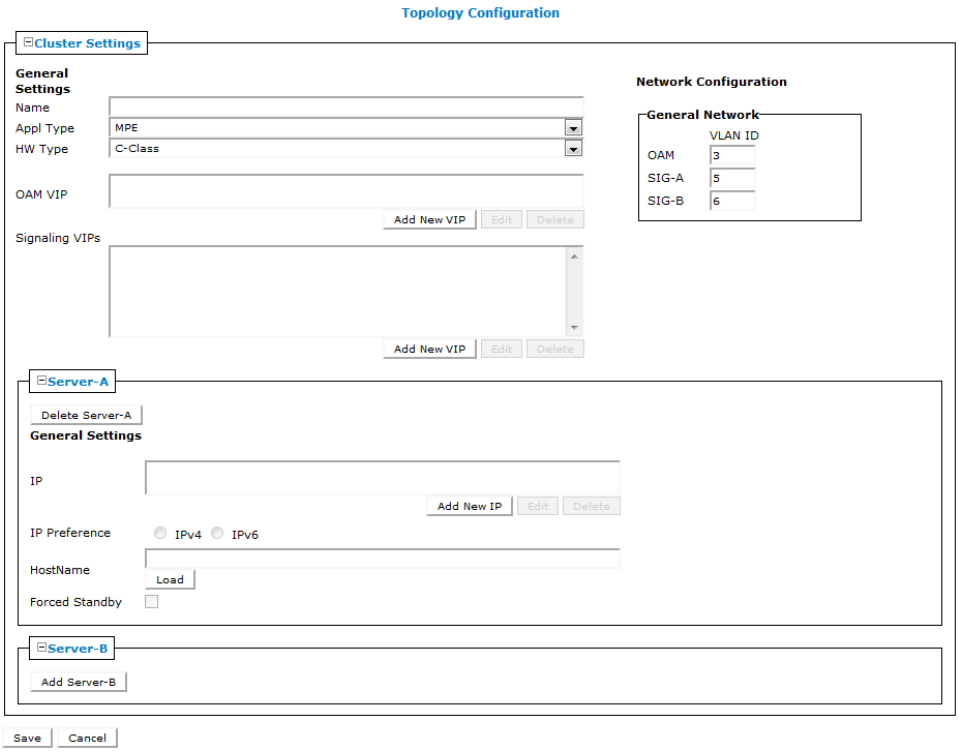


Figure 8: Cluster Settings Page for MPE Cluster

Modifying the Topology

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

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

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

Modifying a C-level Cluster

To modify a C-level cluster:

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

The **Topology Configuration** page displays information about the cluster.

3. Click the appropriate button for the changes you want to make:
   - To modify cluster settings, click **Modify Cluster Settings**.
   - To modify the primary site configuration, click **Modify Server-A**.
   - To modify the secondary site configuration, click **Modify Server-B**.

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

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

   CAUTION

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

   Note: If you add, remove, or modify a server, the active server restarts.
5. When you finish, click **Save**.
   The following message displays: `Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect.`
6. Click **OK**.

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

Modifying a CMP Cluster

To modify a CMP cluster:

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

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

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

   Note: If you add, remove, or modify a server, the active server restarts.
5. When you finish, click **Save**.
   The following message displays: `Warning: You may need to restart the application or reboot the server for the new topology configuration to take effect.`

6. Click **OK**.

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

Removing a Cluster from the Topology

You can remove an C-level or Site 2 CMP cluster from the topology. (You cannot remove the Site 1 (primary) CMP cluster from the topology.)

Before removing a C-level cluster from a fully configured system:

- Remove it from the MPE pool on an MRA device, or remove it as a backup MRA device.
- Remove the profiles of its servers; see *Deleting a Policy Server Profile*.

To remove a cluster from the topology:

1. From the **Platform Setting** section of the navigation pane, select **Topology Settings**.
   The **Cluster Configuration** page opens.
2. From the content tree, select the **All Clusters** folder.
   The **Cluster Configuration** page opens, displaying the Cluster Settings table that lists the information about the clusters defined in the topology.
3. In the topology configuration table, in the row listing the cluster you want to remove, click **Delete**.
   You are prompted with a confirmation message. Click **OK**.
4. Click **Delete**.
   The page closes.

The cluster is removed from the topology.

Forcing a Server into Standby Status

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

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

- If the server is active, it demotes itself.
- 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

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

To force a server into standby status:

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

2. In the Cluster Settings table, in the row listing the cluster containing the server you want to force into standby status, click **View**.
   The **Topology Configuration** page displays information about the cluster.
3. Select the server and click **Modify Server-A** or **Modify Server-B**.
4. Select **Forced Standby**.
5. Click **Save**.
   The page closes.

The server is placed in standby status.

Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network. You can configure the Policy Management network such that the CMP system collects and forwards all traps, or such that each server generates and delivers its own traps. To configure the SNMP trap forwarding, see *Table 2: SNMP Attributes* for information about the settings.

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

To configure SNMP settings:

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

   The navigation pane is displayed.

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

   The **SNMP Settings** page displays.

3. Click **Modify**.

   The **SNMP Settings** page opens.

4. Edit the settings.
5. When you finish, click **Save**.

Table 2: SNMP Attributes describes the SNMP attributes that can be edited.

Table 2: SNMP Attributes

Field Name	Description
Manager 1-5	SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IPv4/IPv6 address. These fields have the following restrictions: • A hostname should include only alphanumeric characters. • Maximum length is 20 characters. • Case insensitive (uppercase and lowercase are treated as the same). • This field can contain an IP address. An IP address should be in a standard dot-formatted IP address string.

Field Name	Description
	• Port configuration is optional for each manager and it can have a value between 1 and 65535. If this field is left blank, the port defaults to 162. By default, these fields are blank.
Enabled Versions	Supported SNMP versions: • **SNMPv2c** • **SNMPv3** • **SNMPv2c and SNMPv3 (default)**
Traps Enabled	Enable the sending SNMPv2 traps (default is enabled). **Note:** This option must be selected to use the SNMP Trap Forwarding feature. Clear the checkbox to disable sending SNMPv2 traps.
Traps from individual Servers	Enable sending traps from an individual server (default is disabled). **Note:** To use the SNMP Trap Forwarding feature, ensure that this option is not selected. Clear the checkbox to send traps from the active CMP system only.
SNMPv2c Community Name	The SNMP read-write community string. This field has the following restrictions: • The field is required if SNMPv2c is enabled. • The name can contain alphanumeric characters and cannot exceed 31 characters in length. • The name cannot be either **`private`** or **`public`**. The default value is **`snmppublic`**.
SNMPv3 Engine ID	Configured Engine ID for SNMPv3. This field has the following restrictions: • The field is required If SNMPv3 is enabled. • The Engine ID includes only hexadecimal digits (0-9 and a-f). • The length can be from 10 to 64 digits. The default is no value (empty).
SNMPv3 Security Level	SNMPv3 Authentication and Privacy options are: • **No Auth No Priv** — Authenticate using the Username. No Privacy. • **Auth No Priv** — Authentication using MD5 or SHA1 protocol. • **Auth Priv** — Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol. The default value is **Auth Priv**.

Field Name	Description
SNMPv3 Authentication Type	Authentication protocol for SNMPv3. Options are: • **SHA-1** — Use Secure Hash Algorithm authentication. • **MD5** — Use Message Digest authentication. The default value is **SHA-1**.
SNMPv3 Privacy Type	Privacy Protocol for SNMPv3. Options are: • **AES** — Use Advanced Encryption Standard privacy. • **DES** — Use Data Encryption Standard privacy. The default value is **AES**.
SNMPv3 Username	The SNMPv3 User Name. This field has the following restrictions: • The field is required if SNMPv3 is enabled. • The name must contain alphanumeric characters and cannot not exceed 32 characters in length. The default value is **`TekSNMPUser`**.
SNMPv3 Password	Authentication password for SNMPv3. This value is also used for msgPrivacyParameters. This field has the following restrictions: • The field is required If SNMPv3 is enabled. • The length of the password must be between 8 and 64 characters and can include any character. The default value is **`snmpv3password`**.

Platform Configuration Settings

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

Configuring the Upsync Log Alarm Threshold

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

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

To configure the upsync log alarm threshold:

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

   The **Platform Configuration** page is displayed.

2. Click **Modify**.
3. Enter the threshold.
4. When you finish, click **Save**.

Configuring Concurrent Bulk Transfers

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

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

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

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

   The **Platform Configuration** page is displayed.

2. Click **Modify**.
3. Enter the number bulk transfers. Valid values are 1 to 8. 1 is the default.
4. When you finish, click **Save**.

Chapter 4

Managing Multimedia Policy Engine Devices

Topics:

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

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

Policy Server Profiles

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

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

Creating a Policy Server Profile

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

To create a policy server profile:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Policy Server Administration** page opens in the work area.
3. Click **Create Policy Server**.
   The **New Policy Server** page opens.
4. Enter values for the configuration attributes:
   a) **Associated Cluster** (required) — Select the cluster with which to associate this MPE device.
   b) **Name** — Name of this MPE device. The default is the associated cluster name. A name is subject to the following rules:
      - Case insensitive (uppercase and lowercase are treated as the same)
      - Must be no longer than 255 characters
      - Must not contain quotation marks (") or commas (,)
   c) **Description / Location** (optional) — Information that defines the function or location of this MPE device.
   d) **Secure Connection** — Designates whether or not to use the HTTPS protocol for communication between Policy Management devices. If selected, devices communicate over port 8443.
   e) **Type** — Defines the policy server type:
      - **Oracle** (default) — The policy server is an MPE device and can be fully managed by the CMP.
      - **Unmanaged** — The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non-Oracle policy server.
5. (Optional) Associate templates. See *Managing Configuration and Virtual Templates* for information about virtual templates.
6. When you finish, click **Save**.

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

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

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

Configuring or Modifying a Policy Server Profile

To configure or modify a policy server profile:

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

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

   The page contains the following tabs:

   - **System** — Defines the system information associated with this policy server, including the name, host name or IP address in IPv4 or IPv6 format, information about the policy server, and whether or not the policy server uses a secure connection to any management system (such as the CMP).
   - **Reports** (read only)— Displays various statistics and counters related to the physical hardware of the cluster, policy execution, and network protocol operation. Reports cannot be modified.
   - **Logs** — Displays the Trace Log, Syslog, and SMS log configurations.
   - **Policy Server** — Lets you associate applications and network elements with the MPE device and configure protocol information.
   - **Diameter Routing** — Lets you configure the Diameter peer and route tables.
   - **Policies** — Lets you manage policies that are deployed on the policy server.
   - **Data Sources** — Lets you configure interfaces to LDAP (Lightweight Directory Access Protocol), Diameter Sh, or SPR (Subscriber Profile Repository) systems.
   - **Session Viewer** (read only)— Displays static session and binding data for a specific subscriber from the Policy Management device that is managing the session.

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

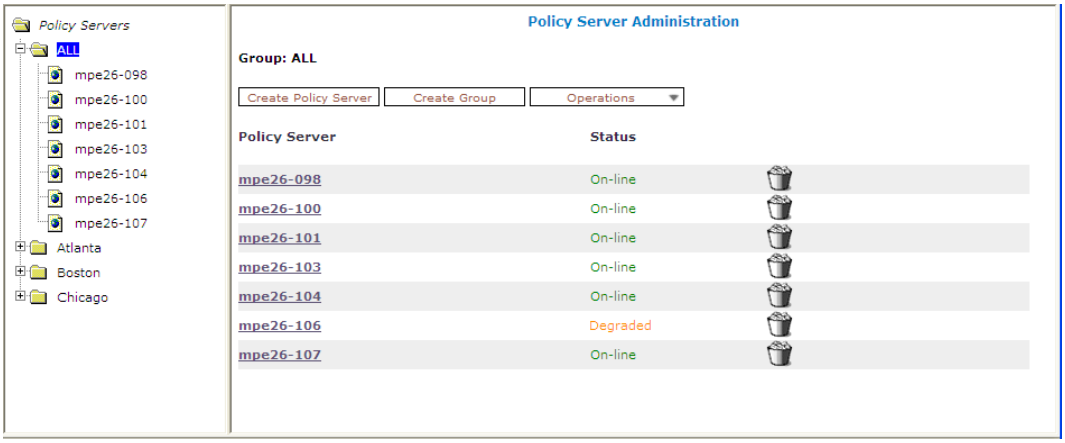
Deleting a Policy Server Profile

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

To delete an MPE device profile:

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

   The **Policy Server Administration** page opens in the work area, displaying all defined MPE devices; for example:



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

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

The policy server profile is deleted.

Managing Configuration and Virtual Templates

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

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

Overlaps

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

- Remove the overlaps and use the settings from the template.
- Keep the overlaps and use the settings from the server.

Creating a Template

Since an MPE or an MRA can exist independently of one another, there are two locations in the Policy Management interface where, both virtual and configuration, templates can be created. Either in the **MRA** or the **Policy Server** section of the navigation pane. After the template is created, the template has the functionality that is specific to their instance (MPE or MRA).

Note: This procedure applies to both MPE or MRA devices

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

To create a configuration template:

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

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

5. (Optional) Select a template from the **Copy From** list
6. (Optional) Enter a **Description / Location** (limited to 255 characters).
7. When you finish, click **Save**.

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

Modifying a Template

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

Note: This procedure applies to both MPE or MRA devices

To modify a configuration template:

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**. The content tree displays a list of all templates including Virtual and Configuration.
2. From the content tree, select the configuration template for modification.
   The **Configuration Template Administration** page opens with the template.
3. Click **Modify**. From the **MRA** and **Diameter Routing** tabs, you can configure the following:
   - From the **MRA** section you have the following tabs and options:
     - **Template** tab
       - **Name**

    - **Description**
  - **MRA** tab - **Modify** button
    - **Associations** or
    - **MPE Pools**
    - **Subscriber Indexing**
    - **Diameter** settings
  - **MRA** tab - **Advanced** button
    - **Expert Settings**
    - **Service Overrides**
    - **Load Shedding Configuration**
  - **Diameter Routing** tab
    - **Diameter Peers**
    - **Diameter Routes**

- From the **Policy Server** section you have the following tabs and options:
  - **Template** tab
    - **Name**
    - **Description**
  - **Logs** tab
    - **Modify Policy Log Settings**
    - **SMS Log Configuration**
    - **SMTP Log Configuration**
  - **Policy Server** tab - **Modify** button
    - **Associations**
    - **Subscriber Indexing**
    - **Configuration**
    - **Diameter** settings
    - **User Profile Lookup Retry on Session Updates**
    - **Diameter AF Default Profiles**
    - **Default Charging Servers**
  - **Policy Server** tab - **Advanced** button
    - **Expert Settings**
    - **Service Overrides**
    - **Load Shedding Configuration**
  - **Diameter Routing** tab
    - **Diameter Peers**
    - **Diameter Routes**
  - **Policies** tab
    - **Deployed Policies**

- **Data Sources** tab
  - **Data Sources**
  - **General Settings**
  - **Sh Settings**

4. When you finish, click **Save**.

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

Reordering Templates

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

Note: This procedure applies to both MPE or MRA devices

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

1. From the **MRA** or **Policy Server** section of the navigation pane, select **Configuration Template**.
   The content tree displays a list of all templates including Virtual and Configuration.
2. From the content tree, select the configuration template for modification.
   The **Configuration Template Administration** page opens with the template.
3. Click **Modify**.
4. Edit the numbers in the priority field.
5. Click **Update Order**.
   The associated templates are reodered.

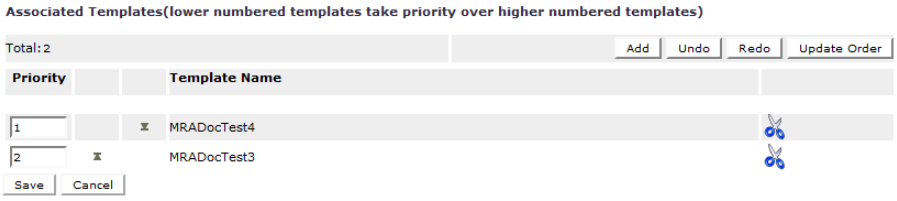


Figure 9: Original Template List

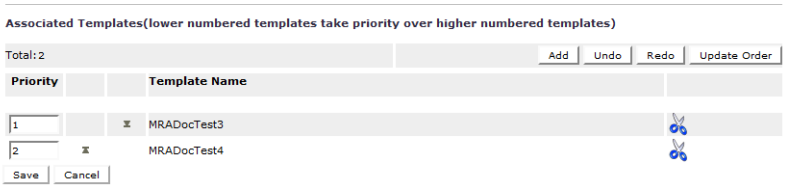


Figure 10: Reordered Template List

Creating Virtual Templates

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

Note: This procedure applies to both MPE or MRA devices

Complete these steps to create a configuration template.

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

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

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

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

5. Select a template from the **Associated Configuration Template** pull-down menu.
6. (Optional) Type in a **Description**.
7. When you finish, click **Save**.

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

Configuring Protocol Options on the Policy Server

To configure protocol options on an MPE device:

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

   Selecting or choosing **undefined** signifies that the value come from a configuration profile. If there is not a configuration profile, then the default is used. The following tables define the available options. (The options you see vary depending on the mode configuration of your system.)

   - *Table 3: Associations Configuration Options*

- *Table 4: Subscriber Indexing Configuration Options*
- *Table 5: General Configuration Options*
- *Table 6: RADIUS-S Configuration Options*
- *Table 7: Diameter Configuration Options*
- *Table 8: User Profile Lookup Retry and Session Updates Configuration Options*
- *Table 9: Diameter AF Default Profiles Configuration Options*
- *Table 10: Default Charging Servers Configuration Options*
- *Table 12: SMS Relay Configuration Options*
- *Table 13: SMPP Configuration Options*
- *Table 14: Primary SMSC Host Configuration Options*
- *Table 15: Secondary SMSC Host Configuration Options*
- *Table 16: SMTP Configuration Options*
- *Table 17: RADIUS Configuration Options*

5. When you finish, click **Save**.

You have defined the protocol options for this MPE device.

Table 3: Associations Configuration Options

Attribute	Description
Applications	The application profiles associated with this MPE device. To modify this list, click **Manage**. For more information on application profiles, see the *Policy Wizard Reference*.
Network Elements	The network elements associated with this MPE device. To modify this list, click **Manage**. For more information on network elements, see *Managing Network Elements* .
Network Element Groups	The network element groups associated with this MPE device. To modify this list, select or deselect groups. For more information on network element groups, see *Managing Network Elements* .

Table 4: Subscriber Indexing Configuration Options

Attribute	Description
Index by IPv4	Select if the associated Subscriber Profile Repository is indexed by IPv4 address.
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.

Attribute	Description
Index by IMSI	Select if the associated Subscriber Profile Repository is indexed by International Mobile Subscriber Identity (IMSI) number.
Overrides by APN	Select to configure an alternate subscriber indexing by IP address, Username, NAI, E.164 (MSISDN) and IMSI for a specific access point name (APN). In the **Overrides by APN** section, click **Add**. Enter the APN and click **Save** to enable Index by IPv4, Index by IPv6, or both. You can create new APN overrides by cloning or editing existing APN overrides. You can also delete an APN override.

Table 5: General Configuration Options

Attribute	Description
Time of Day Triggering	Select **Enable** or **Disable** (default) from the pulldown menu. If you select **Enable**, this MPE device supports time-of-day triggering when evaluating policy rules. For more information on time-of-day triggering, see the *Policy Wizard Reference*.
Billing Day	If enabled, you can configure a global monthly billing day for subscribers who do not have a specific day configured in their profiles in a backend database.
Billing Day of Month	If **Billing Day** is enabled, enter the day of the month on which subscriber usage counters are reset. This date is the default billing date for all 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 selected, the MPE device observes Daylight Saving Time for the configured Billing Time Zone.
Default Local Time Mode	Select the time used within a user's session from the pulldown menu: **System Local Time** to use the local time of the MPE device (default) or **User Local Time** to use the user's local time. **Note:** If the time zone was never provided for the user equipment, system local time is applied.
Enable Pro Rate	If disabled, the full monthly quota for the subscribers is granted for the billing cycle following a quota reset. If enabled, the monthly quota for subscribers is prorated, on a per-quota basis (for up to 30 quotas), for the billing cycle following a quota reset, based on the value of the **Billing Date Effective** field in the subscriber's profile. This is a global setting affecting all subscribers. (If the field value is null, usage will not be prorated.)

Attribute	Description

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

Track Usage for Unknown Users	If enabled, the MPE device tracks usage and state per subscriber ID, even if the subscriber is not registered in the SPR. If tracking was enabled and is now disabled, usage and state is no longer tracked for unknown users, but existing usage and state data is retained.
Subscribe For Unknown Users	If Validate User is *off* (at the MPE device), then the unknown users are allowed to create sessions. In this case, if Subscribe for Unknown Users is enabled, then the MPE device will subscribe for those users. **Note:** This setting is only for the MPE device and does not have any effect on the SPR. There are settings in the SPR that must be set to allow auto-enrolling.
Use Single Lookup	If enabled, the MPE device reads multiple Sh user data blocks (subscriber, quota usage, and entity state) with a single read request. If you enable this feature, you must also configure the Sh data source with the option **Notif-Eff**. If disabled, separate lookups are used.
Use Combined Writes	The MPE device will combine the updates (PUR messages) resulting from a single user request into a single PUR update to the SPR. The PUR will contain both the quota usage and state updates for the user. This reduces the number of transactions between the MPE and SPR.
Cache Quota Usage	If enabled, the MPE device caches the quota usage objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.
Cache Entity State	If enabled, the MPE device caches the entity state objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.
Subscribe Quota Usage	Subscribe to receive notifications from the SPR for any changes to the quota.
Subscribe Entity State	Subscribe to receive notifications from the SPR for any changes to the entity state.

Table 6: RADIUS-S Configuration Options

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

Table 7: Diameter Configuration Options

Attribute	Description
Diameter Realm	The domain of responsibility (for example, **`galactel.com`**) for the MPE device.
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, **`mpe3.galactel.com`**).
Default Resource Id	The bearer used if a GGSN does not send any bearer information in a Credit-Control Request (CCR). Enter an alphanumeric string of up to 100 characters. The default is no resource ID (that is, no bearer).
Correlate PCEF sessions	If selected, the primary PCEF Gx session will share information with all secondary sessions that share an IP address within the same IP-CAN session. Up to 10 different Gx sessions can be correlated to one subscriber. By default, PCEF sessions are not correlated, and do not share information.
Validate user	If enabled, sessions for unknown users are rejected.

Attribute	Description
Diameter PCEF Default Profile	Select the default traffic profile from the list that will be applied during PCEF session establishment using the Gx or Ty protocols, or if no other SCE traffic profile is applied as a result of a policy being triggered.
Use Synchronous Sd	If selected, the MPE device establishes an Sd session before sending a Gx CCA message to a traffic detection function (TDF).
Identify Duplicate sessions based on APN	If enabled, the MPE device will detect duplicate sessions. This makes it possible to remove duplicate sessions if their number becomes excessive.
Subscriber ID to detect duplicate sessions	Available only if **Identify Duplicate sessions based on APN** is selected. Select the subscriber index type to use from the pulldown list: • **Username** • **NAI** • **E.164 (MSISDN)** • **IMSI**
Protocol Timer Profile	The timer profile to use.
Prevent Overlapping Rule Names	If selected, rule names that are dynamically generated on the primary and spare MPE devices in the same Gx session are unique.
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).

Table 8: User Profile Lookup Retry and Session Updates Configuration Options

Attribute	Description
Enforcement	If enabled, allows user profile lookup retry on session updates for Gx and Gxx updates.
Application	If enabled, allows user profile lookup retry on session updates for Rx.

Table 9: Diameter AF Default Profiles Configuration Options

Attribute	Description
Default	Define the bandwidth parameters that are used when a request from an Application Function (AF) does not contain sufficient information for the MPE device to derive QoS parameters. These profiles are defined per media type: The **Default** profile is used when a profile for a media type is not defined. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.

Attribute	Description
Audio	The profile for the audio. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.
Video	The profile for the video. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.
Data	The profile for data. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.
Application	The profile for application. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.
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. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.
Message	The profile for messages. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.
Other	The profile for all other media types. **Note:** To select a profile, first create a Diameter profile in the general profile configuration.

Table 10: Default Charging Servers Configuration Options

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

Table 11: Default Charging Methods Configuration Options

Attribute	Description
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.

Table 12: SMS Relay Configuration Options

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

Table 13: SMPP Configuration Options

Attribute	Description
SMPP Enabled	Select to enable Short Message Peer to Peer (SMPP) messaging to subscribers. To send an SMS message to a subscriber, a Mobile Station International Subscriber Directory Number (MSISDN) must be present in the subscriber's profile. Messages can be up to 254 characters long.
Validate Message Length	Select to validate message length.
SMPP Long Message Support	If selected, SMS messages longer than 160 characters are split into segments and reassembled by the receiving device. Messages of up to 1000 characters are supported.
Delivery Method for Long Message	Select the message delivery method for long messages from the pulldown list: • **Segmentation and Reassembly (SAR)** (default) • **Message Payload**

Table 14: Primary SMSC Host Configuration Options

Attribute	Description
SMSC Host	Enter the FQDN or IP address of the primary Short Messaging Service Center store-and-forward server, which accepts SMS messages from the relay server.

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

Table 15: Secondary SMSC Host Configuration Options

Attribute	Description
SMSC Host	Enter the FQDN or IP address of the secondary Short Messaging Service Center store-and-forward server, which accepts SMS messages from the relay server. The secondary SMSC server is used if the primary server fails.
SMSC Port	Enter the port number on which the secondary Short Messaging Service Center store-and-forward server is listening for SMS messages. The default port is 2775.
ESME System ID	Enter the system ID of the secondary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source. **Note:** This value must be configured on the secondary SMPP server.
ESME Password	Enter the password of the secondary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source. **Note:** This value must be configured on the SMPP server.
Confirm ESME Password	Re-enter the secondary ESME password for verification.
ESME Source Address	Enter the source address for a SUBMIT_SM operation in SMPP Protocol V3.4. The default is none.
ESME Source Address TON	Select the source address Type of Number (TON) from the pulldown menu: • **UNKNOWN** (default) • **INTERNATIONAL** • **NATIONAL** • **NETWORK SPECIFIC**

Attribute	Description
	• **SUBSCRIBER NUMBER** • **ALPHANUMERIC** • **ABBREVIATED**
ESME Source Address NPI	Select the source address Number Plan Indicator (NPI) from the pulldown menu: • **UNKNOWN** (default) • **ISDN (E163/E164)** • **DATA (X.121)** • **TELEX (F.69)** • **LAND MOBILE (E.212)** • **NATIONAL** • **PRIVATE** • **ERMES** • **INTERNET (IP)** • **WAP CLIENT ID**
Character Encoding Scheme	Select the character-set encoding for SMS messages from the pulldown menu: • **SMSC Default Alphabet** • **IA5 (CCITT T.50)/ASCII (ANSI X3.4)** • **Latin 1 (ISO-8859-1)** • **Cyrillic (ISO-8859-5)** • **Latin/Hebrew (ISO-8859-8)** • **UCS2 (ISO/IEC-10646)** • **ISO-2022-JP (Music Codes)** • **JIS (X 0208-1990)** • **Extended Kanji JIS(X 212-1990)**
SMSC Default Encoding Scheme	Select the SMSC default encoding from the pulldown menu: **UTF-8** or **GSM7**.
Request Delivery Receipt	Select the global default behavior when evaluating the policy action **send SMS** from the pulldown menu: • **No Delivery Receipt** • **Delivery Receipt on success and failure** • **Delivery Receipt on failure**

Table 16: SMTP Configuration Options

Attribute	Description
SMTP Enabled	Select to enable Simple Mail Transport Protocol (SMTP) messaging (email) to subscribers. SMTP notifications are triggered from policy action and sent through an SMS Relay (SMSR) function to an external mail transfer agent (MTA).

Attribute	Description
	Note: There is no delivery receipt for the SMTP messages sent from the SMSR, only confirmation that it reached the configured MTA.
MTA Host	Enter the FQDN or IP address of the Mail Transfer Agent server, which accepts SMTP messages from the SMSR function.
MTA Port	Enter the port number on which the MTA server is listening for SMTP messages. The default port is 25.
MTA Username	Enter the system ID of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. **Note:** This value must be configured on the MTA.
MTA Password	Enter the password of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. **Note:** This value must be configured on the MTA.
Confirm MTA Password	Re-enter the password for verification. **Note:** This is a new configuration setting for the SMTP connection.
Default From Address(es)	Enter the source address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none. **Note:** The total number of To, CC, and BCC addresses is limited to five.
SMTP Connections	The number of SMTP connections. Enter a number from 1–10. **Note:** SMTP connections can be increased to support a higher throughput.
Default Reply-To Address(es)	Enter the email address automatically inserted into the To field when a user replies to an email message. For most email messages, the From and Reply-To fields are the same, but this is not necessarily so. If no Default Reply-To is specified here, the From address is used. Optionally, enter a static email address to use for Reply-To. The default is none.
Default CC Address(es)	Enter the copy address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none. **Note:** The total number of To, CC, and BCC addresses is limited to five.
Default BCC Address(es)	Enter the blind copy recipient address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none. **Note:** The total number of To, CC, and BCC addresses is limited to five.
Default Signature	Enter the text that appears as a signature in an SMTP message. The default is none.

Table 17: RADIUS Configuration Options

Attribute	Description
RADIUS Enabled	When selected, the MPE device processes RADIUS messages; when deselected, 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 unset as well, then the MPE device ignores RADIUS requests and responses. The default is **radius**.
Correlate to RADIUS	If selected, Diameter DPI sessions will share information with RADIUS sessions. By default, sessions are not correlated, and do not share information.

Configuring Data Source Interfaces

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

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server.
   The **Policy Server Administration** page opens.
3. Select the **Data Sources** tab.
   The current data sources are displayed, listing the following information:
   - Administrative state
   - Name
   - Role
   - Type
   - Primary host
   - Secondary host

- Tertiary host

4. To modify the list of data sources, click **Modify**.

   The **Modify Data Sources** page opens. The functions available from this table are as follows:

   - Adding a data source.
     1. Click **Add**.
     2. Select the data source type from the **Add** pulldown list. The appropriate **Add Data Source** window opens.
     3. Configure values.
        - For LDAP data sources, see *Configuring an LDAP Data Source*.
        - For an Sh data source, see *Configuring an Sh Data Source*.
        - For an Sy data source, see *Configuring an Sy Data Source*.
   - Cloning a data source in the table
     1. Select an existing data source in the table.
     2. Click **Clone**. The **Clone Data Source** window opens with the information for the data source.
     3. Make changes as required.
     4. When you finish, click **Save**. The data source is added to the table
   - Editing a data source in the table
     1. Select the data source in the table.
     2. Click **Edit**. The **Edit Data Source** window opens, displaying the information for the data source.
     3. Make changes as required.
     4. When you finish, click **Save**. The data source is updated in the table.
   - Deleting a data source from the table
     1. Select the data source in the table.
     2. Click **Delete**. A confirmation message displays.
     3. Click **Delete** to remove the data source entry. The data source is removed from the table.
   - Ordering the list.

     If you define multiple entries, they are searched in the order displayed in this list. To change the order:
     1. Select an entry.
     2. Click **Up** or **Down**. The search order is changed.

   When you finish, click **Save**.

5. The following general settings are available:
   - **Merge Search Results** — If you define multiple data sources and a search returns results from more than one source, the results are displayed in source order. To display one sorted list instead, select this option.
   - **Subscription Enabled Via Policy Only** — For detailed information, see the SPR documentation.

6. The following Sh general settings are available:
   - **Combine Lookup And Subscription** — If selected, lookup and subscription requests are combined.
7. The following Sy general setting is available:
8. When you finish, click **Save**.

Configuring an LDAP Data Source

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

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

Server Info Tab

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

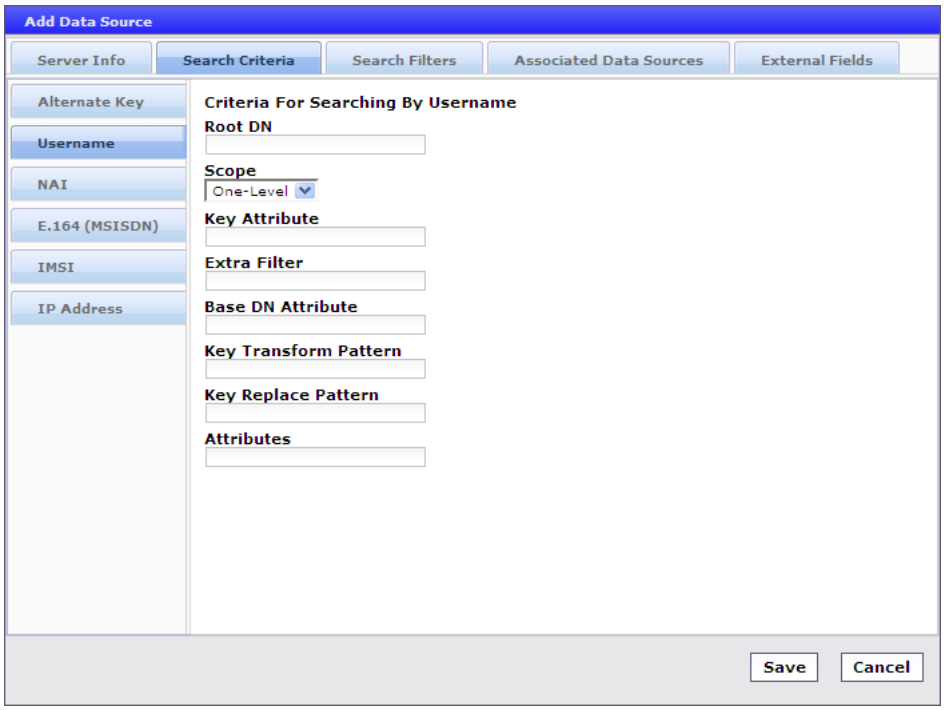
Role	Data source attribute:	
	Primary	The data source which performs the initial level of lookups.
	Secondary	Indicates a dependency on the results of the prior lookup. It must initially be associated with the primary data source and configured to be used in a subscriber lookup.
Unique Name	Name given to associate with the created LDAP.	
Admin State	Select to enable this data source. Selected by default.	
Read Enabled	Select to enable read access to this data source. Selected by default.	
Write Enabled	Select to enable write access to this data source.	
Primary Host	FQDN or IP address in IPv4 or IPv6 format of primary LDAP server.	
Primary Port	Port number of primary server. The default port number is 389.	
Secondary Host	FQDN or IP address in IPv4 or IPv6 format of secondary LDAP server.	
Secondary Port	Port number of secondary server. The default port number is 389.	
Tertiary Host	FQDN or IP address in IPv4 or IPv6 format of tertiary LDAP server.	
Tertiary Port	Port number of tertiary server. The default port number is 389.	
Authentication DN	The Distinguished Name (DN) used for binding to the LDAP server. The DN can refer to an entry in the directory or to a relative distinguished name (RDN). RDN attributes include cn (common name), uid (user ID), ou (organizational unit), and o (domain name). For example:	

	`cn=PolicyServer,ou=galactel,o=galactel.com`
LDAP Password	Provides read-only access to the LDAP directory. The MPE device must bind to the LDAP server with the DN and password to access the database. Example: **`LDAPpassword`**.
Read Connections	Enabled for data sources set in the Secondary role. Select up to 10 connections.
Write Connections	Disabled for data sources set in the Secondary role. Select up to 10 connections.

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

Search Criteria Tab

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



1. Select how the LDAP database is indexed:
   - **Alternate Key** — The Alternate Key has an LDAP data source role of primary.

     Note: If you select alternate key indexing, there are no options, so the rest of tab becomes blank.

   - **Username** — The database is indexed by user name (account ID).
   - **NAI** — The database is indexed by NAI (network access ID).

- **E.164 (MSISDN)** — The database is indexed by E.164 (E.164 phone number).
- **IMSI** — The database is indexed by International Mobile Subscriber Identity.
- **IP Address** — The database is indexed by IP address.

2. **Root DN** — The root distinguished name for the LDAP search.
3. **Scope** — Scope of the LDAP search:
   - **Object** — Restrict the scope of the LDAP search to the specified object.
   - **One-Level** (the default) — Extend the scope of the LDAP search one level under the given search base.
   - **Sub-Tree** — Extend the scope of the LDAP search to the whole subtree under the given search base.
4. **Key Attribute** — The attribute whose value is checked to match the key value; used to construct a search filter of the form *KeyAttribute=KeyValue*.
5. **Base DN Attribute** — This attribute will be prefixed to the root distinguished name when building the DN for a search.
6. **Key Transform Pattern** — Regular expression (regex) pattern to use to transform a key.
7. **Key Replace Pattern** — Replacement string to use to transform the key.

   For example, **`17$2`** means the new string starts with 17 and is followed by the group 2 ($2) pattern.
8. **Attributes** — Comma-separated list of entries defining how to save attributes in the object returned from the LDAP search.

   The default is null, meaning that all values are saved using the attribute name used in LDAP. Otherwise, each entry should be one of the following:
   - *attr* — A field is saved with the same name and value as the specified attribute.
   - *field=attr* — A field with the specified name is saved with the value of the specified attribute.
   - *field=attr*[*from*:*to*] — A field with the specified name is saved with a substring of the value of the specified attribute.

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

Search Filters Tab

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

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

1. **Key Type** — Select from the list:
   - **User Name** (the default) — User name (account ID)
   - **NAI** — Network address ID
   - **E.164(MSISDN)** — E.164 phone number
   - **IMSI** — International Mobile Subscriber Identity
   - **IP Address** — IP address
2. **Expression** — Enter a regular expression.

   For example:

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

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

3. When you finish, click **Save**.
   The expression is added to the filters.

The LDAP data source filters are defined.

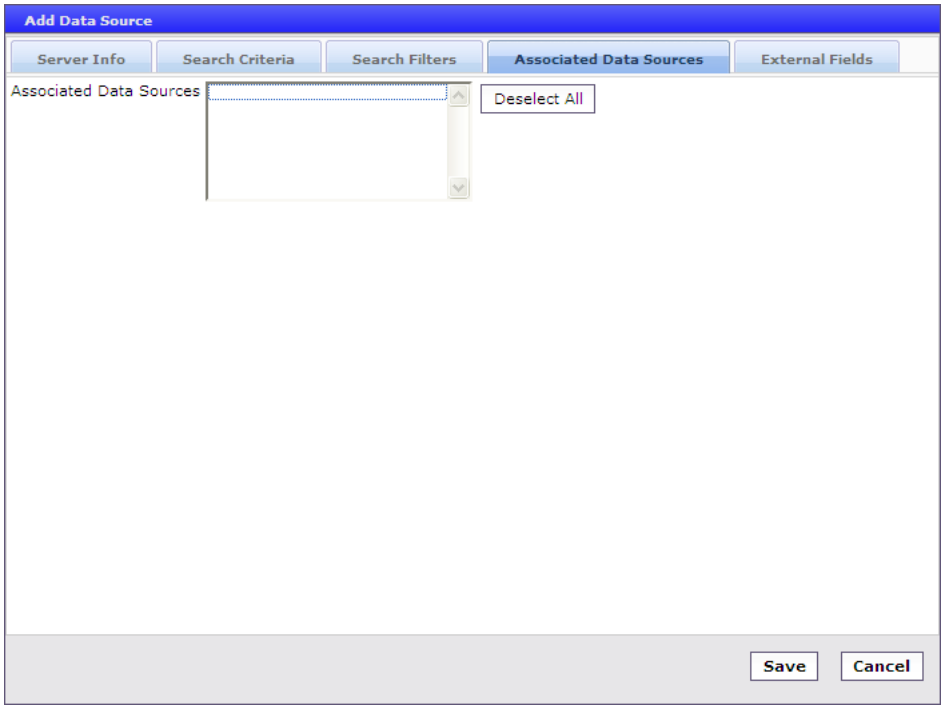
Associated Data Sources Tab

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

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

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

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



External Fields Tab

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

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

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

Configuring an Sh Data Source

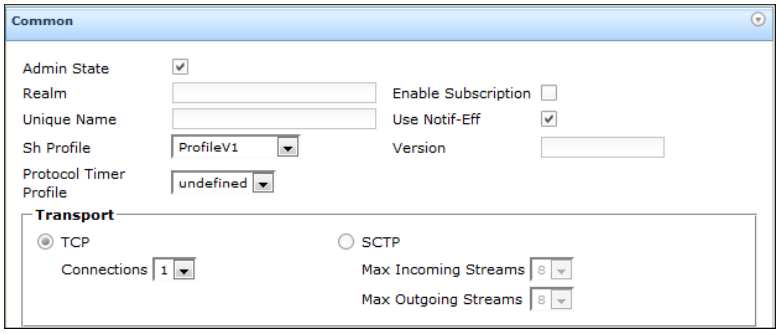
For an Sh data source, you can define two active primary connections and two standby backup connections. An incoming message can be handled from either active connection. You can subscribe through the MPE device (via the Sh interface) to receive notifications on changes to the Quota and Entity State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

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

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

Server Info Tab

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



1. **Admin State** — Enable this data source.

   Selected by default.

2. **Realm** — Server realm; for example, **`galactel.com`**

   - **Enable Subscription** — Allow the MPE device to receive subscription notifications as changes are implemented to the Quota and Entity state. This function manages dynamic profile changes. The data is returned in one XML response. If this option is disabled, separate lookups are used.

3. **Unique Name** — Provide the MPE device with a specific name for organizational purposes.

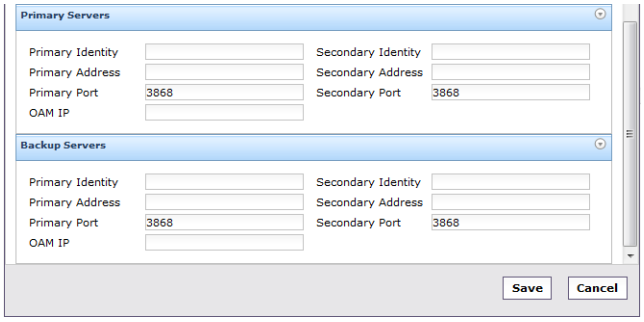
   - **Use Notif-Eff** — Enable reads of multiple user data blocks (subscriber, quota, and entity state).

4. **Sh Profile**:

   - **ProfileV1** (default) — third-party HSS
   - **ProfileV2** — HSS/Sh (7.5 or earlier version)
   - **ProfileV3** — SPR (8.0 or later version)
   - **ProfileV4** — Oracle Communications User Data Repository-Base
   - **ProfileV1 MDF** — MDF data source.

5. **Version**— If Sh data source is SDM, the value is 9.x. If Sh data source is UDR, value is 10.x.
6. **Protocol Timer Profile** — Select a protocol timer profile. For information on creating Protocol Timers, see *Managing Protocol Timer Profiles*.
7. **Transport** — Provides the transport mode for the MPE device.

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

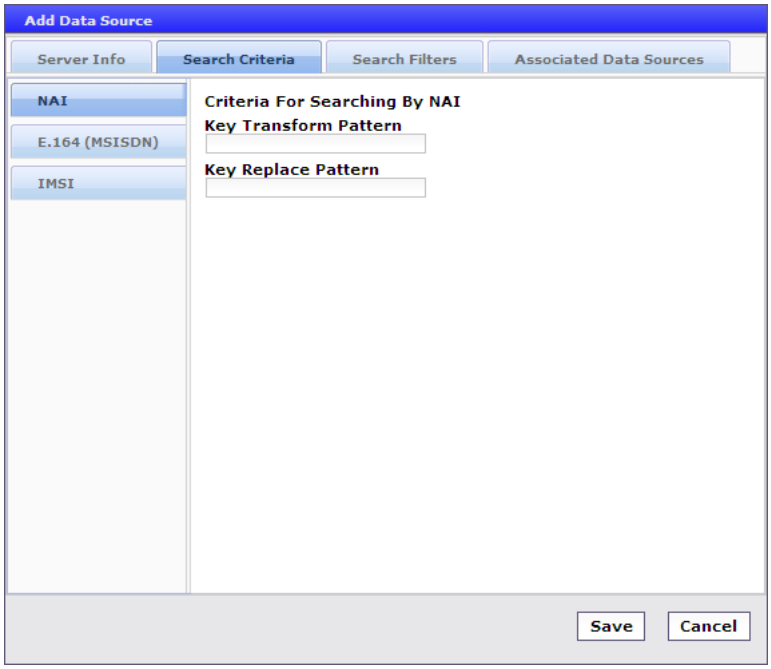


8. **Primary Servers**:
   a) **Primary Identity** — Primary server host name.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary server.
   c) **Primary Port** — Primary server port number.
      The default port number is 3868.
   d) **Secondary Identity** — Secondary server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

The Sh data source is configured.

Search Criteria Tab

Define the search criteria by entering the following:



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

   For example, **`17$2`** means the new string starts with 17 and is followed by the group 2 ($2) pattern.
5. When you finish, click **Save**.

Search Filters Tab

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

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

1. **Key Type** — Select from the list:
   - **NAI** — Network address ID
   - **E.164 (MSISDN)** — E.164 phone number
   - **IMSI** (the default) — International Mobile Subscriber Identity
2. **Expression** — Enter a regular expression. For example:
   - **`508.*`** — Matches numbers beginning with `508`

- `*@galactel.com` — Matches strings ending with `@galactel.com`
- `.*` — Matches any input string

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

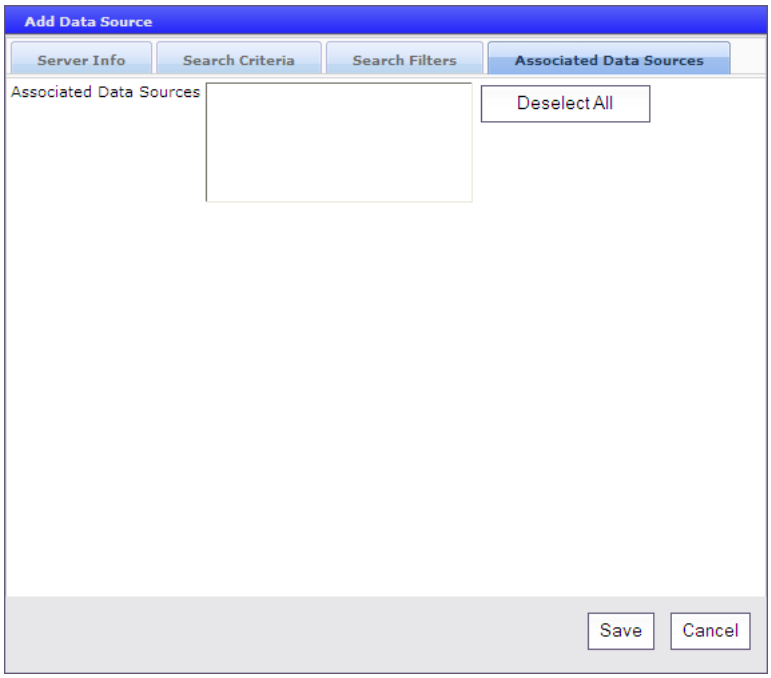
3. When you finish, click **Save**.

The Sh data source filters are defined.

Associated Data Sources Tab

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

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



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

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

2. When you finish, click **Save**.

The associated data sources are defined.

Configuring an Sy Data Source

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

The Sy interface is session stateful—a session is normally established when the Gx session for the first PDN is established for a subscriber. A Diameter Subscription for Notification Request (SLR) message causes a subscription to be registered until it is explicitly canceled or the Sy session is lost. A policy counter read is included with the SLR message. The subscriber's profile indicates whether the subscriber requires the use of policy counters. The MPE device reads a subscriber's policy counters when the subscriber's first session is established, and caches the profile until the subscriber's last session is terminated. If the MPE device receives a Policy Counter Change Notification (SNR) message, the cached policy counters are updated, and policies for all sessions using the policy counters are re-evaluated.

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

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

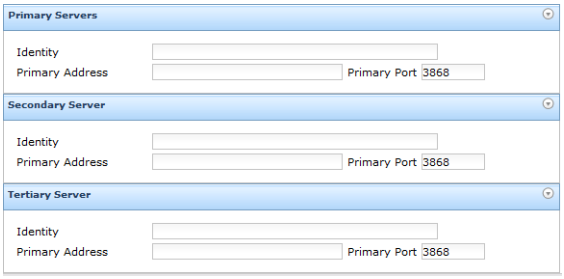
Server Info Tab

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

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

      Indicates whether the Sy data sources support the SCTP protocol. If checked, an MPE device can communicate with the Sy data sources using SCTP. The default is to use the TCP protocol.
   g) Select the number of **Connections** for either transport protocol.

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



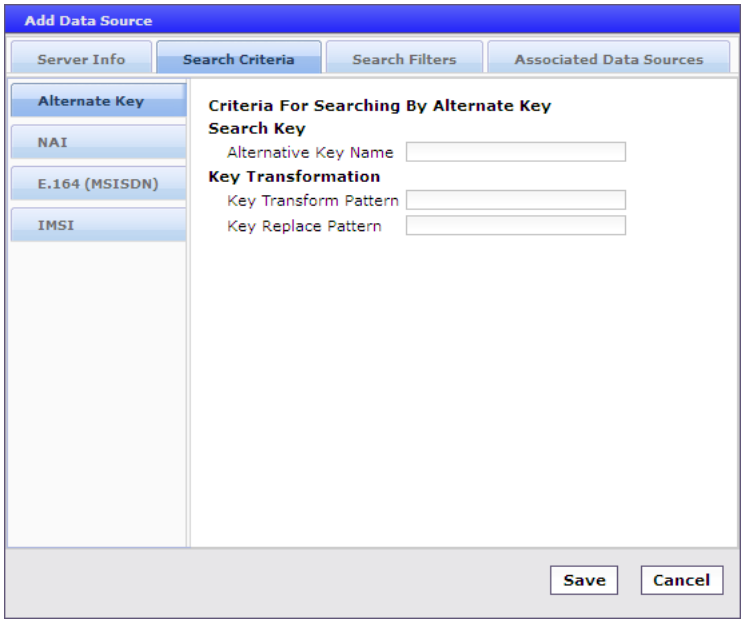
a) **Identity** (required) — Fully qualified domain name (FQDN) of the primary server.
b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary server. If omitted, the primary identity is used to look up the server address.
c) **Primary Port** — Primary server port number. The default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

3. **Secondary Server**:
   a) **Identity** — FQDN of the secondary server.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the backup server. If omitted, the secondary server primary identity is used to look up the server address.
   c) **Primary Port** — Secondary server port number. The default port number is 3868.
4. **Tertiary Server**:
   a) **Identity** — FQDN of the tertiary server.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the tertiary server. If omitted, the tertiary server primary identity is used to look up the server address.
   c) **Primary Port** — Backup server port number. The default port number is 3868.
5. When you finish, click **Save**.

The Sy data source is configured.

Search Criteria Tab

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



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

   For example, **`17$2`** means the new string starts with 17 and is followed by the group 2 ($2) pattern.
4. When you finish, click **Save**.

You have defined the search criteria.

Search Filters Tab

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

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

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

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

The Sy data source filters are defined.

Associated Data Sources Tab

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

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

To associate a data source:

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

   Note: Select **Deselect All** if you want to deselect your choices.
3. When you finish, click **Save**.

The associated data sources are defined.

Working with Policy Server Groups

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

Creating a Policy Server Group

To create a policy server group:

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

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; use Ctrl or Shift-Ctrl to select multiple policy servers.
5. When you finish, click **Save**.

The policy server is added to the selected group.

Creating a Policy Server Sub-group

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

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

5. When you finish, click **Save**.

The sub-group is added to the selected group.

Renaming a Policy Server Group

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

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

   The name cannot contain quotation marks (") or commas (,).
5. When you finish, click **Save**.

The group is renamed.

Removing a Policy Server Profile from a Policy Server Group

Removing a policy server profile from a policy server group or sub-group does not delete the profile. To delete a policy server profile, see *Deleting a Policy Server Profile*.

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

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

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

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

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

Deleting a Policy Server Group

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

To delete a policy server group or subgroup:

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

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

2. From the content tree, select the policy server group or sub-group.
   The **Policy Server Administration** page opens in the work area, displaying the contents of the selected policy server group or sub-group.
3. On the **Policy Server Administration** page, click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the group.

The policy group is deleted.

Reapplying the Configuration to Policy Management Devices

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

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

To reapply the configuration associated with an MPE device:

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

   The content tree displays a list of Policy Management device groups; the initial group is **ALL**.
2. To reapply the configuration to a single device continue with the next step.
3. From the content tree, select the **ALL** group.
   The **Policy Server Administration** page opens in the work area.
4. From the group **ALL**, select the MPE device.
   The **Policy Server Administration** page opens to the **System** tab, displaying information for that device.
5. Click **Reapply Configuration**.
   The profile information is saved to the MPE device.

6. From the content tree, select the group.
   The appropriate **Administration** page opens in the work area.
7. From the **Operations** menu, select **Reapply Config**.
   The **Bulk Reapply Config** dialog displays stating the number of servers affected.
8. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.
9. Click **Reapply Config** to reapply the configuration.

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

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

Resetting Counters

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

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

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

The counters are reset.

Enabling or Disabling All Sh Connections

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

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

To manually disable or enable all Sh connections:

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

4. Specify the delay time for applying the operation to each server. The number of seconds is 0 to 60. 0 is the default.
5. Click **Enable Sh** or **Disable Sh** to perform the action.

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

Checking the Status of an MPE Server

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

Group View

Select **ALL** from the policy server content tree to view all the defined MPE servers, or select a specific policy server group or sub-group to view just the servers associated with that group. The display in the work area includes a status column that indicates the following states:

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

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

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

Policy Server Profile View

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

Figure 11: Group View shows an example of a Group View in which one of the servers is degraded.

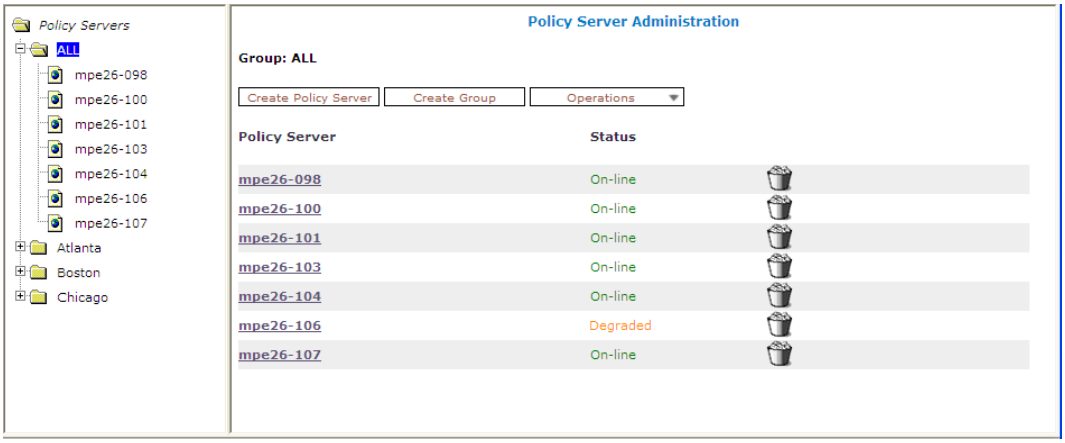


Figure 11: Group View

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

Managing Sessions

Managing Sessions describes how to 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.

Viewing Sessions

To view a session:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **All**.
2. Select the Policy Management device managing the session you are interested in.
   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, select the **Session Viewer** tab.
   The Session Viewer tab opens.
4. Enter search information as follows:
   a) **Identifier type** (required) — Select **NAI** (the default), **E.164(MSISDN)**, **IMSI**, **IPv4Address**, or **IPv6Address** from the pulldown list.

      The identifier types you can specify are determined by the configuration of the Policy Management device. For example, if the IndexByNAI setting is not specified on the device, then you cannot select **NAI**.

   b) **Identifier name** — Free-form text.

      Enter up to 250 characters.
5. Click **Search**.

If sessions are available for the subscriber, subscriber session data is displayed. *Figure 12: Session Viewer Page* shows an example.

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 device, you can click on the identifier to view session data from the MPE device.

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.

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 (?).

If the KT mode is not enabled, you can click **Delete Session** to delete the session. If the KT mode is enabled, then for each Gx session, you can click **Terminate Session** to terminate the session. Clicking **Terminate Session** causes the CMP system to send an event to the MPE device to trigger session termination. The **Delete Session** button is hidden for non-Gx sessions.

CAUTION

Caution: You should only delete or terminate obsolete sessions. If you delete or terminate an active session, then there is no signal to any associated gateways or external network elements.

The Session Viewer page displays subscriber profiles that defined in the KT-Sp SPR. The page is formatted to display the data in the following groups:

- Gx sessions
- AF session
- Subscriber profile

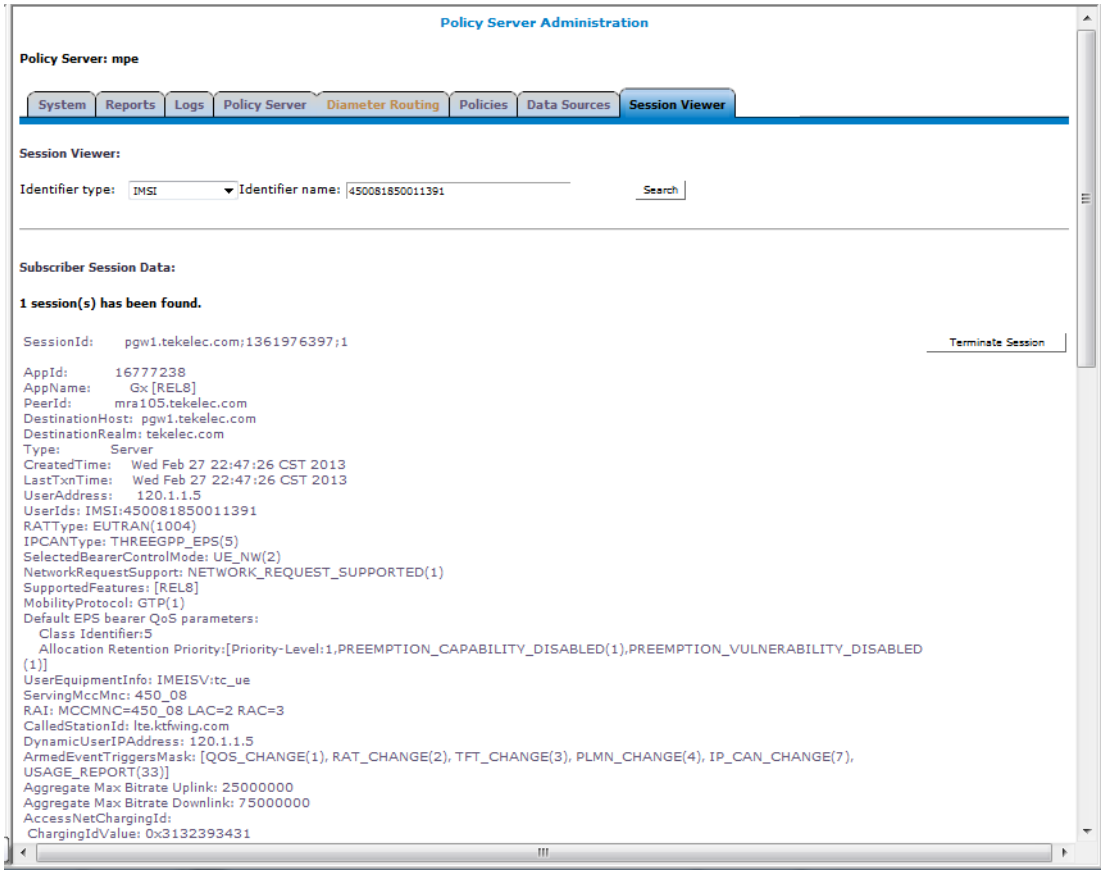


Figure 12: Session Viewer Page

Policy Server Reports

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

Report pages provide the following information:

Mode Shows whether data collection is currently Active or Paused, Absolute (displaying statistics since the last reset) or Delta (displaying changes in the statistics during the last 10-second refresh period).

Buttons The buttons let you navigate between reports, or control the information displayed within the report. The following list describes the buttons; which buttons are available depend on your configuration and differ from one report page to the next:

Show Absolute/Show Deltas	Switches between absolute mode (statistics since last reset) and delta mode (statistics since last display).
Reset Counters/Reset All Counters	Resets counters on the current page, or all counters under Policy Statistics and Protocol Statistics, back to initial values (except for Session count and Downstream Bandwidth in the Network Elements) section.

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

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

Cluster	Information about the cluster.
Blades	Information about the individual physical components in the cluster.
Time Period	Information about the current time period and transition status.
Policy Statistics	Information about the execution of policy rules.
Quota Profile Statistics	Information about quota profiles.
Traffic Profile Statistics	Information about traffic profiles.
Session Cleanup Statistics	Information about removal of stranded subscriber sessions.
Protocol Statistics	Information about the active network protocols.
Latency Statistics	Information about protocol latency.
Event Trigger Statistics	Information about triggered events.
Error Statistics	Information about any errors, arranged by protocol.
Data Source Statistics	Information about LDAP, Sh, Sy, and SPR activity.
KPI Interval Statistics	Information about the configured reporting interval for key performance indicator (KPI) statistics.

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

Cluster Information Report

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

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

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

- **Overall** — Displays the current topology state (Active, Standby, Forced-Standby, or Spare), number of server (blade) failures, and total uptime (time providing active or standby policy or GUI service). For the definitions of these states, see *Server Status*.
- **Utilization** — Displays the percentage utilization of disk (of the /var/camiant filesystem), average value for the CPU utilization, and memory.

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

Time Period

The Time Period section shows the current time period for the cluster (none 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 finishing.
Maximum Execution time (ms)	The longest execution duration of the policy.

Average Execution time (ms)	The average of all execution durations of the policy.
Processing Time Statistics	The number of policies processed per time range, in milliseconds. Ranges include 0-20, 20-40, 40-60, 60-80, 80-100, 100-150, 150-200, 200-250, and >250.

Quota Profile Statistics

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

The following statistics are included:

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

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

Traffic Profile Statistics

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

The following statistics are included:

- **Name** — Name of the traffic profile.
- **Install Attempts** — Number of times the MPE device attempted to install the traffic profile.
- **Removed by PCRF** — Number of times the MPE device removed a traffic profile.
- **Failed or Removed by Gateway** — Number of times the traffic profile failed or was removed by a gateway.

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

Session Cleanup Statistics

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

For information on configuring session cleanup, see *Configuring Expert Settings*.

The following statistics are included:

- **Ready for Cleanup** — Number of sessions that are stale.
- **Removed on unknown session id** — Number of sessions removed because the session ID is no longer valid.

- **Reauthorized** — Number of sessions reauthorized.
- **Reauthorization Timeout** — Number of sessions for which the reauthorization request timed out.
- **Removed for Expiration** — Number of sessions removed.

Protocol Statistics

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

The summary protocol statistics are the following:

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

Figure 13: Sample Protocol Statistics shows a sample.

Protocol Statistics

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

Figure 13: Sample Protocol Statistics

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

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

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

Note:

1. Statistical information is returned from the MPE device as a series of running peg counts. To arrive at interval rate information, such as session success and failure counts, two intervals are needed to perform the difference calculation. Also, statistical information, such as session activation counts,

is kept in memory and is therefore not persisted across the cluster. After a failover, non-persistent metrics must be repopulated based on a sampling from the newly active primary server. Therefore, when an MPE device is brought on line, or after a failover, one or more sample periods will display no statistical information.

2. Historical network element statistical data is inaccurate if configuration values (such as capacity) were changed in the interim. If the network element was renamed in the interim, no historical data is returned.

For example, the DRMA statistics are the following:

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

Latency Statistics

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

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

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

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

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

Event Trigger Statistics

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

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

Error Statistics

The Error Statistics section summarizes any protocol-related errors reported by the MPE device. This is presented as a table of overall statistics for each protocol that is configured for the MPE device. *Figure 14: Sample Error Statistics* shows a sample.

Error Statistics

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

Figure 14: Sample Error Statistics

The following summary statistics are displayed:

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

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

Data Source Statistics

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

LDAP Statistics

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

- **Number of successful searches**
- **Number of unsuccessful searches**

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

Sh Statistics

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

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

- **Average time spent on successful subscriptions (ms)**
- **Average time spent on unsuccessful subscriptions (ms)**
- **Number of successful unsubscriptions**
- **Number of unsuccessful unsubscriptions**
- **Number of unsubscriptions that failed because of errors**
- **Number of unsubscription errors that triggered the retry**

Sy Statistics

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

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

SPR Statistics

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

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

- **Average time spent on unsuccessful subscriptions (ms)**

Database Statistics

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

KPI Interval Statistics

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

The following interval statistics are displayed:

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

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

Pause/Resume	Stops or restarts automatic refreshing of displayed information.
Cancel	Returns to the previous page.

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

Policy Server Logs

The log files trace the activity of a Policy Management device. You can view and configure the logs for an individual cluster.

To view the log:

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

   Log information, including the log levels, is displayed. Refer to example for *Figure 15: Policy Server Administration, Logs Tab — Wireless*. You can configure the following logs:

   - **Trace log** — Records application-level notifications.
   - **Policy Log Settings** — Records the policy-level messages.
   - **Policy Syslog** — Records policy-processing activity. Supports the standard UNIX logging system, in conformance with RFC 3164.
   - **SMPP log** — Contains all Short Message Peer-to-Peer Protocol (SMPP) notification sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server.
   - **SMTP log** — Contains all Simple Mail Transfer Protocol (SMTP) messages sent by the MPE device.

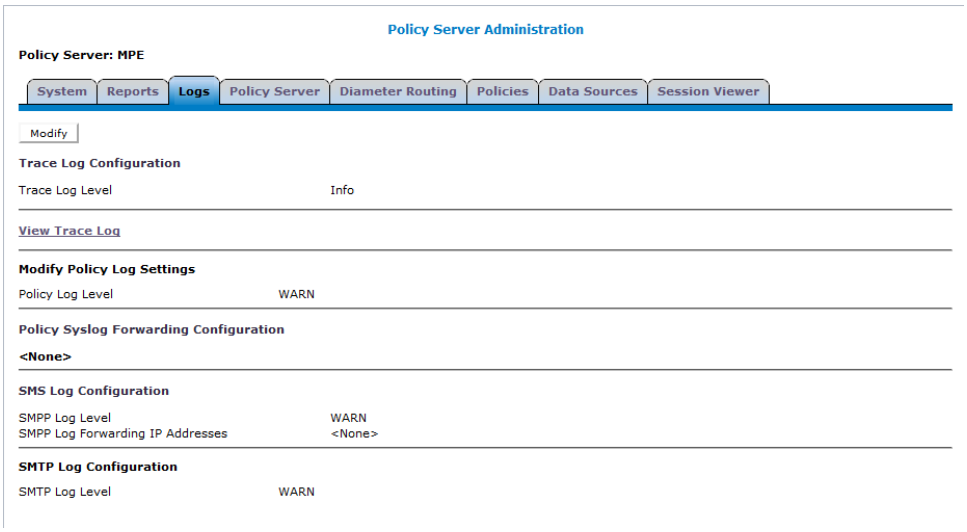


Figure 15: Policy Server Administration, Logs Tab — Wireless

Viewing the Trace Log

The trace log records Policy Management application notifications, such as protocol messages, policy messages, and custom messages generated by policy actions, for individual servers. Trace logs are not replicated between servers in a cluster, but they persist after failovers. You can use the log to debug

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

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

To view log information using the Trace Log Viewer:

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

   The content tree displays a list of groups; the initial group is **ALL**.
2. From the content tree, select the device.
   The appropriate **Administration** page opens in the work area.
3. On the **Administration** page, select the **Logs** tab.
   Log information for the selected device is displayed.
4. Click **View Trace Log**.

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

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

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

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

By default, the window displays 25 events per page. You can change this to 50, 75, or 100 events per page by selecting a value from the **Display results per page** pulldown list.

Events that occur after the Trace Log Viewer starts are not visible until you refresh the display. To refresh the display, click any of the following:

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

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

Failure Log Lookup

The MRA trace log can be used to locate failed Diameter response messages (any response message that does not have a result code of 2001 (DIAMETER_SUCCESS)) for a particular session.

To use the MRA trace log to locate failed Diameter response messages:

1. Open the trace log for the MRA of interest. See *Viewing the Trace Log* for more information on trace logs.
2. Search the MRA trace log by entering the subscriber IMSI or MSISDN in the **Contains** field and clicking **Search**.
   This search provides a list of associated session IDs.
3. Search the MRA trace log a second time by entering the session ID of interest in the **Contains** field and clicking **Search**.
   This search provides all request and response messages, including failed messages, for the session.

Syslog Support

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

Note: This feature is separate from TPD syslog support.

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

The SMPP Log

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

The SMTP Log

The SMTP log contains all Simple Mail Transfer Protocol (SMTP) messages sent by the MPE device, as well as any ACK messages received from a Mail Transfer Agent (MTA). In SMPP or XML mode, SMTP log info appears on the **Logs** tab of the **Policy Server Administration** page, under the **Policy Server: Configuration: MPE** menu. Using the **Modify** button, you can configure the severity of messages that are written to the SMTP log.

Configuring Log Settings

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

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

   This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:

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

   CAUTION

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

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

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

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

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

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

   CAUTION

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

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

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

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

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

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

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

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

   Valid levels are:

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

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

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

   This setting indicates the minimum severity of messages that are recorded in the SMTP log. These severity levels correspond to the syslog message severities from RFC 3164. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the SMTP log. The levels are:

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

7. When you finish, click **Save**.

The log configurations are changed.

Analytics Data Stream

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

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

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

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

The ADS feature is configured from the **Mode Settings** page. See *CMP Modes* for information on configuring the ADS feature.

CAUTION

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

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

Chapter 5

Configuring Protocol Routing

Topics:

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

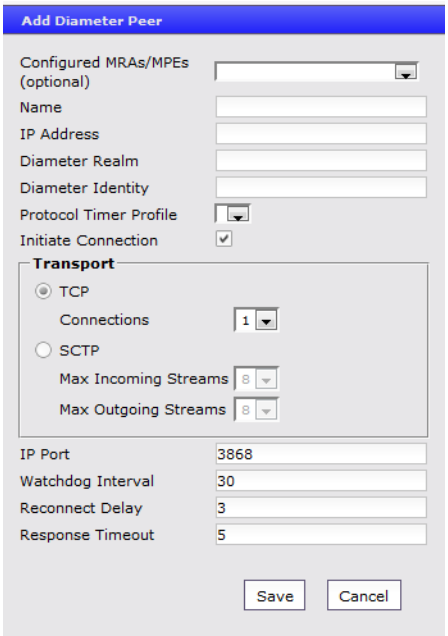
- Diameter applications: Rx, Gq, Ty, Gxx, Gx, Gy, and Sd

Configuring Diameter Peers

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

To configure Diameter peers:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups.
2. From the content tree, select the MPE device.
   The **Policy Server Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Peers**.
   The **Modify the Diameter Peer Table** page opens.
5. Add a peer to the table.
   a) Click **Add**. The **Add Diameter Peer** window opens.



   b) Enter the following:

   - **Configured MRAs/MPEs (optional)** — If you are defining an existing Policy Management cluster as a Diameter peer, select it from this list; the other fields are populated.
   - **Name** (required) — Name of the peer device (which must be unique within the CMP database).
   - **IP Address** (required) — IP address in IPv4 or IPv6 format of the peer device.

If not specified, the MPE device uses a DNS lookup to resolve the value in the Diameter Identity field into an IP address and try to connect.

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

c) When you finish, click **Save**.

6. Add, edit or delete additional Diameter Peers.
   - Cloning an entry in the table
     1. Select an entry in the table.
     2. Click **Clone**. The **Clone** window opens with the information for the entry.
     3. Make changes as required.
     4. When you finish, 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. When you finish, click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     1. Select the entry in the table.
     2. Click **Delete**. A confirmation message displays.
     3. Click **Delete** to remove the entry. The entry is removed from the table.
7. When you finish, click **Save**.

You have defined a Diameter peer.

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.

To configure the Diameter route table:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups.
2. From the content tree, select the policy server.
   The **Policy Server Administration** page opens in the work area.
3. Select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Routes**.
   The **Modify the Diameter Route Table** page opens.
5. Add a route to the table
   a) Click **Add**.
      the **Add Diameter Route** window opens.
   b) Configure the route using the following fields.
      - **Diameter Realm** — For example, `galactel.com`.
      - **Application ID** — Select **Rx** (the default), **Gq**, **Ty**, **Gx**, **Gy**, **Gxx**, or **All**.

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

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

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

   c) When you finish, click **Save**.
6. (Optional) 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. When you finish, 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. When you finish, click **Save**. The entry is updated in the table.

- Deleting a value from the table
  1. Select the entry in the table.
  2. Click **Delete**. A confirmation message displays.
  3. Click **Delete** to remove the entry. The entry is removed from the table.
- Ordering the list.

  If you define multiple entries, they are searched in the order displayed in this list. To change the order:
  1. Select an entry.
  2. Click **Up** or **Down**. The search order is changed.

7. Define the default route:
   a) Click **Edit** in the **Default Route** section.
   b) Select the default action: **PROXY**, **RELAY**, or **LOCAL**.
   c) Select the peer server ID.
   d) When you finish, click **Save**.
8. To delete the default route, click **Delete**.
9. When you finish, click **Save**.

The Diameter routes are configured.

Chapter 6

Configuring Advanced Device Settings

Topics:

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

Configuring Expert Settings

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

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

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

   The configuration settings for the device display.
3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Modify**.
   The advanced configuration settings can be edited.
5. Select a configuration key in the **Expert Settings** table and click **Edit**.
   The **Edit Expert Setting Value** dialog opens.
6. Modify the settings and click **OK** to save.

   See *Table 18: Expert Settings for MPE* and *Table 19: Expert Settings for MRA* for information about the configurations keys.

Table 18: Expert Settings for MPE

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

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

Category	Configuration Key	Description	Default
		sessions database. Valid range is 1-100000.	
Diameter	DIAMETER.Cleanup. MaxSySessionValidityTime	The maximum amount of time in seconds after which the Sy session is cleaned up on any error. Valid range is 1-8640000.	172800 (2 days)
Diameter	DIAMETER.Cleanup.OverrideCleanupAudit	This specifies if the regular audit processing for cleaning up a stale session is overridden. When enabled, the cleanup task bypasses the audit process and deletes all sessions that are stale for the session validity time.	False
Diameter	DIAMETER.Cleanup.RXSessionValidityTime	The amount of time in seconds after which the session is expired and is purged if EnabledAFSessionCleanup is enabled.	86400 (1 day)
Diameter	DIAMETER.Cleanup.SessionCleanupInterval	The amount of time in seconds after which the cleanup task will run to look for stale sessions.	21600 (5 hours)
Diameter	DIAMETER.Cleanup.SessionCleanupStartTime	Schedules the cleanup task once a day at a specified time. If the start time is specified, then it is scheduled to run once a day at the given time. The value can be specified in either a 24-hr format (*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	DIAMETER.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Valid range is 1- 8640000.	432000 (5 days)
Diameter	DIAMETER.Cleanup.SySessionValidityTime	The amount of time in seconds after which the session is declared stale and deemed a candidate for cleanup.	36000 (10 hours)
Diameter	DIAMETER.EnableSessionCleanUp	Enables the DiameterSessionCleanUp Task.	True
Diameter	DIAMETER.ENF.Forward.SPRBusyResultMapping	When the MPE device receives result codes defined in this configuration, this result code is forwarded to the ENF as DIAMETER_TOO_BUSY. This configuration can contain multiple values delimited by a comma. This configuration is valid when the setting Forward_SPR_TOO_BUSY is true.	3004

Category	Configuration Key	Description	Default
Diameter	DIAMETER.ENF.Forward_SPR_TOO_BUSY	The forwarding of the busy state of the SPR device to the ENF. This value is used in conjunction with the DIAMETERDRA.ENF.Forward_SPR_TOO_BUSY on MRA device and must contain the same value.	False
Diameter	DIAMETER.ENF.TranslatedSPRBusyCode	The MPE sends the DIAMETER_SPR_TOO_BUSY to the MRA device when forwarding an SPR too busy state in a CCA message. The value of DIAMETER_SPR_TOO_BUSY is configurable. The format of the value is: `VendorId:Code` The default value is pre-defined. This value is used in conjunction with DIAMETERDRA.ENF.TranslatedSPRBusyCode on the MRA device and must contain the same value.	10415:5149
PCMM	PCMM.Cleanup.CleanupStalePcmmSessions	Enables the inclusion of PCMM sessions in regular cleanup cycles. If enabled, PCMM sessions are considered expired if they have lived longer than the specified PcmmSessionValidityTime or license timeout duration configured in the application.	
PCMM	PCMM.Cleanup.PcmmSessionValidityTime	The amount of time in seconds after which the session is deemed expired and is purged if the setting EnabledAFSessionCleanup is enabled.	86400 (1 day)

Table 19: Expert Settings for MRA

Category	Configuration Key	Description	Default
Admission	ADMISSION.DIAMETER.RequestProcessingLimit	The maximum amount of time in milliseconds a request can be processed before being dropped, if no answer has been sent.	5000
Diameter	DIAMETERDRA.Cleanup.BindingCleanupInterval	The interval in seconds at which the cleanup task that looks for stale bindings occurs. Valid range is 1-8640000.	86400 (1 day)
Diameter	DIAMETERDRA.Cleanup.BindingValidityTime	The amount of time in seconds elapsed until a binding is deemed stale. Valid range is 1-8640000.	864000 (10 days)

Category	Configuration Key	Description	Default
Diameter	DIAMETERDRA.Cleanup.CheckForStaleBindings	Check for stale bindings during the cleanup cycle, which is determined by the current time being greater than the DIAMETERDRA.Cleanup. BindingValidityTime. If this is set to false, the cleanup task will not check if the entire binding is stale.	False
Diameter	DIAMETERDRA.Cleanup. CheckForStaleSessionsInBinding	Check for stale sessions in binding determined by the current time being greater than the SessionValidityTime. If this is disabled, the cleanup task checks the entire binding only.	True
Diameter	DIAMETERDRA.Cleanup.CheckForSuspectBindings	Check for suspect bindings during the cleanup cycle. If this is set to false, the cleanup task checks that an entire binding is stale.	True
Diameter	DIAMETERDRA.Cleanup.CleanupStartTime	Schedules the cleanup task once a day at a specified time. If a time is specified, then it is scheduled to run once a day at the given time. The value can be specified in either a 24-hr format (*HH*:*mm*) or an exact date and time (*YYYY-MM-dd*Thh:*mm*:*ss*) of when it will first run and then repeat at the interval specified.	
Diameter	DIAMETERDRA.Cleanup.MaxBindingCleanupRate	The rate (in bindings/sec) at which the cleanup task attempts to clean stale bindings. Valid range is 1-40000.	250
Diameter	DIAMETERDRA.Cleanup.MaxBindingIterationRate	The rate (in bindings/sec) at which the cleanup task iterates through the binding database. Valid range is 1-100000.	1000
Diameter	DIAMETERDRA.Cleanup. MaxDurationForBindingIteration	The maximum duration in seconds to iterate through the bindings. Valid range is 1-2147483647.	21600 (5 hours)
Diameter	DIAMETERDRA.Cleanup.MaxSessionValidityTime	The maximum amount of time in seconds after which the session is cleaned up on any error. Valid range is 1-8640000.	864000 (10 days)
Diameter	DIAMETERDRA.Cleanup.SessionValidityTime	The amount of time in seconds after which a session in a binding is declared stale. Valid range is 1-8640000.	432000 (5 days)
Diameter	DIAMETERDRA.StaticMigrationModeEnabled	Enables the static to stateful MRA migration mode. While in this mode,	False

Category	Configuration Key	Description	Default
		static routes are used for MPE selection only.	
Diameter	DIAMETERDRA.ENF.Forward_SPR_TOO_BUSY	The forwarding of the busy state of the SPR to the ENF. This value is used in conjunction with the setting DIAMETER.ENF.forward_SPR_TOO_BUSY on the MPE device and must contain the same value.	False
Diameter	DIAMETERDRA.ENF.TranslatedSPRBusyCode	The MPE device sends the message DIAMETER_SPR_TOO_BUSY to the MRA device when forwarding an SPR too busy state in a CCA message. The value of DIAMETER_SPR_TOO_BUSY is configurable. The format of the value is: `VendorId:Code` The default value is pre-defined. This value is used in conjunction with the setting DIAMETER.ENF.TranslatedSPRBusyCode on the MPE device and must contain the same value.	10415:5149

7. When you finish, click **Save**.

The settings are applied to the selected device.

Configuring Service Overrides

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

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

Make service override changes as follows:

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

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

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

The configuration settings for the device display.

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

        CAUTION

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

     2. Enter the following values:
        - **Configuration Key** — The attribute to set
        - **Value** — The attribute value (up to 255 characters)
        - **Comments** — Information about the key.
     3. When you finish, click **OK**. The key is displayed in the table with its defined and default values.
   - Cloning a key in the table:
     1. Select an existing key in the table.
     2. Click **Clone**. The **Clone Configuration Key Value** window opens with the information for the key.
     3. Make changes as required.
     4. When you finish, click **Save**.
   - Editing a key in the table:
     1. Select an existing key in the table.
     2. Click **Edit**. The **Edit Configuration Key Value** window opens with the information for the key.
     3. Make changes as required.
     4. When you finish, click **Save**.
   - Deleting a key from the table:
     1. Select an existing key in the table.
     2. Click **Delete**. You are prompted with a confirmation message.
     3. Click **Delete** to remove the key.
6. When you finish, click **Save**.

The settings are applied to the selected device.

Configuring Load Shedding Rules

You can configure load shedding rules to determine how an device reacts to a processing backlog. This state is called "busyness." By default there are three levels of busyness, from Level 1, the least busy, to Level 3, the most busy. With each successive level, the device becomes more aggressive in rejecting or discarding messages in an attempt to prevent the main queue from become full. At any level of busyness, requests that have been queued longer than a configurable time are silently discarded without further processing, since the originator would have already given up on that request. The following table shows the default load-shedding rules for an device.

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

Table 20: Default Device Busyness Level 2

Rule Name	Actions
DefaultRule7	Reject Rx AAR-I messages with DIAMETER_TOO_BUSY

Table 21: Default Device Busyness Level 3

Rule Name	Actions
DefaultRule11	Reject Rx AAR-I messages with DIAMETER_TOO_BUSY

Use the **Load Shedding Configuration** section of the **Advanced Configuration** page to edit, reorder, or add new rules at each of the three levels of busyness for a device based on the amount of backlog. To reach a configured level of busyness:

- The backlog of outstanding messages in a node crosses a pre-defined threshold for the level.
- The backlog has been above the busyness level threshold for a minimum amount of time.

At each level, the device can be configured to take one of the following actions (referred to as rules) until the busyness level clears:

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

Note: Configuration keys must also be used in configuring load shedding options. Contact MOS for assistance.

Configure the load shedding rules as follows:

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

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

The configuration settings for the device display.

3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Modify**.
   The advanced configuration settings can be edited.
5. In the **Load Shedding Configuration** section of the page, select the enabled state.
   - **true** (default)—Enables load shedding.
   - **false**—Disables load shedding.
   - **undefined**— The value for this field is taken from the associated Configuration Template. If there is not a configuration template associated, then the default value is used.
6. Configure the rules for the busyness levels:
   a) Click ▶ (right arrow) next to the level to expand the level.
   b) Click **Add** and select the category.
      The **Add Load Shedding Rule** dialog appears.
   c) Enter the values for the load shedding rule:
      - **Name** — Name of the rule.
      - **Application** — Select the application the rule applies to. You can select **Gx**, **Gy**, **Gxx**, **Rx**, **Sh**, or **Sy**.
      - **Message** — Type of message the rule applies to (which depends on the application chosen).
      - **Request Types** (available only when the CCR message type is selected) — Select the Request-Type attribute-value pairs (AVPs) that the message must contain. You can select **Initial**, **Update**, and/or **Terminate**.
      - **APNs** — Enter a CSV list of one or more access point names that the message must contain.
      - **Action** — Select the action to be taken if the criteria are met for the busyness level. You can select **Drop** (drop the message); **Answer With** (select a code from the drop-down list), or **Answer With Code** (enter a code) and **Vendor ID** (enter a vendor ID).
   d) Click **OK**.
      The rule is displayed in the table.
7. Once a rule is defined, you can clone, edit, or delete it by selecting the rule and clicking the appropriate button.
8. When you finish, click **Save**.

The settings are applied to the selected device.

Resetting Configuration Keys to Defaults

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

To reset the configuration keys in the Expert Settings table:

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

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

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

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

   The configuration settings for the device display.
3. Click **Advanced**.
   The advanced settings for the device display.
4. Click **Modify**.
   The advanced configuration settings can be edited.
5. Click **Set to Default**.
   A confirmation message displays.
6. Click **OK**.

All the configuration keys for Expert Settings are set to default values.

Filtering the Configuration Keys

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

To filter the configuration key table:

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

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

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

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

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

Exporting the Configuration Keys

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

To export the configuration key table:

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

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

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

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

Chapter 7

Managing Protocol Timer Profiles

Topics:

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

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

About Protocol Timer Profiles

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

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

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

Table 22: Supported Diameter Applications and Messages lists the Diameter applications and message types supported.

Table 22: Supported Diameter Applications and Messages

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

Viewing a Protocol Timer Profile

To view a Protocol Timer Profile:

1. From the **Policy Server** section of the navigation pane, select **Protocol Timer Profiles**.
   The content tree displays the **Protocol Timer Profiles** folder.
2. Select a profile.
   The configuration for the profile displays in the Work Area.
3. Change the view of the list using the following options:
   - When the list is expanded, click **Collapse All** to show the list of applications/interfaces only.
   - When the list is collapsed, click ▶ (right arrow) to the left of the interface/application to view the settings for an individual application/interface.
   - When the list is collapsed, click **Expand All** to show list of settings for all the applications/interfaces.
   - When the list is expanded, click ▼ (down arrow) to the left of the interface/application to close the settings view for an individual application/interface.

The Protocol Timer Profile Timeout configuration displays by Application and Interface Message type. Timeout values are in milliseconds (msec).

Creating a Protocol Timer Profile

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

To create a Protocol Timer Profile:

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

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

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

Table 23: Supported Diameter Applications and Messages

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

4. When you finish, click **Save**.

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

Modifying a Protocol Timer Profile

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

To modify a Protocol Timer Profile:

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

   Note: The timeout value must be expressed in multiples of 100. For example, 4955 is not a valid value and displays a validation error.
6. When you finish, 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 (trash can). 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 updated.

Chapter 8

Managing Charging Servers

Topics:

Managing Charging Servers describes how to define and manage charging servers within the CMP system.

A charging server is an application that calculates billing charges.

About Charging Servers

A charging server is an application that calculates billing charges for a wireless subscriber. The CMP system supports both online and offline charging servers:

- An online charging server (OCS) calculates charges against a prepaid account for an event and returns information on how long the subscriber can use the service; it can affect, in real time, the service rendered.
- An offline charging server (OFCS) calculates charges for a service to an account, and does not affect (in real time) the service rendered.

Defining a Charging Server

To define a charging server:

1. From the navigation pane, select **Charging Servers**.
   The content tree displays the **Charging Servers** group.
2. Select the **Charging Servers** group.
   The **Charging Server Administration** page opens in the work area.
3. Click **Create Charging Server**.
   The **New Charging Server** page opens.
4. Enter information as appropriate for the charging server:
   a) **Name** (required) — The name you assign to the charging server.

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

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

      Enter up to 250 characters.

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

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

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

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

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

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

5. When you finish, click **Save**.

The charging server is displayed on the **Charging Server Administration** page.

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

Modifying a Charging Server

To modify the definition of a charging server:

1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.
   The **Charging Server Administration** page opens in the work area, listing the defined charging servers.
2. Select the charging server you want to modify.
   The **Charging Server Administration** page displays information about the charging server.
3. Click **Modify**.
   The **Modify Charging Server** page opens.
4. Modify charging server information as required.

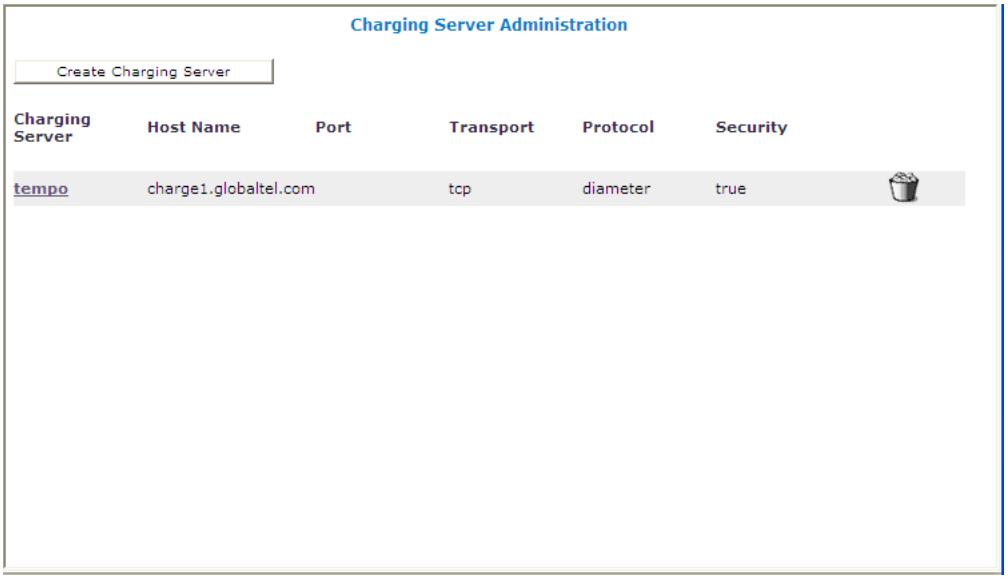
   For a description of the fields contained on this page, see *Defining a Charging Server*.
5. When you finish, click **Save**.

The charging server definition is modified.

Deleting a Charging Server

To delete a charging server:

1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.
   The **Charging Server Administration** page opens in the work area, listing the defined charging servers; for example:



2. Delete the charging server using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the charging server.
   - From the content tree, select the charging server and click **Delete**.

   A confirmation message displays.
3. Click **OK** to delete the charging server.

The charging server definition is removed from the list.

Associating a Charging Server with an MPE Device

To associate a charging server with an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the policy server.
   The **Policy Server Administration** page opens in the work area.
3. Select the **Policy Server** tab.
   The **Default Charging Servers** section of the page lists charging servers associated with this policy server.
4. Click **Modify**.
   The **Modify Policy Server** page opens.
5. In the **Default Charging Servers** section, select the Primary Online Server, the Primary Offline Server, the Secondary Online Server, and the Secondary Offline Server from the lists.
6. When you finish, click **Save**.

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. When you finish, click **Save**.

The charging methods are defined for this MPE device.

Chapter 9

Mapping Serving Gateways to MCCs/MNCs

Topics:

Mapping Serving Gateways to MCCs/MNCs 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

An SGSN (Serving GPRS Support Node) may not provide a GGSN (Gateway GPRS Support Node) with accurate or complete mobile country code (MCC) or mobile network code (MNC) information. If not, the GGSN cannot pass this information on to the PCRF (including an MPE device), reducing the PCRF's ability to detect specific roaming scenarios. The MCC/MNC mapping table provides a mechanism for the MPE device to convert an SGSN IP address (a value the GGSN can determine without SGSN input) to the proper MCC/MNC value. You can map multiple serving gateways to each MCC/MNC pair. Once the MCC/MNC values are determined, they can be used in policies to differentiate subscriber treatment based on the specific roaming scenario.

Creating a Mapping

To create a mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
   The content tree displays the **Serving Gateway/MCC-MNC Mappings** group.
2. Select the **Serving Gateway/MCC-MNC Mappings** group.
   The **Serving Gateway/MCC-MNC Mappings Administration** page opens in the work area, listing available mappings.
3. Click **Create Serving Gateway/MCC-MNC Mapping**.
   The **New Serving Gateway/MCC-MNC Mapping** page opens.
4. Enter the following information:
   a) **Name** (required) — The name assigned to the mapping.
      The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
   b) **Description** — A descriptive phrase.
   c) **MCC-MNC** (required) — The MCC-MNC pair, in the format *mccmnc*; for example, 310012 for Verizon Wireless in the United States.
   d) **Serving Gateway IP Address/Subnet** (required) — The IP address or subnet, in IPv4 or IPv6 format, of a serving gateway.
      - To add an address to the mapping list, enter it and click **Add**.
      - To remove one or more mappings from the list, select them and click **Delete**.
5. When you finish, 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 opens.
2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.
   The **Serving Gateway/MCC-MNC Mappings Administration** page opens, displaying the list of defined mappings.
3. Select the mapping you want to modify.
   Mapping information is displayed.
4. Click **Modify**.
   The **Modify Serving Gateway/MCC-MNC Mapping** page opens.
5. Modify mapping information as required.
   For a description of the fields contained on this page, see *Creating a Mapping*.
6. When you finish, click **Save**.

The mapping is modified.

Deleting a Mapping

To delete a serving gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
   The content tree opens.
2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.
   The **Serving Gateway/MCC-MNC Mappings Administration** page opens, displaying the list of defined mappings.
3. Delete the mapping using one of the following methods:
   - From the work area, click 🗑 (trash can icon), located to the right of the mapping you want to delete.
   - From the content tree, select the mapping and click **Delete**.

   A confirmation message displays.
4. Click **OK** to delete the Serving Gateway/MCC-MNC mapping.

The mapping is deleted.

Chapter 10

Call Clearance

Topics:

Call Clearance describes how to remove an MPE from a PCRF topology. The Call Clearance feature enables you to systematically terminate active Gx sessions in the MPE. You can query the process from the CMP. The **Status** column for the selected MPE(s) will show a status of **Idle** if the clean up process is successfully completed.

Note: There are situations where the sessions cannot be deleted after doing call clearance. If this occurs, the **Gx Sessions** and **Active Sessions** columns will not be zero (0), showing that all the sessions have not been cleaned up.

Removing an MPE Device Using Call Clearance

The **Route New Subscribers** option must not be selected in the **Add Diameter MPE Peer** screen. For more information, see the section about associating a diameter MPE peer with an MRA in the *Oracle Communications Front End User's Guide*.

To create a mapping:

1. From the **Policy Server** section of the navigation pane, select **Call Clearance**.
2. Select the **Sever(s)** that will be removing the Gx sessions from the MPE.
3. Click **Clean Up**.
4. Click **OK** at both prompts.

   Note: If the selected server is not correct, click **Cancel**.

When the status changes from Running to Idle, the process is complete. An audit log is generated for the event. For more information on audit logs, see the system administration section of the *CMP Wireless User's Guide*.

Chapter 11

Managing Subscriber Profile Repositories

Topics:

Managing Subscriber Profile Repositories describes how to define and manage an optional Subscriber Profile Repository (SPR) using the CMP system.

An SPR is a system for storing and managing subscriber-specific policy control data as defined in the 3GPP standard.

Note: For information on operating Oracle Communications Enhanced Subscriber Profile Repository devices, refer to the ESPRUDR documentation.

About Subscriber Profile Repositories

A Subscriber Profile Repository (SPR) is a system for storing and managing subscriber-specific policy control data as defined under the 3GPP standard.

An SPR can be deployed in environments where the MPE device needs access to a separate repository for subscriber data. The SPR acts as a centralized repository for this data so that multiple MPE devices can access and share the data. This data may include profile data (pre-provisioned information that describes the capabilities of each subscriber), quota data (information that represents the subscriber's use of managed resources), or other subscriber-specific data.

The following SPR systems can be used in the CMP system:

- The Oracle Communications Subscriber Database Management (SDM) product includes interfaces for provisioning subscriber information, as well as managing, changing, and accessing this information. These interfaces include an application programming interface (API) for XML provisioning of subscriber profile data, as well as an interactive user interface through the CMP system using a proprietary RESTful API interface.

  The SDM is built upon an existing software base and technology. It not only manages static provisioned subscriber data, but also dynamic intra- and inter-session data from MPE devices—for example, when it is critical to store inter-session quota data centrally so that it can be retrieved upon the next subscriber attachment, wherever that attachment occurs within the network. Intra-session data such as mappings from IP addresses to MSISDNs becomes important as well, especially when managing enforcement points such as DPI devices and optimization gateways where MSISDN/IMSI data is not available. With this the SDM provides both a storage and notification platform for policy operations, as well as a platform for operator provisioning.

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

- The Oracle Communications User Data Repository (UDR) is a highly-scalable, consolidated database back end for subscriber and profile data. UDR utilizes multiple application front ends with the database. UDR supports the Oracle Communications Enhanced Subscriber Profile Repository (ESPR) application, a function used for the storage and management of subscriber policy control and pool data. XML-REST and XML-SOAP interfaces are used by ESPR for creating, retrieving, modifying, and deleting subscriber and pool data.

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

- A customer specified SPR.

  See the SPR documentation for more information.

To use an SPR with CMP, 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

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

To reconfigure the CMP operating mode, complete the following:

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

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 before you can look up subscriber information from the CMP system.

To configure the CMP connection to an SPR database:

1. From the **SPR** section of the navigation pane, select **Configuration**.
   The **SPR Connection Configuration** page opens in the work area, displaying connection information.
2. On the **SPR Connection Configuration** page, click **Modify**.
   The **Configuration** page opens.
3. Enter information as appropriate for the SPR system:
   a) **SPR Operation Mode** (required) — Select from the 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. When you finish, click **Save**.
   The connection definition is added to the CMP database.

The SPR connection is configured.

Modifying the SPR Connection

To modify the SPR connection:

1. From the **SPR** section of the navigation pane, select **Configuration**.
   The **SPR Connection Configuration** page opens in the work area, displaying connection information.
2. 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. When you finish, click **Save**.

The SPR connection configuration is modified.

Finding a Subscriber Profile

Once you have defined SPR devices, you can search them for a subscriber profile.

To find a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select the **Data Source Primary Diameter Identity**.
   This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.
3. Select the **Key Type**:
   - **E.164 (MSISDN)** (default) — search by Mobile Station International Subscriber Directory Number. This is a number of up to 15 digits.
   - **IMSI** — search by International Mobile Subscriber Identity. This is a number of up to 15 digits.
   - **NAI** — search by Network Access Identifier.
   - **Pool ID** — search by quota pool identifier.
4. **Key String** — enter a search string in the format appropriate for the selected key type.

The string must match exactly; partial or wildcard searching is not supported.

5. Click **Search**.
   The **Subscriber Profile** page opens, displaying information about the subscriber.

   Note: If no matching subscriber profile is found, the page displays the message `No matching user is found`.

6. When you finish, click **Back to Search Page**.
   The **Subscriber Profile Administration** page opens.

Creating a Subscriber Profile

If an SPR database is configured to use the RESTful API interface, you can manually create a subscriber profile.

To create a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Click **Create Subscriber Profile**.
   The **New Subscriber Profile** page opens in the work area.
3. Enter the following information:
   a) Select the **Data Source Primary Diameter Identity**.
      You can select any SPR device configured for the Policy Management network.
   b) In the **Key Fields** section, enter one format:
      - **NAI** — Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters &*+0-9?a-z_A-Z{}!#$%'^/=`|~-, optionally separated by a period (.). A valid realm name consists of the characters 0-9a-zA-Z- separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
      - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
      - **IMSI** — International Mobile Subscriber Identity. Enter up to 15 Unicode digits.
   c) Optionally, in the **Subscriber Information** section, enter the following:
      - **Account ID** — Free-form string that can identify the account for the subscriber. You can enter up to 255 characters.
      - **Billing Day** — The day of the month on which the subscriber's associated quota is reset. If you enter 0 or leave this field blank, then the default global value configured for this MPE device is used instead.
      - **Tier** — The subscriber's tier. Enter a tier name defined in the CMP database; or, if you click **Manage**, a window opens from which you can select a tier name. In order to add a tier, you must enter the tier name prior to clicking **Manage**. See *Managing Subscribers* for information on managing tiers.
      - **Entitlements** — The subscriber's entitlement(s). Enter the entitlement name(s); or, if you click **Manage**, a window opens from which you can enter or select entitlement names defined in the CMP database. 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.

4. When you finish, click **Save**.

The subscriber profile is defined.

Modifying a Subscriber Profile

To modify a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click **Modify**.
   The **Subscriber Profile Administration** page opens.
4. Modify subscriber profile information as required.
   For a description of the fields contained on this page, see *Creating a Subscriber Profile*.
5. When you finish, 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. Find the subscriber profile you want to delete.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the subscriber profile.

The subscriber profile is deleted.

Viewing Subscriber Entity States

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

To view the entity states associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click the **State** tab.
   Entity state information is displayed.
4. When you finish, click **Back to Search Page**.

You have viewed the subscriber entity states.

Creating a Subscriber Entity State Property

To create a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **State** tab.
   Entity state information is displayed.
4. Click **Create**.
   The **Create Property** page opens.
5. Enter the following information:
   a) **Name** — The name assigned to the property.
      The name cannot be blank and must be unique within this list of properties.
   b) **Value** — The property value.
      The value cannot be blank.
6. Click **Save**.
   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. When you finish, click **Back to Search Page**.
   The page displays the message `Properties created successfully`.

The subscriber entity state property is defined.

Modifying a Subscriber Entity State Property

You can modify the value (but not the name) of a subscriber profile entity state property. To modify a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **State** tab.
   Entity state information is displayed.
4. In the list of entity state properties, click the property you want to modify.
   The **Modify Property** page opens.
5. Modify the property value as required.
   The value cannot be blank.
6. When you finish, click **Save**.

The subscriber entity state property value is modified.

Deleting a Subscriber Entity State Property

To delete a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **State** tab.
   Entity state information is displayed.
4. In the list of entity state properties, use the check boxes to select the property or properties you want to delete.
   To select all properties, click **All**. To deselect all properties, click **None**.
5. Click **Delete**.
   A confirmation message displays.
6. Click **OK**.
   The property or properties are removed from the list.

The subscriber entity state properties are deleted.

Viewing Subscriber Quota Information

To view the quotas associated with a subscriber:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select the subscriber profile.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on locating a subscriber profile.)
3. Select the **Quota** tab.
   The **Subscriber Profile Quota Usage** page is displayed. The table provides the following information:
   - **Name** — Quota name defined in the CMP system.
   - **Time Usage** — Usage counter, in seconds, to track time-based resource consumption.
   - **Time Limit** — Time limit, in seconds, defined in the named quota.
   - **Total Volume Usage** — Usage counter, in bytes, to track volume-based resource consumption.
   - **Total Volume Limit** — Volume limit, in bytes, defined in the named quota.
   - **Upstream Volume Usage** — Usage counter, in bytes, to track upstream bandwidth volume-based resource consumption. Also known as Input Volume.
   - **Upstream Volume Limit** — Upstream volume limit, in bytes, defined in the named quota.
   - **Downstream Volume Usage** — Usage counter, in bytes, to track downstream bandwidth volume-based resource consumption. Also known as Output Volume.
   - **Downstream Volume Limit** — Downstream volume limit, in bytes, defined in the named quota.
   - **Service Specific Event** — Usage counter to track service-specific resource consumption.
   - **Service Specific Event Limit** — Resource consumption limit defined in the named quota.
   - **Next Reset Time** — The time after which the usage counters need to be reset.
   - **CID** — A unique identifier, assigned by the CMP system. Top-ups and rollovers have the CID of their associated plan.
   - **Type** — Defines whether the data is for a quota (plan), pass, rollover, top-up, or default rollover.
   - **Quota State** — An internal identifier, which defines whether the option selected in the **Type** field is active or expired.
   - **RefInstanceId** — The CID of the plan.
4. When you finish, click **Back to Search Page**.

You have viewed the subscriber quota information.

Adding a Subscriber Quota Category

To add a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)

3. Select the **Quota** tab.
   The Quota Usage information appears in the work area.
4. Click **Create**.
   The **Quota Usage** page opens. If you exceed 10 quotas, you are prompted whether to add more. Click **Yes** to continue, or **No** to stop.
5. Enter the following information:
   a) **CID** — A unique identifier assigned by the CMP system. Rollovers and top-ups have the CID of their associated plan.

      Note: This information is assigned by the system, and you should not change it.

   b) **Name** (required) — Select the name of a quota. You cannot add the same quota twice for a subscriber. See the *Policy Wizard Reference* for information on creating quotas.
   c) **Type** — Select the type of quota defined in the CMP system. You can select **quota** (plan), **pass**, **rollover**, **top-up**, or **default rollover**.
   d) **Time (seconds)** — Enter a value, in seconds, to track time consumption.
      The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
   e) **Total Volume (bytes)** — Enter a value, in bytes, to track bandwidth volume consumption.
      The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
   f) **Upstream Volume (bytes)** — Enter a value, in bytes, to track upstream bandwidth volume consumption.
      The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
   g) **Downstream Volume (bytes)** — Enter a value, in bytes, to track downstream bandwidth volume consumption.
      The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
   h) **Service Specific Event** — Enter a value representing service-specific resource consumption.
      The valid range is -2^{63} to $2^{63} - 1$ (a 64-bit value).
   i) **Next Reset Time** (required) — Enter a date and time after which the quotas need to be reset, in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*[*Z*] (for example, **`2011-11-01T00:00:01-5:00`**).
      Alternatively, click (calendar) and select a date, enter a time, and optionally select a UTC offset (time zone). When you finish, click **OK**.
   j) **Quota State** — This field is an internal identifier and should not be defined by the user.
   k) **RefInstanceID** — The CID of the associated plan. This field only applies to a top-up.

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

6. When you finish, click **Save**.

The subscriber quota is defined.

Modifying a Subscriber Quota Category

To modify a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)

3. Select the **Quota** tab.
   The **Subscriber Profile Quota Usage** page is displayed.
4. Click the name of the quota you want to modify.
   The **Quota Usage** page opens, displaying information about the quota.
5. Modify subscriber quota information as required.
   For a description of the fields contained on this page, see *Adding a Subscriber Quota Category*.
6. When you finish, click **Save**.

The subscriber quota category is modified.

Deleting a Subscriber Quota Category

To delete a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the **Quota** tab.
   Entity quota information is displayed.
4. In the list of quotas, use the check boxes to select the quota or quotas you want to delete.
   To select all quotas, click **All**. To deselect all quotas, click **None**.
5. Click **Delete**.
   A confirmation message displays.
6. Click **OK**.
   The quota or quotas are removed from the list.

The subscriber quota categories are deleted.

Adding a Member to a Pooled Quota Group

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

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

   The pool ID is an alphanumeric string of up to 255 characters that can contain hyphens (-) and underscores (_) but no spaces. **`0`** is invalid.

5. (Optional) In the **Pool Information** section of the page, enter the following:
   a) **Billing Day** — The billing day of the subscriber pool. This field is used only for monthly billing.
   b) **Tier** — Enter the name of a tier defined in the CMP database; or click **Manage** to select a tier.
   c) **Entitlements** — Click **Manage** and select one or more entitlement names defined in the CMP database.
   d) **Custom 1, Custom 2, Custom 3, Custom 4, Custom 5** — Enter name value fields. You can refer to them in policies.
   e) **Custom N** — If you click **Add**, you can add additional custom fields.
6. (Optional) In the **Membership Information** section of the page, to add a member or associate a subscriber to the pooled quota group.

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

   a) **Key Type** — The type of subscriber identifier type. 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.
   c) Click **Add** to add the subscriber to the pooled quota group.
7. When you finish, click **Save**.

The member is added to the pooled quota group.

Querying by Pool ID

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

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Select **Pool ID** in the **Key Type** pulldown and enter a **Key String**. Click **Search**.
   The **Pool Group Quota Profile** page opens with the search results. The following tabs are displayed:
   - **Pool Profile**
   - **Pool Quota**
   - **Pool State**
3. You can select the **Modify**, **Delete**, or **Back to Search Page** options.

Creating a Pool Quota Profile

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

To create a pool quota profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.

2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens.
4. Click **Pool Quota Profile**.
   The **Quota Usage** section displays.
5. Click **Create**.
6. Enter the following:
   a) **Name** — Select the name of the pool state.
   b) **Type** — Select the quota being assigned to the pool. You can select **quota** (plan), **pass**, **top-up**, **roll-over**, or **roll-over-def**.

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

      Note: This is typically the billing day, although for a daily quota the usage is normally reset at midnight or shortly thereafter.
7. When you finish, click **Save**.

The pool quota profile is created.

Modifying a Pool Quota Profile

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

To modify a pool quota profile:

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

   Note: The **Name** field cannot be changed.
7. When you finish, click **Save**.

The pool quota profile is modified.

Deleting a Pool Quota Profile

A pool quota profile can be deleted.

To delete a pool quota profile:

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

Modifying a Pool Profile

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

To modify a pool profile:

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

The pool profile is modified.

Deleting a Pool Profile

A pool profile can be deleted.

To delete a pool profile:

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

The pool profile is deleted.

Creating a Pool State

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

To create a pool state:

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

The pool state is created. The **Pool Entity State Properties** section displays the Pool Quota Group Key Fields and the searched Pool ID.

Modifying a Pool State

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

To modify a pool profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.

2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID**.
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The **Pool Profile** page opens with **Pool Profile** as the default.
4. Click **Pool State**.
   The **Pool Entity State Properties** section displays.
5. Select the **Name** of the pool state that you want to modify.
   The **Modify Property** section displays.
6. The **Name** and **Value** fields are displayed. You can only modify the **Value** field.
7. Modify the **Value** field.
8. When you finish, click **Save**.

The pool state content is modified.

Deleting a Pool State

A pool state can be deleted.

To delete a pool state:

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

The properties are deleted.

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. 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 Usage page is displayed. 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. When you finish, click **Back to Search Page**.

You have viewed the subscriber dynamic quota information.

Adding a Subscriber Dynamic Quota Category

To add a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the Dynamic Quota tab.
   The Dynamic Quota page is displayed.
4. Click **Create**.
   The **Create Subscriber Dynamic Quota** page opens. If you exceed 10 dynamic quotas, you are prompted with a message to add more; click **Yes** to continue, or **No** to stop.
5. Enter the following information:
   - **InstanceID** — A unique identifier.

     Note: Do not enter a colon (:) as part of this identifier.
   - **Name** — Select the name of a dynamic quota.
   - **Description/Location** — Free-form text.
   - **Type** — Select the type of quota defined in the CMP system. You can select **pass** or **top-up**.
   - **Priority** — Defines the order in which the dynamic quota is processed.

     The range is -32768 to 32767 (Max 16-bit short). Higher priority passes are used before lower priority passes. A higher number indicates a higher priority.
   - **Initial Time Limit (seconds)** — The initial value for time units granted by the dynamic quota.
   - **Initial Total Volume Limit (bytes)** — The initial value for total volume units granted by the dynamic quota.

     The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).

- **Initial Upstream Volume Limit (bytes)** — Enter a value, in bytes, to track upstream bandwidth volume consumption.

  The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).

- **Initial Downstream Volume Limit (bytes)** — Enter a value, in bytes, to track downstream bandwidth volume consumption.

  The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).

- **Initial Service Specific Limit (events)** — Enter a value representing service-specific resource consumption.

  The valid range is -2^{63} to $2^{63} - 1$ (64-bit value).

- **Purchase Time** — The date and time that the dynamic quota was purchased.

  For the **Purchase Time**, **Active Time**, and **Expire Time** fields, use the format *yyyy-mm-dd*T*hh*:*mm*:*ss*[*Z*] (for example, **`2011-11-01T00:00:01-5:00`**). Alternatively, click on the calendar icon, and from the window that opens, select a date, enter a time, and optionally select a UTC offset (time zone). When you finish, 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. When you finish, click **Save**.

The subscriber quota is defined and the page displays the message `Quota created successfully`.

Modifying a Subscriber Dynamic Quota Category

To modify a subscriber dynamic quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The **Subscriber Profile Administration** page opens.
2. Find the subscriber profile you want to view.

Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)

3. Select the **Dynamic Quota** tab.
   The **Dynamic Quota** page is displayed.
4. Select the name of the quota you want to modify.
   The **Modify Subscriber Dynamic Quota** page opens, displaying information about the dynamic quota.
5. Modify subscriber quota information.
   For a description of the fields contained on this page, see *Adding a Subscriber Dynamic Quota Category*.
6. When you finish, 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. When you finish, 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 quota(s) you want to delete.
   To select all dynamic quotas, click **All**. To deselect all dynamic quotas, click **None**.
5. Click **Delete**.
   A confirmation message displays.
6. Click **OK**.

The subscriber dynamic quota categories are deleted.

Chapter 12

Managing Subscribers

Topics:

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

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

Creating a Tier

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

To create a subscriber tier:

1. From the **Subscriber** section of the navigation pane, select **Tiers**.
   The content tree displays the **Tiers** folder.
2. Select the **Tiers** folder.
   The **Tier Administration** page opens.
3. Click **Create Tier**.
   The **New Tier** page opens.
4. Enter information as follows:
   a) **Name** (required) — Name of the tier.

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

   b) **Description/Location** — Free-form text.

      Enter up to 250 characters.

   c) **Downstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the downstream direction in bits per second.

      You can enter a value followed by M or G; for example, 4G for 4 gigabits per second.

   d) **Upstream bandwidth limit (bps)** — The maximum amount of bandwidth capacity available in the upstream direction in bits per second.

      You can enter a value followed by M or G; for example, 10M for 10 megabits per second.

5. When you finish, click **Save**.
   The tier is added to the CMP database.

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. Once you define entitlements, you can use them in policy rules.

To create an entitlement:

1. From the **Subscriber** section of the navigation pane, select **Entitlements**.
   The content tree displays the **Entitlements** folder.
2. Select the **Entitlements** folder.
   The **Entitlement Administration** page opens.
3. Click **Create Entitlement**.
   The **New Entitlement** page opens.
4. Enter information as follows:
   a) **Entitlement ID** (required) — Name of the tier.
      The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
      Enter up to 250 characters.
5. When you finish, click **Save**.

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.

Managing Sessions

You can display static session and binding data for a specific subscriber from the Policy Management device that is managing the session. Depending on how the data is indexed on the device, you can search for a subscriber by IMSI, MSISDN, IP address, or NAI. You can also delete obsolete sessions.

Note: This function is not supported by Policy Management devices before V7.5.

To view a session:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **All**.
2. Select the Policy Management device managing the session you are interested in.
   The **Policy Server Administration** page opens in the work area.
3. Select the **Session Viewer** tab.
   The **Session Viewer** tab opens.
4. Enter search information as follows:
   a) **Identifier type** (required) — Select one of the following identifier types:
      - **NAI** (default)
      - **E.164(MSISDN)**
      - **IMSI**
      - **Diameter Session ID**
      - **Diameter IPv4Address**
      - **Diameter IPv6Prefix**

      The identifier types you can specify are determined by the configuration of the Policy Management device. For example, if the IndexByNAI setting is not specified on the device, then you cannot select **NAI**.

      Note: When searching primary Gx sessions by IPv6 prefix, only 64-bit masks are supported.

   b) **Identifier name** — Free-form text.
      Enter up to 250 characters.
5. Click **Search**.
   If sessions are available for the subscriber, subscriber session data is displayed. *Figure 16: Session Viewer Page* shows an example. If the subscriber has correlated secondary sessions, the correlated secondary session data is also displayed.

If you are viewing subscriber data from a stateful MRA system, subscriber binding data is displayed, including an identifier for the MPE device handling sessions for that subscriber. If that MPE device is managed by this CMP system, you can click the identifier to view session data from the MPE device.

Note: If an external system generates data that, when translated to ASCII, creates illegal characters, they are displayed by the Session Viewer as question marks (?).

For each session displayed from an MPE device, you can click **Delete Session** to delete the session. For each subscriber displayed from an MPE device, you can click **Delete Subscriber's All Session** to delete all sessions for that subscriber. For each session binding displayed from an MRA device, you can click **Delete Binding** to delete the binding. This deletes the record in the appropriate database.

CAUTION

Caution: Only obsolete sessions should be deleted. If you delete an active session, there is no signal to any associated gateways or external network elements.

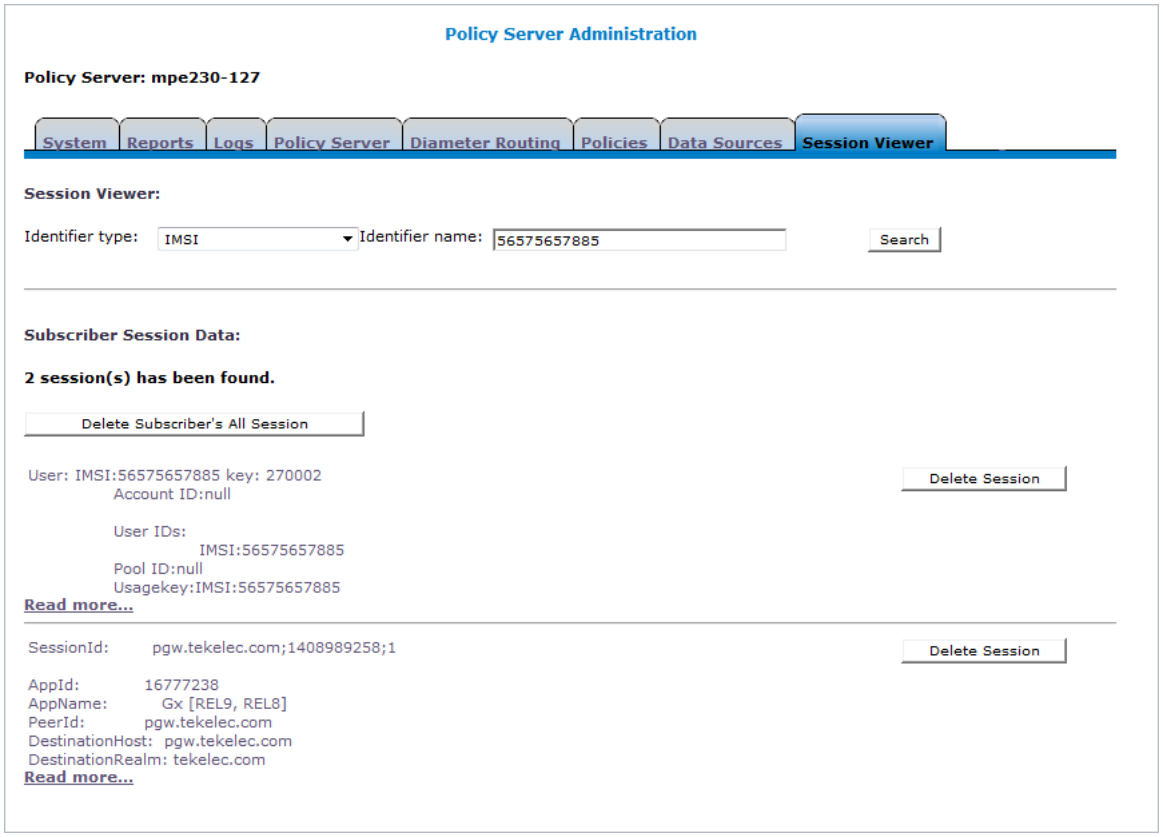


Figure 16: Session Viewer Page

Chapter 13

Managing Network Elements

Topics:

Managing Network Elements describes how to define network elements within the CMP system.

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

About Network Elements

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

- Gateway GPRS support node (GGSN)
- Router
- Server

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

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

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

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

Defining a Network Element

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group in which you want to define the network element.

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

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

      Enter up to 250 alphanumeric characters. The name can include underscores (_), hyphens (-), colons (:), and periods (.).

   b) **Host Name/IP Address** (required) — Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element.
   c) **Backup Host Name** — Alternate address that is used if communication between the MPE device and the network element's primary address fails.
   d) **Description/Location** — Free-form text.

Enter up to 250 characters.

e) **Type** (required) — Select the type of network element.

The supported types are:

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

- **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
- **Radius-BNG** — RADIUS broadband network gateway
- **HSGW** — HRPD Serving Gateway
- **PGW** — Packet Data Network Gateway
- **SGW** — Serving Gateway
- **DPI** — Deep Packet Inspection device
- **DSR** — Diameter Signaling Router device
- **NAS** — Network Access Server device

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

g) **Capacity** — The bandwidth allocated to this network element.

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

You have created the definition for a network element.

Modifying a Network Element

To modify a network element:

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

The network element definition is modified.

Deleting Network Elements

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

To delete a network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Network Element Administration** page opens in the work area, displaying all defined network elements.
3. From the work area, click (trash can icon), located to the right of the network element you want to delete:

   A confirmation displays.
4. Click **OK** to delete the network element.
   The network element is removed from the list.

You have deleted the definition of the network element.

Bulk Delete

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select **ALL**.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Bulk Delete**.
   The **Bulk Delete Network Elements** page opens.
4. Select the network elements or network element groups to delete.

   By default, the **Search Pattern** entry box contains an asterisk (*) to match all network elements. To search for a subset of network elements, enter a search pattern (for example, `star*`, `*pGw`, or `*-*`), click **Filter**, and select from the filtered results.
5. Click **Bulk Delete**.
   A confirmation message displays.
6. Click **OK** to delete the network elements.

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

Finding a Network Element

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select **ALL**.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, click **Search**.
   The **Network Element Search Criteria** window opens.
4. Enter the search criteria. Searches are not case sensitive. You can use the asterisk (*) and question mark (?) wildcard characters.
   - **Name** — The name assigned to the network element.
   - **Host Name/IP Address** — The domain name or IP address, in IPv4 or IPv6 format, of the network element.
   - **Description** — The information pertaining to the network element that helps identify it within the network. Enter up to 250 characters.
5. After entering search criteria, click **Search**.

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

Configuring Options for Network Elements

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

Note: Configuration changes made in the CMP system could potentially be reverted on an MPE device if the scheduled run time of the OSSI Distributor task on the Management Agent is before the scheduled run time for the CMP system. The discrepancy is resolved when the OSSI Distributor Task runs on the CMP system. See *Managing Scheduled Tasks* for more information.

PDSN

To configure options for a packet-switched data network (PDSN) network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the PDSN tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the RADIUS-S features:
   a) **RADIUS Enabled**— Click on this checkbox to enable/disable RADIUS-S support for this network element.
   b) **RADIUS Shared Secret**— Enter the value that is used by the network element to authenticate RADIUS messages sent from the MPE device. This field must be configured with the same value that is provisioned on the network element or the MPE device will not be able to send messages to the network element.

5. Configure the Diameter features:
   a) **Diameter Realm**— Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

      Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.
6. When you finish, click **Save**.

The PDSN device is defined.

Home Agent

To configure options for a Home Agent network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the Home Agent tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the RADIUS-S features:
   a) **RADIUS Enabled**— Click on this checkbox to enable/disable RADIUS-S support for this network element.
   b) **RADIUS Shared Secret**— Enter the value that is used by the network element to authenticate RADIUS messages sent from the MPE device. This field must be configured with the same value that is provisioned on the network element or the MPE device will not be able to send messages to the network element.
5. Configure the Diameter features:
   a) **Diameter Realm**— Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

      Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

6. When you finish, click **Save**.

The Home Agent device is defined.

GGSN

To configure interface information for a gateway GPRS support node (GGSN) network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **GGSN** tab and then click **Modify**.
   The **Modify Network Element** page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

      Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.
5. When you finish, click **Save**.

The GGSN device is defined.

HSGW

To configure interface information for an HSGW network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **HSGW** tab and then click **Modify**.
   The **Modify Network Element** page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

      Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use

the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. When you finish, click **Save**.

The HSGW device is defined.

PGW

To configure interface information for a packet data network gateway (PGW) network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **PGW** tab and then click **Modify**.
   The **Modify Network Element** page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **FQDN** — Customer-specific fully qualified domain name of the network element.
   c) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

   Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

   A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. When you finish, click **Save**.

The PGW device is defined.

SGW

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

      Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.
5. When you finish, click **Save**.

The SGW device is defined.

DPI

To configure interface information for a deep packet inspection (DPI) network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The **Network Element Administration** page opens in the work area.
3. On the **Network Element Administration** page, select the **DPI** tab and then click **Modify**.
   The **Modify Network Element** page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

      Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

      A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.
   c) **SCTP Enabled** (available if DPI capability is **TDF-Solicit**) — By selecting the check box, you connect to the traffic detection function (TDF) using the SCTP protocol. TCP is the default connection protocol.
   d) **Allow direct connection from MPE** (available if DPI capability is **TDF-Solicit**) — By selecting the check box, TDF connects directly to Sd with the MPE device (bypassing the MRA device).
   e) **TDF Port** (available if DPI capability is **TDF-Solicit**) — Enter the port number used to communicate with the TDF device. The default port is 3868.

f) **Watch Dog Interval** (available if DPI capability is **TDF-Solicit**) — Enter the watchdog timer interval in seconds. The default is 30 seconds.
g) **Response Timeout** (available if DPI capability is **TDF-Solicit**) — Enter the response timeout interval in seconds. The default is 5 seconds.
h) **Reconnect Delay** (available if DPI capability is **TDF-Solicit** and **Allow direct connection from MPE** is selected) — Enter the response time in seconds. The default is 3 seconds.
i) **Associated MRA identity** (available if DPI capability is **TDF-Solicit**) — Select the MRA device from the drop-down list.
You cannot associate a DPI device with an MRA device if you have selected **Allow direct connection from MPE**.
j) **Backup TDF Identity** (available if DPI capability is **TDF-Solicit**) — Select the backup TDF device from the drop-down list.

5. When you finish, click **Save**.

The DPI device is defined.

DSR

To configure interface information for an Oracle Communications Diameter Signaling Router (DSR) network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
The **Network Element Administration** page opens in the work area.
3. Select the **DSR** tab and then click **Modify**.
The **Modify Network Element** page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity**— Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`).

   Note: A vendor-specified host name and realm name (such as `ne.galactel.com`) resolves to an internal DNS server for vendor network access only. For Internet (roaming) access, use the format defined in the 3GPP Technical Specification: host name, network code, country code, and domain name.

   A single network element can have multiple Diameter identities with each represented as a separate Diameter connection from the same appliance. Click **Add** to add the identity to the list. To delete one of the identities, select it form the list and click **Delete**.

5. When you finish, click **Save**.

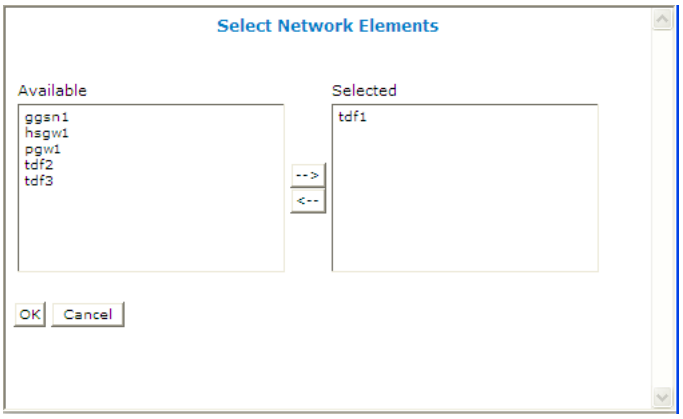
The DSR device is defined.

Associating a Network Element with an MPE Device

To associate a network element with an MPE device:

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

   The **Select Network Elements** window opens; for example:



6. Select the network elements in the **Available** list and click **-->**.

   If there are 50 or fewer defined network elements, they appear in the **Available** list. Select a network element from the **Available** list and click **-->**. The network element is moved to the **Selected** list.

   If there are more than 50 defined network elements, the **Available** list is initially blank. To add available items, enter a search string in the **Search Patterns** field. Searches are not case sensitive. You can use the wildcard characters * and ?. When you finish, click **Filter**. The network elements are moved to the **Selected** list.

   To disassociate a network element from the MPE device, select the network element from the **Selected** list and click **<--**. To select multiple entries, use the Ctrl and Shift keys.
7. When you finish, click **OK**.
   The selected network elements are added to the list of network elements managed by this MPE device.
8. To associate a network element group with the MPE device, select the group from the list of network element groups located under **Associations**.
9. When you finish, click **Save**.

The network element is associated with this MPE device.

Working with Network Element Groups

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

Creating a Network Element Group

To create a network element group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Network Element Administration** page opens in the work area.
3. Click **Create Group**.
   The **Create Group** page opens.
4. Enter the name of the new network element group.

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

You have created a network element group.

Adding a Network Element to a Network Element Group

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

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

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

   - If there are 25 or fewer network elements defined, the page displays the network elements not already part of the group. (*Figure 17: Add Network Element Page* shows an example.)
   - If there are more than 25 network elements defined, the page does not display any of them. Instead, use the **Search Pattern** field to filter the list. Enter an asterisk (*) to generate a global search, or a search pattern to locate only those network elements whose name matches the pattern (for example, **`star*`**, **`*pGw`**, or **`*-*`**). When you have defined a search string, click **Filter**; the page displays the filtered list.

4. Select the network element you want to add; use the Ctrl or Shift keys to select multiple network elements.

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

5. When you finish, click **Save**.

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

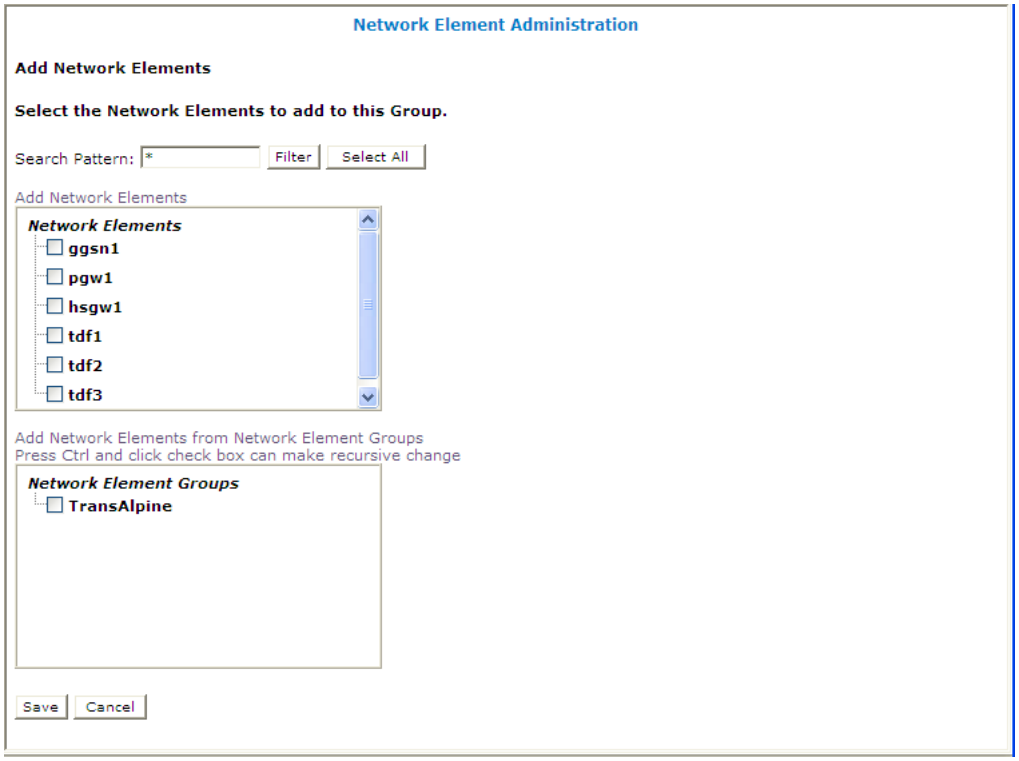


Figure 17: Add Network Element Page

Creating a Network Element Sub-group

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group.
   The **Network Element Administration** page opens in the work area, displaying the contents of the selected network element group.
3. Click **Create Sub-Group**.
   The **Create Group** page opens.
4. Enter the name of the new sub-group.

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

5. Enter a text description of the sub-group.

6. When you finish, click **Save**.

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. Delete a network element using one of the following methods.
   - On the **Network Element Administration** page, click (scissors icon), located to the right to the network element you want to remove.
   - From the content tree, select the network element. The **Network Element Administration** page opens. Click the **System** tab and then click **Delete**.

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

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

Modifying a Network Element Group

To modify a network element group or sub-group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group or sub-group.
   The **Network Element Administration** page opens in the work area.
3. Click **Modify**.
   The **Modify Group** page opens.
4. Modify the name or description.
5. When you finish, click **Save**.

The group is modified.

Deleting a Network Element Group or Sub-group

Deleting a network element group also deletes any associated sub-groups. However, any network elements associated with the deleted groups or sub-groups remain in the **ALL** group, from which they can be used again if needed. You cannot delete the **ALL** group.

To delete a network element group or sub-group:

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

The network element group or sub-group is deleted.

Chapter 14

Managing Policy Front End Devices

Topics:

Managing Policy Front End Devices describes how to define and manage Oracle Communications Policy Management Policy Front End (also known as MRA) devices in the CMP system.

Note: For more information on using MRA servers, refer to the *Policy Front End Wireless User's Guide*.

Configuring the CMP System to Manage an MRA Cluster

The Policy Front End (also known as the MRA) device is a standalone entity that supports MPE devices. The CMP system is used to manage all MRA functions. Before this can occur, the CMP operating mode must support managing MRA clusters.

To reconfigure the CMP operating mode, complete the following:

CAUTION

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

1. From the **Help** navigation pane, select **About**.
   The **About** page opens, displaying the CMP software version number.
2. Click the **Mode** button.

   Consult with My Oracle Support for information on this button.

   The **Mode Settings** page opens.
3. At the bottom of the page, select **Manage MRAs**.
4. Click **OK**.
   The browser page closes and you are automatically logged out.
5. Refresh the browser page.
   The **Welcome admin** page is displayed.

You are now ready to define an MRA cluster profile, specify network settings for the MRA cluster, and associate MPE devices with the MRA cluster.

Defining an MRA Cluster Profile

You must define a profile for each MRA cluster you are managing. To define an MRA cluster profile:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the ALL group.
   The **MRA Administration** page opens in the work area.
3. Click **Create Multi-protocol Routing Agent**.
   The **New MRA** page opens.
4. Enter information as appropriate for the MRA cluster:
   a) **Associated Cluster** (required) — Select the MRA cluster from the pulldown list.
   b) **Name** (required) — Enter a name for the MRA cluster.

      The name can contain any alphanumeric characters except quotation marks (") and commas (,).
   c) **Description/Location** (optional) — Free-form text.

      Enter up to 250 characters.
   d) **Secure Connection** — Select to enable a secure HTTP connection (HTTPs) instead of a normal connection (HTTP).

The default is a non-secure (HTTP) connection.

e) **Stateless Routing** — Select to enable stateless routing. In stateless routing, the MRA cluster only routes traffic; it does not process traffic.

The default is stateful routing.

5. When you finish, click **Save**.

The MRA cluster profile is defined. If you are setting up multiple MRA clusters, you must define multiple cluster profiles. Repeat the above steps to define additional profiles.

Modifying an MRA Cluster Profile

To modify MRA cluster profile settings:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA cluster profile.
   The **MRA Administration** page opens in the work area.
3. Select the **System** tab of the **MRA Administration** page
4. Click **Modify**.
   The **Modify System Settings** page opens.
5. Modify MRA system settings.
6. When you finish, click **Save**.

The MRA cluster profile settings are modified.

Working with MRA Groups

MRA groups let you organize MRA cluster profiles into groups. You can create, rename, and delete MRA groups, and add and remove MRA cluster profiles from groups.

Creating an MRA Group

To create an MRA group:

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

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

5. When you finish, click **Save**.

The MRA group is created.

Adding an MRA Cluster Profile to an MRA Group

Once an MRA group is created, you can add MRA cluster profiles to it. To add an MRA cluster profile to an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select an MRA group.
   The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.
3. Click **Add Multi-protocol Routing Agent**.
   The **Add Multi-protocol Routing Agent** page opens.
4. Select the MRA cluster profile you want to add or use the Ctrl or Shift keys to select multiple MRA cluster profiles.
5. When you finish, click **Save**.

The MRA cluster profile is added to the MRA group.

Deleting an MRA Cluster Profile from an MRA Group

Removing an MRA cluster profile from an MRA group does not delete the MRA cluster profile from the ALL group, so it can be used again if needed. Removing an MRA cluster profile from the ALL group removes it from all other groups.

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

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the MRA group.
   The **MRA Administration** page opens in the work area, displaying the contents of the selected MRA group.
3. Remove the MRA cluster profile using one of the following methods:
   - On the **MRA Administration** page, click the **Delete** icon, located to the right of the MRA cluster profile you want to remove.
   - From the content tree, select the MRA cluster profile; the **MRA Administration** page opens. On the **System** tab, click **Remove**.

   The MRA cluster profile is removed from the group.

Deleting an MRA Group

Deleting an MRA group also deletes any associated sub-groups. However, any MRA cluster profiles associated with the deleted groups or sub-groups remain in the ALL group. You cannot delete the ALL group.

To delete an MRA group or sub-group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is**ALL**.
2. Select the MRA group or subgroup from the content tree.
   The contents of the selected MRA group are displayed.
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the selected group.

The MRA group is deleted.

Enabling Stateless Routing

To hide configuration relevant to a stateful MRA device in the CMP display, perform the following procedure.

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is**ALL**.
2. Select the MRA from the content tree.
   The **MRA Administration** page displays the configuration for the MRA.
3. Select the **System** tab.
   The **Modify System Settings** page opens.
4. Select **Stateless Routing** (*Figure 18: Enabling Stateless Routing* shows an example).

The stateful MRA configuration is hidden.

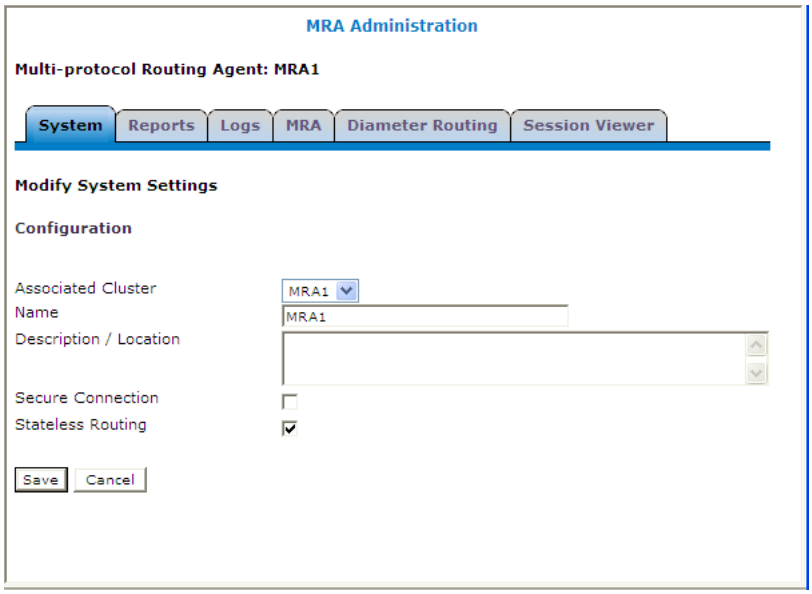


Figure 18: Enabling Stateless Routing

Reapplying the Configuration to Policy Management Devices

You can reapply the configuration to an individual MPE or MRA device (server), or to all MPE or MRA devices in a group. When you reapply the configuration, the CMP system completely reconfigures

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

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

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

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

Resetting Counters

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

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

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

The counters are reset.

Chapter 15

Managing Message Distribution Function Servers

Topics:

Managing Message Distribution Function Servers describes how to define and manage Message Distribution Function (MDF) servers in the CMP system.

Note: For more information on using MDF servers, refer to the *Message Distribution Function Reference*.

Message Distribution Function Overview

The Message Distribution Function (MDF) is a standalone server deployed between a Mediation Gateway (MGW) and a data source. An SPR system can be one of the following:

- Oracle Communications Subscriber Database Management (SDM) system
- Oracle Communications User Data Repository (UDR) system
- A customer SPR system

The MDF system provides the modifications necessary to map provisioning requests from an MGW system to the data schema required for Policy Management systems and policies. This includes mapping subscriber profile data to relevant usage data that is then distributed to Policy Management subscriber profile, quota, state, and dynamic quota data objects. The MDF system provides the logic necessary to map the provisioning data associated with the one person, multiple devices (OPMD) feature to the pool profiles that are needed to manage the capability within Multimedia Policy Engine (MPE) and SPR systems.

The MDF system presents a set of Simple Object Access Protocol (SOAP) application programming interfaces (APIs) to support migration, provisioning, subscriber management, and quota management.

The MDF system provides an interface to collect alarm, event log, and performance metrics from the SPR system and distribute them to an enterprise management system (EMS) through an Oracle Communications Policy Management Configuration Management Platform (CMP) system. This insulates the EMS from the SPR operations, administration, and management (OAM) interfaces.

The MDF system includes a load-shedding mechanism to reduce latency and remain stable and reliable for SOAP transactions under overload conditions. If the MDF system becomes overloaded (busy), requests to add subscribers are rejected. The configuration parameters are factory-preset and should not be changed.

The MDF system includes a throttling mechanism to gracefully reduce performance under overload conditions. The throttling mechanism is implemented using a token bucket algorithm that limits the rate of sending requests to the SPR provisioning interface. The configuration parameters are factory-preset and should not be changed.

Defining a MDF Server

To define a new MDF server:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is **ALL**.
2. From the content tree, select **ALL**.
   The **Mediation Server Administration** page opens in the work area.
3. Click **Create Mediation Server**.
   The **New Mediation Server** page opens.
4. Enter information as appropriate for the MDF server:
   a) **Associated Cluster** (required) — Select a MDF cluster from the pulldown list.
   b) **Name** (required) — Enter a name for the MDF server.

The name can be up to 32 characters long. The name can contain any alphanumeric characters except quotation marks (") and commas (,).

c) **Description/Location** (optional) — Free-form text that described the cluster.

Enter up to 250 characters.

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

The default is a non-secure (HTTP) connection.

5. When you finish, click **Save**.

The MDF server is defined.

Modifying an MDF Server Profile

To modify an MDF server profile:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is **ALL**.
2. From the content tree, select the MDF profile.
   The **Mediation Server Administration** page opens in the work area.
3. Select the **System** tab.
   The current profile settings are displayed.
4. Click **Modify**.
   The **Modify System Settings** page opens.
5. Make changes as necessary. See *Defining a MDF Server* for information on settings.
6. When you finish, click **Save**.

The MDF profile is modified.

Creating an MDF Server Group

You can create groups for MDF servers to organize and simplify management.

To create an MDF server group:

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

   The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. When you finish, click **Save**.

The MDF group is created.

Adding an MDF Server to an MDF Server Group

To add an MDF server to an MDF server group:

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

The MDF server is added to the selected group.

Creating an MDF Server Sub-group

You can create sub-groups to further organize your Policy Management network. To add an MDF sub-group to an existing MDF group:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is **ALL**.
2. From the content tree, select the MDF group.
   The **Mediation Server Administration** page opens in the work area, displaying the contents of the selected MDF group.
3. Click **Create Sub-Group**.
   The **Create Group** page opens.
4. Enter the name of the new MDF sub-group.

   The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. When you finish, click **Save**.

The MDF sub-group is created.

Renaming an MDF Server Group

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

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

2. From the content tree, select the MDF group or sub-group.
   The **Mediation Server Administration** page opens in the work area.
3. Click **Modify**.
   The **Modify Group** page opens.
4. Enter the new name in the **Name** field.

   The name cannot contain quotation marks (") or commas (,).
5. When you finish, click **Save**.

The group is renamed.

Removing an MDF Server from an MDF Group

Removing an MDFprofile from an MDF group or sub-group does not delete the profile. To delete an MDF profile, see *Deleting an MDF Server*.

To remove an MDF profile from an MDF group or sub-group:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is**ALL**.
2. From the content tree, select the MDF group or sub-group.
   The **Mediation Server Administration** page opens in the work area, displaying the contents of the selected MDF group or sub-group.
3. Remove the MDF profile using one of the following methods:
   - Click the Remove ( ) icon located next to the MDF profile you want to remove.
   - From the content tree, select the MDF profile; the **Mediation Server Administration** page opens. Click the **System** tab; the **System** tab opens. Click **Remove**.

   The MDF profile is removed immediately; there is no confirmation message.

The MDF profile is removed from the group or sub-group.

Deleting an MDF Server

Deleting an MDF profile from the ALL group also deletes it from any associated group.

To delete an MDF profile:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is**ALL**.
2. From the content tree, select the **ALL** group.
   the **Mediation Server Administration** page opens in the work area, displaying all defined MDF profiles.
3. Use one of the following methods to select the MDF profile to delete:
   - From the work area, click (trash can icon) located next to the MDF profile you want to delete.

- From the MDF group tree, select the MDF profile. The **Mediation Server Administration** page opens. Click the **System** tab. Click **Delete**.

A confirmation message displays.

4. Click **OK**.

The MDF definition is removed from the CMP database.

Deleting an MDF Server Group

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

To delete an MDF group or sub-group:

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

The MDF group is deleted.

Reapplying the Configuration to an MDF Server

You can reapply the configuration to an MDF cluster. When you reapply the configuration the CMP system completely reconfigures the servers in the cluster with topology information, ensuring that the configuration matches the data in the CMP database. This action is not needed during normal operation but is useful in the following situations:

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

CAUTION

Caution: Reapplying the configuration pushes the settings on the CMP system to the selected MDF server and overwrites the current settings stored on that server.

To reapply the configuration to an MDF server:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is**ALL**.
2. Select the MDF group from the content tree.
   The contents of the selected group are displayed.
3. Select an MDF server from the group.
   The information for the server displays in the **Mediation Server Administration** page.
4. Select the **System** tab.
   The configuration information for the server displays.
5. Click **Reapply Configuration**.
   If the application was successful, you receive the message, `The configuration was applied successfully`.

The configuration is reapplied to the MDF server.

Viewing MDF Server Settings

To view MDF server settings:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is**ALL**.
2. Select the MDF group from the content tree.
   The contents of the selected group are displayed.
3. Select an MDF server from the group.
   The information for the server displays in the **Mediation Server Administration** page.
4. Click the **Settings** tab.
   The settings for the MDF server display.

Settings for the SOAP interface, Diameter, MGW data source, and load shedding configuration are displayed.

Modifying MDF Server Settings

To modify MDF server settings:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is **ALL**.
2. From the content tree, select the MDF server.
   The **Mediation Server Administration** page displays information for the server.
3. Select the **Settings** tab.
   The current configuration options are displayed.

4. Click **Modify**.
   The **Modify Mediation Server** page opens.
5. Make changes to the configuration as necessary.
   See the following tables for the available options.
   - *Table 24: MDF SOAP Interface Settings*
   - *Table 25: MDF Diameter Settings*
   - *Table 26: MDF MGW Data Source Settings*
   - *Table 27: MDF Load Shedding Settings*
6. When you finish, click **Save**.

The modifications are stored in the CMP database.

Table 24: MDF SOAP Interface Settings

Attribute	Description
SOAP User Name	Enter the account user name used to authenticate SOAP requests. This field can be left blank.
SOAP Password	Enter the account password used to authenticate SOAP requests. The value is stored as an MD5 digest. This field can be left blank.
Enable HTTP Service	If enabled, the MDF system communicates using HTTP protocol. Either **Enable HTTP Service** or **Enable HTTPS Service** must be enabled; both can be enabled.
HTTP port	Enter the port number of the HTTP server. The default port is 80.
Enable HTTPS Service	If enabled, the MDF system communicates using HTTPS protocol. Either **Enable HTTP Service** or **Enable HTTPS Service** must be enabled; both can be enabled.
HTTPS port	Enter the port number of the HTTPS server. The default port is 443.

Table 25: MDF Diameter Settings

Attribute	Description
Diameter Port	Enter the Diameter port number of the MDF server. The default is 3868.
Diameter Realm	The domain of responsibility (for example, **`galactel.com`**) of the MDF server.
Diameter Identity	Enter the fully qualified domain name (FQDN) of the MDF server (for example, **`mdf2.galactel.com`**).

Table 26: MDF MGW Data Source Settings

Attribute	Description
MGW User Name	Enter the user name for the messaging gateway access account (if the MGW requires authentication).

Attribute	Description
MGW Password	Enter the password for the messaging gateway access account (if the MGW requires authentication).
MGW Base URI	Enter the uniform resource identifier for the messaging gateway.
MGW IP	Enter the IP address of the messaging gateway.
MGW Port	Enter the port number of the messaging gateway. The default is 80.

Table 27: MDF Load Shedding Settings

Attribute	Description
Enabled	If enabled, the MDF system performs load shedding during periods of excessive usage.

Configuring MDF Advanced Settings

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

CAUTION

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

To configure an advanced setting on an MDF device:

1. From the **Mediation** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MDF groups; the initial group is **ALL**.
2. From the content tree, select an MDF device.
   The **Mediation Server Administration** page opens.
3. Select the **Settings** tab.
   The MDF configuration settings are displayed.
4. Click **Advanced**.
   The **Other Advanced Configuration Settings** table opens.
5. Click **Add**.
   The **Add Configuration Key Value** window opens.
6. Enter the following values:
   a) **Configuration Key** — The attribute to set
   b) **Value** — The attribute value
7. When you finish, click **Save**. The key is added to the table.

CAUTION

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

8. (Optional) Add, edit, delete, or order keys.
   - 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. When you finish, 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. When you finish, 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.
9. When you finish, click **Save**.

The settings are applied to the selected MDF device.

Data Source Interfaces for MDF Devices

Before the MDF device can communicate with any external data sources, you must configure the interface. You can configure data source interfaces for an individual MDF device. See *Configuring Data Source Interfaces for an MDF Device*.

From within the **Data Sources** window, you can configure Sh (SDM or UDR) or provisioning (customer SPR) data sources. See the following tasks:

- *Configuring Data Source Interfaces for an MDF Device*
- *Configuring the Sh Data Source for an MDF Server*
- *Configuring the SPR Provisioning Data Source for an MDF Server*

Subscriber data can be mapped by IMSI prefix to an SDM , UDR, or a customer SPR system. For information, see *Selecting Data Sources for MDF Devices*.

Configuring Data Source Interfaces for an MDF Device

To configure a data source interface for an MDF device:

1. From the **Mediation** 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 MDF server.
   The **Mediation Server Administration** page opens.
3. Select the **Data Sources** tab.
   The current data sources are displayed, listing the administrative state, name, type, primary address, and primary port.
4. Click **Modify**
   The **Data Sources** page opens.
5. Add a data source to the table.
   a) Select the data source type from the **Add** pulldown list. The appropriate **Add Data Source** window opens.
   b) Configure the values.
   c) When you finish, click **Save**. The data source is added to the table.

   For more information, see *Configuring the SPR Provisioning Data Source for an MDF Server* and *Configuring the Sh Data Source for an MDF Server*.
6. (Optional) Add, modify, delete, or order the data sources using the following functions:
   - Cloning an entry in the table
     1. Select an entry in the table.
     2. Click **Clone**. The **Clone** window opens with the information for the entry.
     3. Make changes as required.
     4. When you finish, click **Save**. The entry is added to the table
   - Editing a data source in the table
     1. Select the data source in the table.
     2. Click **Edit**. The **Edit Data Source** window opens, displaying the information for the data source.
     3. Make changes as required.
     4. When you finish, click **Save**. The data source is updated in the table.
   - Deleting a data source from the table
     1. Select the data source in the table.
     2. Click **Delete**. A confirmation message displays.
     3. Click **Delete** to remove the data source entry. The data source is removed from the table.
   - Ordering the list.

     If you define multiple entries, they are searched in the order displayed in this list. To change the order:
     1. Select an entry.
     2. Click **Up** or **Down**. The search order is changed.

7. Configure the **General Settings**.
   - **OCUDR Enabled Multiple Key validation**—Enables the use of the UDR multiple key validation. This option is only valid for UDR 10.2 and later.
8. When you finish, click **Save**.

The data source interface for the MDF is configured.

Configuring the Sh Data Source for an MDF Server

See *Configuring Data Source Interfaces for an MDF Device* for information on the **Add Data Source** page.

An Sh data source is usually an Oracle Communications Subscriber Database Management (SDM) or Oracle Communications User Data Repository (UDR) device. To define an Sh data source, on the **Add Data Source** page, enter the following information:

1. **Admin State** — Enable this data source.

   Selected by default.
2. **Sh Profile** — Select **ProfileV4** (to support provisioning of pass, rollover, and top-up information).

   Note: ProfileV4 is the only Sh profile available for MDF servers.
3. Specify the data source version number in the form ***x.x***.

   This number identifies the data source as either SDM or UDR. A version number of 9.*x* specifies an SDM data source. A version number of 10.*x* specifies a UDR data source.
4. **Primary Servers**:
   a) **Primary Identity** — Primary server host name.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary server.
   c) **Primary Port** — Primary server port number.

      The default is 3868.
   d) **Secondary Identity** — Secondary server host name.
   e) **Secondary Address** — IP address, in IPv4 or IPv6 format, of the secondary server.
   f) **Secondary Port** — Secondary server port number.

      The default is 3868.
5. **Backup Servers**:
   a) **Primary Identity** — Primary backup server name.
   b) **Primary Address** — IP address, in IPv4 or IPv6 format, of the primary backup server.
   c) **Primary Port** — Primary backup server port number.

      The default is 3868.
   d) **Secondary Identity** — Secondary backup server name.
   e) **Secondary Address** — IP address, in IPv4 or IPv6 format, of the secondary backup server.
   f) **Secondary Port** — Secondary backup server port number.

      The default is 3868.
6. **Common**:
   a) **Realm** — Sh server realm; for example, `galactel.com`.
   b) **Unique Name** — The unique name assigned to the Sh server.

c) **Connect SCTP** — Indicates whether the Sh data source can support SCTP protocol. If checked, an MDF device can communicate with the Sh data source in SCTP.

7. When you finish, click **Save**.

The Sh data source is configured.

Configuring the SPR Provisioning Data Source for an MDF Server

See *Configuring Data Source Interfaces for an MDF Device* for information on the **Add Data Source** page.

A provisioning data source is a customer SPR system. To define a provisioning data source, on the **Add Data Source** page, enter the following information:

1. **Admin State** — Enable this data source.

   Selected by default.

2. Specify the data source version number in the form ***x.x***.

   This number identifies the data source as either SDM or UDR. A version number of 9.*x* specifies an SDM data source. A version number of 10.*x* specifies a UDR data source.

3. **Unique Name** — The unique name assigned to the SPR Provisioning Data Source. Identifies which SPR data source to use.
4. **Host** — The FQDN or IP address of the SPR data source. Enter the standard dot-formatted IP address string.
5. **User Name** — The user name for the SPR access account for authentication. The default is **`admin`**.
6. **Password** — The password for the SPR access account for authentication. The default is **`admin`**.
7. **Module Name** — The module name to use for authentication. The default is **`Mediation`**.
8. **Key Transform Pattern** — A matching expression for filtering MDF routing to the SPR system.
9. When you finish, click **Save**.

The SPR Provisioning data source is configured.

Selecting Data Sources for MDF Devices

MDF devices determine whether a subscriber record is located on an Oracle Communications Subscriber Database Management (SDM) Oracle Communications User Data Repository (UDR), or a customer SPR system using matching rules based on the IMSI value. The rules apply globally to all MDF devices.

The selection algorithm is as follows:

- If no data source is selected, the MDF device writes data to the SDM or UDR, system.
- If one data source is selected, it is configured as either an Internal-SPR (SDM or UDR system) or an External-SPR (customer SPR system). The MDF device writes data to the SDM or UDR system when the IMSI matches an Internal-SPR data source. (It will not write data to an External-SPR data source.)
- If multiple data sources are selected, the MDF device writes data to an SPR system based on the rule with the longest IMSI prefix match.

To define a data source rule for MDF devices:

1. From the **Global Configuration** section of the navigation pane, select **Data Source Selection**.
   The **Data Source Selection Administration** page opens.
2. Define the following fields:
   a) **IMSI Prefix** — Enter an IMSI substring.
   b) **Datasource Type** — Select **Internal-SPR** (SDM or UDR system) or **External-SPR** (customer SPR system) from the pulldown list.
   c) **MPE Datasource** — Select the SPR device name from the pulldown list.
   d) **Prov Datasource** — Select the provisioning SPR device name from the pulldown list.
3. When you finish, click **Add**.
   The IMSI prefix is added to the IMSI Prefix list.
4. Repeat steps 2 and 3 as required.
   Additional rules are added to the IMSI Prefix list.
5. When you finish, click **Reapply Selections**.
   The rules are deployed to MDF and MPE devices.

To modify an existing rule, click the edit (pencil) icon to the right of the rule. The fields become editable. Make changes as necessary, click **Modify**, and click **Reapply Selections**.

To remove an existing rule, click the delete (trash can) icon to the right of the rule. A confirmation message displays. Click **OK** and then click **Reapply Selections**.

Mapping Fields

The attribute names of MDF SOAP requests must match field names in the SPR database. If the names differ, the request will fail. To support flexibility, the MDF system supports attribute mapping between SOAP interface attribute names and SPR database field names.

Each mapping includes the following:

- Unique name — A unique name for the mapping within the CMP database
- SOAP field — The name of the SOAP request attribute
- SDM field — The name of the SPR database field
- Description — Free-form text describing the mapping

To map fields:

1. From the **Mediation** section of the navigation pane, select **Mappings**.
   The content tree displays a list of mapping groups.
2. From the content tree, select the **SDM Mapping** group.
   The **SDM Mapping** page displays the mapping table.
3. On the **SDM Mapping** page, click **Modify**.
   The functions available from the embedded table are as follows:
4. Click **Add**.
   The **Add SDM Mapping** window opens.
5. Enter values for the fields **Unique Name**, **SOAP Field**, **SDM Field**, and (optionally) up to 255 characters in **Description**.

6. When you finish, click **OK**.
   The mapping is added to the table.
7. (Optional) Add, delete, modify. or reorder mappings.
   - 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. When you finish, 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. When you finish, 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.
8. When you finish, click **Save**.

The mappings are stored in the CMP database.

Table 28: Default Subscriber Field Mappings lists the subscriber field mappings supported by default in the MDF system.

Table 28: Default Subscriber Field Mappings

SOAP Attribute Name	SPR Field Name
ASOC	ASSOC
MDN	MSISDN
PID	NAI

Mapping Quotas

The quota provisioning request names in MDF SOAP requests must match quota profile names in the CMP database. If the names differ, the request will fail. To support flexibility, the MDF system supports quota mapping between SOAP interface quota request names and CMP quota profile names.

To map quotas:

1. From the **Mediation** section of the navigation pane, select **Mappings**.
   The content tree displays a list of mapping groups.
2. From the content tree, select the **Quota Mapping** group.
   The **Quota Mapping** page displays the mapping table.
3. Click **Modify**.
   The functions for mapping display.
4. Click **Add**.
   The **Add Quota Mapping** window opens.
5. Enter values for the following fields.
   - **Unique Name** — A unique name for the quota mapping within the CMP database.
   - **Category** — Select a category from the pulldown list. The options are **LIMIT**, **DATA_SVC**, **STYLE_A**, and **COUPON**.
   - **Name** — Enter the quota name used in the SOAP request and click **Add**; the name is added to the list. To remove a quota name, select it from the list and click **Delete**.
   - **Quota Profile Name** — Enter the quota profile from the list and click **Add**; the name is added to the list. To remove a quota profile name, select it from the list and click **Delete**.
   - **Quota Type** — Select the quota type (**quota**, **pass**, or **top-up**) from the pulldown list.
   - **Mid-month Registration** — Select if the quota supports mid-month registration.
   - **OPMD Sharable** — Select if the quota is shared as part of one person, multiple devices (OPMD).
   - **Priority** — Specifies a priority for the quota. Valid values are 1 – 255.
6. When you finish, click **OK**.
   The mapping is added to the table.
7. (Optional) Add, delete, modify. or reorder mappings.
   - 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. When you finish, 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. When you finish, 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.

8. When you finish, click **Save**.

The quota mappings are stored in the CMP database.

Chapter 16

System-Wide Reports

Topics:

System-Wide Reports describes the reports available on the function of Policy Management systems in your network. Reports can display platform alarms, network protocol events, and Policy Management application errors.

KPI Dashboard

The KPI Dashboard provides a multi-site system-level summary of performance and operational health indicators. The display includes indicators for:

- Offered load (transaction rate)
- System capacity (counters for active sessions)
- Inter-system connectivity
- Physical resource utilization (memory, CPU)
- System status
- Alarms
- Protocol errors

The KPI dashboard displays the indicators for all the systems on a single page, with each MRA KPIs in a separate table when MRA systems are managed by the CMP system or with all MPE KPIs in one table when MRA systems are not managed by the CMP system (that is, an MPE-only deployment). Each row within a table represents a single system (either an MPE or MRA server). The table cells are rendered using a color scheme to highlight areas of concern that is well adopted by the telecommunication industry. The table contents are periodically refreshed every 10 seconds; this time period is not configurable. The color changing thresholds are user configurable.

Figure 19: Example of KPI Dashboard with MRA Devices Managed by the CMP System illustrates the dashboard's contents when MRA systems are managed by the CMP system.

KPI Dashboard (Stats Reset: Interval / Last Refresh: 09/20/2013 11:59:27)

Filters | Change Thresholds

	Performance			Alarms			Protocol Errors	
	TPS	PDN	Active Subscribers	Critical	Major	Minor	Sent	Received
MRAs selected	40	6000	6000	0	0	0	0	0
MPEs selected	37	13262	13261	0	0	0	0	0

mra17-118	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-118(Server-A)	Standby				3	34								
mra17-118(Server-B)	Active	20 (0%)	3000 (0%)	3000 (0%)	4	46	3 of 4	2 of 2	1 of 4	0	0	0	0	0
MPE	State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
mpe17-111(Server-A)	Standby				4	37								
mpe17-111(Server-B)	Active	11 (0%)	3953 (0%)	3951 (0%)	4	60	2 of 2	0 of 0		0	0	0	0	0
mpe17-115(Server-A)	Active	7 (0%)	4810 (0%)	4811 (0%)	3	55	1 of 2	0 of 0		0	0	0	0	0

mra17-122	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra17-122(Server-A)	Standby				3	33								
mra17-122(Server-B)	Active	20 (0%)	3000 (0%)	3000 (0%)	3	46	2 of 3	2 of 2	1 of 4	0	0	0	0	0
MPE	State	TPS	PDN	Active Sessions	CPU %	Memory %	MRA	Data Sources		Critical	Major	Minor	Sent	Received
mpe17-116	Off-line	----	----	----	----	----	----	----		----	----	----	----	----
mpe17-117(Server-A)	Standby				4	39								
mpe17-117(Server-B)	Active	19 (0%)	4499 (0%)	4499 (0%)	4	60	2 of 2	0 of 0		0	0	0	0	0

Figure 19: Example of KPI Dashboard with MRA Devices Managed by the CMP System

The **MRAs selected** row displays the aggregation count for user-selected MRA devices. The **MPEs selected** row displays the aggregation count for the MPE devices that belong to the user-selected MRA devices.

The following counts are aggregated for selected MRA databases and the associated MPE devices:

- TPS
- PDNs
- Active Subscribers
- Critical Alarm Count
- Major Alarm Count
- Minor Alarm Count
- Protocol Errors Sent
- Protocol Errors Received

Note: Isolated MPE devices are not included in the aggregation counts.

When there are no MRA devices managed by the CMP system, the displayed headings are:

- Name of MPE
- Performance:
  - State
  - TPS
  - PDN
  - Active Sessions
  - CPU %
  - Memory %
- Connections
  - Data Sources
  - Network Elements
- Alarms
  - Critical
  - Major
  - Minor
- Protocol Errors
  - Sent
  - Received

In the top right corner there is a **Change Thresholds** button that allows you to change threshold settings used to determine cell coloring. When MRA devices are managed by the CMP system, a button on the top left corner lists each of the MRA devices with a checkbox that allows the user to enable/disable the table for that MRA device.

Individual servers are identified by name and the order in which they were defined within their cluster (Server-A, Server-B, Server-C). If any of these are set to Reverse Site Preference, then an “R” will appear by the server's State. For the standby or spare server, several columns are not populated (since those servers are not active); the only columns that contain data are: Status, CPU%, and Memory%. For Connections, Alarms, and Protocol Errors, the column's information is a hyperlink that will open a more detailed report.

If a monitored system is unreachable, or if the data is unavailable for some reason, then the status is set to `Off-line` and the values in all the associated columns is cleared. In this situation, the entire

row is displayed with the error color (red). If a monitored system does not support KPI retrieval then the status is set to N/A and the values in all the associated columns are cleared. No coloring is applied.

The columns that display information in the form of X (Y%) (e.g. TPS and PDN Connections"/"Sessions) correspond to the following: X represents the actual numeric value and Y represents the % of rated system capacity that is consumed.

The columns that display connection counts are displayed in the form X of Y where X is the current number of connections and Y is the configured number of connections. When X and Y are not the same, the column uses the warning color to indicate a connectivity issue, unless X is 0, in which case the error color is displayed.

The Alarm and Protocol Errors columns display the number of current events. If there are any Critical or Major alarms, then these cells will be colored red or yellow, respectively.

Note: To learn more about an alarm and how to resolve it, see the *Policy Management Troubleshooting Guide* for this release.

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

Mapping Display to KPIs

The following tables explain how each of the columns in the KPI dashboard are mapped to a specific statistic in the KPI statistics. On the initial KPI Dashboard window, KPIs for each MRA and MPE device are shown. Since the tables contain row entries for the active, standby and spare servers (if georedundancy is configured), the mapping is described for all three servers. *Table 29: KPI Definitions for MRA Devices* shows the mappings for MRA devices; *Table 30: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System* shows the mappings for MPE devices when the MRA devices are managed by the CMP system; and *Table 31: KPI Definitions for MPE Devices when MRA Devices are not Managed by CMP System* shows the mappings for MPE devices when the MRA devices are not managed by the CMP system.

Table 29: 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

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

Table 30: KPI Definitions for MPE Devices when MRA Devices are Managed by CMP System

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

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

Table 31: 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.

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

Table 32: Policy Statistics

Display	MPE	MRA	Name
Peg Count	Y	N	Policy Count
Evaluated	Y	N	Evaluated Count
Executed	Y	N	Executed Count
Ignored	Y	N	Ignored Count
Policy Details Stats			
Name	Y	N	Policy Name
Evaluated	Y	N	Eval Count
Executed	Y	N	Trigger Count
Ignored	Y	N	Ignore Count

Display	MPE	MRA	Name
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	(Data for each installed rule)

Table 33: 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 34: Diameter Application Function (AF) Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Conn Count
Currently OK peers	Y	Y	Peer Okay Count
Currently down/suspect/reopened peers	Y	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
AAR messages received/sent	Y	Y	AAR Recv Count\AAR Send Count
AAR Initial messages received/sent	Y	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR Modification messages received/sent	Y	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages received/sent	Y	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages received/sent	Y	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages received/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count

Display	MPE	MRA	Name
ASA success messages received/sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages received/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages received/sent	Y	Y	STR Recv Count\STR Send Count
STR messages timeout	Y	Y	STR Timeout Count
STA success messages received/sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages received/sent	Y	Y	STA Recv Failure Count\STA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
Cleanup ASA received	Y	Y	ASA Received Count
Cleanup ASR sent	Y	Y	ASR Sent Count
Current number of active sponsored sessions	Y	N	Current Sponsored Session Count
Max sponsored active sessions	Y	N	Max Sponsored Session Count
Current number of active sponsors	Y	N	Current Sponsor Count
Max number of sponsors	Y	N	Max Sponsor Count
Current number of active service providers	Y	N	Current Service Provider Count
Max number of service providers	Y	N	Max Service Provider Count
	Y	N	Current Emergency Session Count
	Y	N	Max Active Emergency Session Count

Table 35: Diameter AF Peer Stats (in Diameter AF Stats window)

Display	MPE	MRA	Name
ID	Y	Y	
IP Address: Port			

Display	MPE	MRA	Name
Currently active connections			
Currently active sessions			
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time

Table 36: Diameter Policy Charging Enforcement Function (PCEF) Statistics

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

Display	MPE	MRA	Name
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count
	Y	N	Current Emergency Session Count
	Y	N	Max Active Emergency Session Count

Table 37: Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Connections	N	Y	Conn Count
Currently OK peers	N	Y	Peer Okay Count
Currently down/suspect/reopened peers	N	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	N	Y	Msg In Count\Msg Out Count
CCR messages sent/received	N	Y	CCR Recv Count\CCR Send Count
CCA success messages recd/sent	N	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages sent/received	N	Y	CCR-I Recv Count\CCR-I Send Count
CCA-I success messages recd/sent	N	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	N	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages sent/received	N	Y	CCR-U Recv Count\CCR-U Send Count

Display	MPE	MRA	Name
CCA-U success messages recd/sent	N	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	N	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages sent/received	N	Y	CCR-T Recv Count\CCR-T Send Count
CCA-T success messages recd/sent	N	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	N	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages sent/received	N	Y	RAR Recv Count\RAR Send Count
RAA success messages recd/sent	N	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	N	Y	RAA Recv Failure Count\RAA Send Failure Count
ASR messages sent/received	N	Y	ASR Recv Count\ASR Send Count
ASA success messages recd/sent	N	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages recd/sent	N	Y	ASA Recv Failure Count\ASA Send Failure Count
Currently active sessions	N	Y	Active Session Count
Max active sessions	N	Y	Max Active Session Count

Table 38: Diameter Bearer Binding and Event Reporting Function (BBERF) Statistics

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

Display	MPE	MRA	Name
CCR-I messages received/sent	Y	Y	CCR-I Recv Count\CCR-I Send Count
CCR-I messages timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages received/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages received/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter BBERF connections	Y	Y	

Table 39: 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

Display	MPE	MRA	Name
Total messages in/out	Y	Y	Msg In Count\Msg Out Count
CCR messages received/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages received/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages received/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-U messages received/sent	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages received/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages received/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages received/sent	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages received/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages received/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages received/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages received/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages received/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
TSR messages received/sent	Y	Y	
TSA success messages received/sent	Y	Y	
TSA failure messages received/sent	Y	Y	
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count
Diameter TDF connections	Y	Y	

Table 40: Diameter Sh Statistics

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

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

Table 41: 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	

Display	MPE	MRA	Name
DBA-Q success messages received/sent	N	Y	
DBA-Q failure messages received/sent	N	Y	
DBR-QC messages received/sent	N	Y	
DBR-QC messages timeout	N	Y	
DBA-QC success messages received/sent	N	Y	
DBA-QC failure messages received/sent	N	Y	
DBR-U messages received/sent	N	Y	
DBR-U messages timeout	N	Y	
DBA-U success messages received/sent	N	Y	
DBA-U failure messages received/sent	N	Y	
DBR-T messages received/sent	N	Y	
DBR-T messages timeout	N	Y	
DBA-T success messages received/sent	N	Y	
DBA-T failure messages received/sent	N	Y	
DBR-S messages received/sent	N	Y	
DBR-S messages timeout	N	Y	
DBA-S success messages received/sent	N	Y	
DBA-S failure messages received/sent	N	Y	
RUR messages received/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages received/sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages received/sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages received/sent	Y	Y	LNRRecv Count\ LNRSend Count
LNR messages timeout	Y	Y	LNRTimeout Count

Display	MPE	MRA	Name
LNA success messages received/sent	Y	Y	LNARecv Success Count\ LNASend Success Count
LNA failure messages received/sent	Y	Y	LNARecv Failure Count\ LNASend Failure Count
LSR messages received/sent	Y	Y	LSRRecv Count\ LSRSend Count
LSR messages timeout	Y	Y	LSRTimeout Count
LSA success messages received/sent	Y	Y	LSARecv Success Count\ LSASend Success Count
LSA failure messages received/sent	Y	Y	LSARecv Failure Count\ LSASend Failure Count
SQR messages received/sent			
SQR messages timeout			
SQA messages received/sent			
SQA messages timeout			
Session found received/sent			
Session not found received/sent			
Diameter DRMA connections			

Note: The statistics listed in apply only to MRA devices.

Table 42: 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

Display	MPE	MRA	Name
RAA failure messages recd	N	Y	Release RAAs Received Failure
CCR-T messages processed	N	Y	Release CCRTs Received

Table 43: Diameter Sy Statistics

Display	MPE	MRA	Name
Connections	Y	N	Current Connections Count
Currently okay peers	Y	N	Peer Okay Count
Currently down/suspect/reopened peers	Y	N	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	Y	N	Messages In Count\Messages Out Count
SLR messages received/sent	Y	N	SLR Messages Received Count\SLR Messages Sent Count
SLR messages timeout	Y	N	SLRTimeout Count
SLA success messages received/sent	Y	N	SLA Success Messages Received Count\SLA Success Messages Sent Count
SLA failure messages received/sent	Y	N	SLA Failure Messages Received Count\SLA Failure Messages Sent Count
SNR messages received/sent	Y	N	SNR Messages Received Count\SMR Messages Sent Count
SNA success messages received/sent	Y	N	SNA Success Messages Received Count\SNA Success Messages Sent Count
SNA failure messages received/sent	Y	N	SNA Failure Messages Received Count\SNA Failure Messages Sent Count
STR messages received/sent	Y	N	STR Messages Received Count\STR Messages Sent Count
STR messages timeout	Y	N	STRTimeout Count
STA success messages received/sent	Y	N	STA Success Messages Received Count\STA Success Messages Sent Count
STA failure messages received/sent	Y	N	STA Failure Messages Received Count\STA Failure Messages Sent Count
Currently active sessions	Y	N	Active Sessions Count

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

Table 44: 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	

Display	MPE	MRA	Name
Max active sessions	Y	Y	
Messages with Authenticator field mismatch	Y	Y	
Last RADIUS message received time	Y	Y	
COA-request sent	Y	Y	CoA Request Count
COA-request received	Y	Y	
COA-ACK sent	Y	Y	CoA Ack Count
COA-ACK received	Y	Y	CoA Success Count
COA-NAK sent	Y	Y	
COA-NAK received	Y	Y	CoA Nck Count
Parsed under 100m(icro)s	Y	Y	
Parsed under 200m(icro)s	Y	Y	
Parsed under 500m(icro)s	Y	Y	
Parsed under 1m(illi)s	Y	Y	
Parsed over 1m(illi)s	Y	Y	
Total Parse Time	Y	Y	
Average Parse Time	Y	Y	
Maximum Parse Time	Y	Y	
Unknown BNG. Message dropped	Y	Y	Unknown Gateway Request Count
Unknown BNG. Account Start dropped	Y	Y	
Unknown BNG. Account Stop dropped	Y	Y	
Unknown BNG. Interim Update dropped	Y	Y	
Stale sessions deleted	Y	Y	
Stale sessions deleted due to missed Interim Update	Y	Y	
Stale sessions deleted on Account-On or Account-Off	Y	Y	
Invalid subscriber key. Message dropped	Y	Y	
Invalid subscriber identifier specified. Message dropped	Y	Y	Unknown Subscriber Request Count

Table 45: Diameter Latency Statistics shows information for these Diameter Statistics:

- Application Function (AF)
- Policy and Charging Enforcement Function (PCEF)
- Bearer Binding and Event Reporting (BBERF)
- Traffic Detection Function (TDF)
- Diameter Sh protocol
- Distributed Routing and Management Application (DRMA)
- Diameter Sy protocol

Table 45: Diameter Latency Statistics

Display	MPE	MRA	Name
Connections	Y	Y	Active Connection Count
Max Processing Time recd/sent (ms)	Y	Y	Max Trans In Time\ Max Trans Out Time
Avg Processing Time recd/sent (ms)	Y	Y	Avg Trans In Time\ Avg Trans Out Time
Processing Time recd/sent <time frame> (ms)	Y	Y	Processing Time [0-20] ms Processing Time [20-40] ms Processing Time [40-60] ms Processing Time [60-80] ms Processing Time [80-100] ms Processing Time [100-120] ms Processing Time [120-140] ms Processing Time [140-160] ms Processing Time [160-180] ms Processing Time [180-200] ms Processing Time [>200] ms

Table 46: 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 47: 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 48: 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 49: 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

Display	MPE	MRA	Name
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 50: Sh Data Source Statistics

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

Display	MPE	MRA	Name
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	

Display	MPE	MRA	Name
Time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Total Hit Time
Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Total Miss Time
Max Time spent on successful unsubscription (ms)	Y	N	Unsubscription Max Hit Time
Max Time spent on unsuccessful unsubscription (ms)	Y	N	Unsubscription Max Miss Time
Average time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Avg Hit Time
Average time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Avg Miss Time

Table 51: 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 52: KPI Interval Statistics

Display	MPE	MRA	Name
Interval Start Time	Y	Y	Interval Start Time
Configured Length (Seconds)	Y	Y	Configured Length (Seconds)
Actual Length (Seconds)	Y	Y	Actual Length (Seconds)
Is Complete	Y	Y	Is Complete
Interval MaxTransactions Per Second	Y	Y	Interval Max Transactions Per Second

Display	MPE	MRA	Name
Interval MaxMRABinding Count	Y	Y	Interval Max MRABinding Count
Interval MaxSessionCount	Y	Y	Interval Max Session Count
Interval MaxPDNConnectionCount	Y	Y	Interval Max PDNConnection Count

Color Threshold Configuration

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

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

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

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

Subscriber Activity Log

The CMP system can perform real-time tracing of Gx, Rx, SOAP, TCP provisioning, and Sh protocol messages for a subscriber from multiple MPE devices.

Subscriber tracing is activated using a global CMP system setting (see *Configuring the Activity Log*). After activation, traces for subscriber diameter application messages are merged from all MPE devices in the network to the CMP system. Messages are selected for tracing based on a subscriber identification. Allowable subscriber ID types are:

- IMSI
- MSISDN_E.164
- NAI
- UE IPv4/IPv6 address
- Session ID

Up to 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 in the **System Wide Reports** menu:

- View the subscriber activity log.
- Modify subscriber activity log settings. This task includes adding subscribers for tracing.
- View and modify the log backup settings.
- View the real-time subscriber activity log data display window.
- View the subscriber activity log history.

Subscriber Activity Log Limitations

The Subscriber Activity Log has the following limitations:

- Because of the additional processing required for the Subscriber Activity Log, only 20 subscribers can be enabled for logging.
- There is also a limit to the overall amount of data that can be recorded by the system.
- Most MRA messages are not shown in the log because MRA messages do not have user IDs or bindings for a secondary session and cannot be traced.
- CCR-U is rejected by Diameter validation as an invalid message. There is no correlation between the established session and this message.
- For UDR/UDA and CCA-T, use NAI, E164, or IMSI , not Ipv4 or Ipv6.

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. When you finish, 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. Add subscribers to the log in the **Subscriber Identifier List**:
   a) Click **Add**.
      The **Add Subscriber Identifier** window opens.
   b) Select the type of identifier and enter the name of the identifier:
      - **IMSI** (default) — International Mobile Subscriber Identity. Enter up to 15 Unicode digits.
      - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
      - **NAI** — Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters &*+0-9?a-z_A-Z{}!#$%'^/=` | ~-, optionally separated by a period (.). A valid realm name consists of the characters 0-9a-zA-Z- separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
      - **IPv4Address** — An IPv4 address in the standard dot format.
      - **IPv6Address** — An IPv6 address, in the standard 8-part colon-separated hexadecimal string format, and the subnet mask in CIDR notation from 0–128.
      - **SessionID** — A valid session ID. A valid session ID consists of the characters &*+0-9?a-z_A-Z{}!#$%'^/=` | ~-.
5. Select 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. When you finish, click **Save**.
9. (Optional) Add, edit, or delete subscribers.
   - Cloning an entry in the table
     1. Select an entry in the table.
     2. Click **Clone**. The **Clone** window opens with the information for the entry.
     3. Make changes as required.
     4. When you finish, 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. When you finish, click **Save**. The entry is updated in the table.
   - Deleting a value from the table

1. Select the entry in the table.
2. Click ✕**Delete**. A confirmation message displays.
3. Click **Delete** to remove the entry. The entry is removed from the table.

10. When you finish, 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 53: Status and Related Icons

Status	Icon	Condition
Running		Indicates the log is currently active (running). This status occurs when: • The **End Time** has not been reached or has just turned null. • **Enable** is selected.
Disabled		Indicates the log is not active. This status occurs when **Enable** is not selected and the **End Time** has not been reached.
Expired		Indicates the log is no longer active. This status occurs when the **End Time** is reached.

Configuring Subscriber Activity Log Backup Settings

To configure the subscriber activity logs backup settings:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens.
2. Select the **Log Backup Settings** tab.
3. Click **Modify**.
   The **Configuration** page opens.
4. Configure the log backup settings:
   a) Select **Enabled Subscriber Activity log Backup** to create a backup of the log.
   b) Set the start time for the backup. The date must be in the future. In the **First Running Time**, enter a date and time to start the backup in the format *mm/dd/yyyy hh:mm* (for example, **`01/01/2015 12:15`**).
   Alternatively, click (calendar) and select a date. When you finish, click **Enter**.
   c) In **Run Interval(hours)**, set the time between backup runs. Valid values are from 1 to 99,999. The default is 24 hours.

d) In **Max Keep Days**, set the maximum number of day to keep the log. Valid values are from 1 to 60. The default is 60 days.
e) In **Folder Max Size(MB)**, set the maximum size of the backup storage folder. The default is 16000 MB.

5. When you finish, click **Save**.

You have defined and saved the Subscriber Activity Log configuration.

Editing a Subscriber Identifier

To edit a subscriber identifier:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**.
   The **Subscriber Activity Log Settings** page opens.
2. Click **Modify**.
   A new **Subscriber Activity Log Settings** page opens, containing fields for configuring the log.
3. In the **Subscriber Identifier List** section, select a subscriber and identifier and click **Edit**.
   The **Edit Subscriber Identifier** window opens.
4. Edit the identifier.
5. When you finish, 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; use the Ctrl or Shift keys to select multiple subscribers. Click **Delete**.
   A confirmation message displays.
4. Click **Delete** to delete the subscriber identifier(s).
   The subscriber identifier or identifiers are removed from the list.

You have deleted one or more subscriber identifiers.

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** drop-down list to display messages that appear during a specific time period.
- Select a message type from the **Activity Type** drop-down list to filter messages in the window by message type. The message types are:
  - **All** (default)
  - **Gx**
  - **Rx**
  - **GxLite**
  - **Gxx**
  - **Gy**
  - **Sd**
  - **Sh**
  - **Sy**
  - **LDAP**
  - **Policy**
  - **MDF Provisioning**
  - **SPR Provisioning**
  - **MGW Provisioning**

  .
- Enable or disable the **Automatic Scroll** checkbox. When enabled, the output scrolls in the window. When disabled, the window does not scroll, and new messages are added at the bottom of the window.
- Click **Pause** to temporarily keep messages from being added to the window. If selected, the button changes to **Resume**. Click **Resume** for new real-time data to be added to the window.

  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.

Viewing Subscriber Activity Log History

To view the activity log history for subscribers:

1. From the **System Wide Reports** section of the navigation pane, select **Subscriber Activity Log**. The **Subscriber Activity Log Settings** page opens in the work area.
2. Click **Activity Log History**.
   The **Subscriber Activity Log History Log** window opens, displaying the activity log.
3. Filter the display by using one or more of the following criteria and clicking **Filter**:
   - Start Date

Note: If the trace start date and end date are both entered, then the window displays the logs that occur between the two time points.

- End Date
- Identifier Type
- Identifier Value
- Activity Type
- Server
- Contains Text

A filtered view of the history displays.

From the log window you can optionally do the following:

- Click a message summary to display the content for the selected message in the bottom pane of the window.
- Click **Reset** to reset the filter conditions to their defaults. The log is refreshed to show all messages.
- Click **Export** to export the filtered trace logs data into a text file. The traced messages are exported in descending order according to the time stamp.

Viewing the Trending Reports

To view the trending reports, from the **System Wide Reports** section of the navigation pane, select **Trending Reports**.

The navigation pane displays the four trending reports. The reports display separate aggregate MPE and MRA statistics in graph tables.

The trending report columns display the following data:

- **MRA Binding Count** — The number of bindings (for example, UE or Policy rules and charge function MPE pairs) which are maintained in the MRA system.

  Note: A binding is the MPA routing information. The UE stores the user identity UE NAI, UE IP addresses, the selected MPE identity IP-CAN session, and APN if it is available.

- **PDN Connection Count** — The number of PDN connections that communicate to the Diameter network elements.
- **Session Count** — The number of Diameter sessions (for example, Gx or Gy) which are maintained in the MPE device.
- **Transaction Per Second** — The number of Diameter requests and answer pairs processed in a second.

Viewing MRA Binding Count

The MRA binding count determines the number of MRA bindings between user equipment (UE) and MPE devices maintained in the MRA system. This is recorded by the counter MaxMRABindingCount.

To view the MRA Binding Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
   The content tree displays a list of trending reports.

2. From the content tree, select **MRA Binding Count**.
   The **MRA Binding Count** page displays the MRA Binding Count graph.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph.
- **Search Filter** — You can specify which MRA devices are graphed (all or specific devices) and which counters to graph (all or binding counts for MRA devices, which for this report is the same thing). You can also specify the graph parameters:
  - **Start Date & Time** — The start date and time for the graph. Click (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration** — Displays the time duration of the data. A pulldown list provides the following options:
    - **24 hours** (the default)
    - **2 days**
    - **3 days**
    - **4 days**
    - **5 days**
    - **6 days**
    - **7 days**
  - **Show Aggregation** — If you check this box, the aggregated data for all MRA devices is displayed in the graph.
- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_MRA Binding Count.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing PDN Connection Count

This report plots the counter Interval MaxPDNConnectionCount for each managed MPE and MRA device.

To view the PDN Connection Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
   The content tree displays a list of trending reports.
2. From the content tree, select **PDN Connection Count**.
   The **PDN Connection Count** page displays the PDN Connection Count MRA and policy server (MPE device) graphs.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph table.

- **Search Filter** — You can specify which MPE and MRA devices are graphed (all or specific devices) and which counters to graph (all, PDN connections for MPE devices, or PDN connections for MRA devices). You can also specify the graph parameters:
  - **Start Date & Time** — The start date and time for the graph. Click (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration** — Displays the time duration of the data. A pulldown list provides the following options:
    - **24 hours** (the default)
    - **2 days**
    - **3 days**
    - **4 days**
    - **5 days**
    - **6 days**
    - **7 days**
  - **Show Aggregation** — If you check this box, the aggregated data for all selected MPE or MRA content is displayed in the graph.
- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_PDN Connection Count.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing Session Count

The session counts determine the number of Gx or Gy sessions maintained in the MPE device, graphed over time periods equal to the KPI interval length (by default 15 minutes). The session count is recorded by the counter MaxSessionCount.

To view the Session Count trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
   The content tree displays a list of trending reports.
2. From the content tree, select **Session Count**.
   The **Session Count** page displays the Session Count for policy server (MPE) device graph.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph.
- **Search Filter** — You can specify which MPE devices are graphed (all or specific devices) and which counters to graph (all or session counters for MPE devices, which for this report is the same thing). You can also specify the graph parameters:
  - **Start Date & Time** — The start date and time for the graph. Click (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.

- **Duration** — Displays the time duration of the data. A pulldown list provides the following options:
  - **24 hours** (the default)
  - **2 days**
  - **3 days**
  - **4 days**
  - **5 days**
  - **6 days**
  - **7 days**

  Note: The durations available depend on the settings of the OM Statistics scheduled task.
- **Show Aggregation** — If you check this box, the aggregated data of all selected MPE content is displayed in the graph.

- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_Session Count.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Viewing Transaction Per Second

Transactions per second is defined as the number of Diameter request or Diameter answer pairs processed in a second, graphed over time periods equal to the KPI interval length (by default 15 minutes). Transactions are recorded by the counter MaxTransactionsPerSecond.

To view the Transaction Per Second trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
   The content tree displays a list of trending reports.
2. From the content tree, select **Transaction Per Second**.
   The **Transaction Per Second** page displays the Transaction Per Second graph.

The following report options are available:

- **Refresh** — You are provided with the most recently updated graph.
- **Search Filter** — You can specify which Policy Management devices are graphed (all or specific devices) and which counters to graph (all or TPS for each class of Policy Management device). You can also specify the graph parameters:
  - **Start Date & Time** — The start date and time for the graph. Click (calendar icon) to select or enter the year, month, day, and time. The graph uses after the set duration.
  - **Duration** — Displays the time duration of the data. A pulldown list provides the following options:
    - **24 hours** (the default)
    - **2 days**
    - **3 days**

    - **4 days**
    - **5 days**
    - **6 days**
    - **7 days**
  - **Show Aggregation** — If you check this box, the aggregated data for all selected devices is displayed in the graph.

- **Settings** — The table parameters are displayed; click **Run** to generate the graph.
- **Printable Format** — The most recently updated graph is displayed in a separate window.
- **View Raw Data** — The interval data statistics are displayed in a separate window.
- **Export CSV** — A comma-separated value (CSV) file named `Export_Transaction Per Second.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **View Summary** — The distribution of data (average, minimum, and maximum) of the interval statistics for each device are displayed in a separate window.

Custom Trending Reports

Along with the four pre-configured trending reports, you can create custom trending reports based on one or more counters.

The following statistics are associated with the MPE server type:

- AFRatTypeStats
- DiameterAfLatencyStats
- DiameterBberfLatencyStats
- DiameterBberfStats
- DiameterCTFStats
- DiameterDrmaLatencyStats
- DiameterDrmaStats
- DiameterPcefLatencyStats
- DiameterPcefStats
- DiameterShLatencyStats
- DiameterShStats
- DiameterSyLatencyStats
- DiameterSyStats
- DiameterTdfLatencyStats
- DiameterTdfStats
- IntervalStats
- KpiStats
- PDNConnectionAPNStats
- PdnRatTypeStats
- PolicyStats

The following statistics are associated with the MRA server type:

- DiameterMraAfLatencyStats
- DiameterMraAfStats
- DiameterMraBberfLatencyStats

- DiameterMraBberfStats
- DiameterMraCtfStats
- DiameterMraDraStats
- DiameterMraDrmaLatencyStats
- DiameterMraDrmaStats
- DiameterMraPcefLatencyStats
- DiameterMraPcefStats
- DiameterMraTdfLatencyStats
- DiameterMraTdfStats
- IntervalMraStats
- KpiMraStats

After creation, customized trending reports appear in the **Trending Reports** list following the pre-configured Trending Reports in alphabetical order.

Creating a Custom Trending Report

To create a custom trending report:

1. From the **System Wide Reports** section of the navigation pane, select **Trending Reports**.
   The **Trending Report Definition Administration** page opens.
2. Click **Create Trending Report Definition**.
   A new **Trending Report Definition Administration** page opens, containing fields for configuring a customized trending report (*Figure 20: Trending Report Definition Configuration Page* shows a sample).

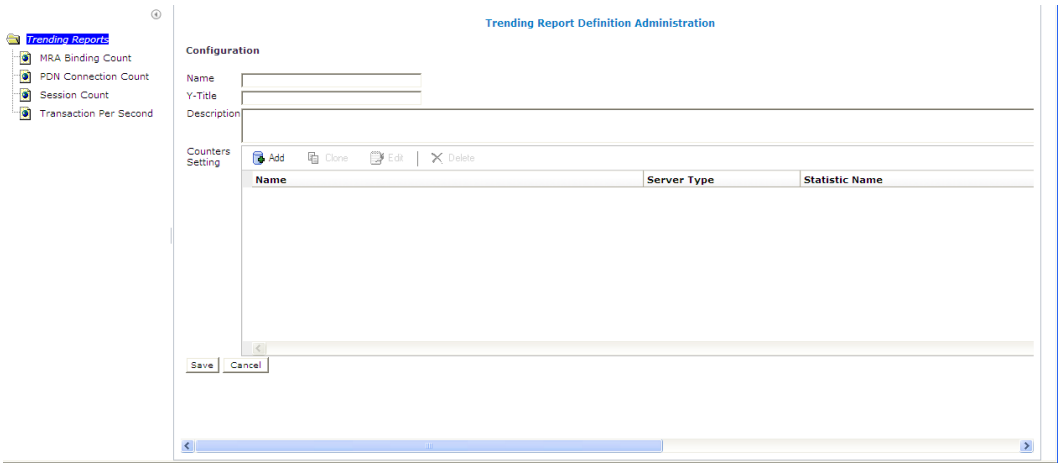


Figure 20: Trending Report Definition Configuration Page

3. Enter the following information for the new trending report:
   a) **Name** — The name of the trending report.
      The name can contain up to 255 characters, cannot contain double quotes or commas, and cannot begin or end with a space.
   b) **Y-title** — The title of the Y series.
      The title can contain up to 40 characters and cannot begin or end with a space.

c) **Description** — The description of the trending report.
The description can contain up to 250 characters and cannot begin or end with a space.

4. Add counters to the report:
   a) Click **Add** next to the **Counters Setting** field.
   The **Add Stats Definition** popup opens.
   b) Enter a name for the counter in the **Name** field.
   The name can contain up to 40 characters, cannot contain double quotes (") or commas (,), and cannot begin or end with a space.
   c) Select the server type from the **Server Type** list.
   d) Select a statistic from the **Statistic Name** list.
   After selecting a statistic, all counters supported by that statistic populate the **Counter Name** list.
   e) Select a counter from the **Counter Name** list.
   f) Click **Save** to add the counter to the **Counters Setting** list.
   You have added a single counter to the trending report. You can continue to add individual counters to the report, using this step. You can also add counters by cloning an existing counter (described in the following step).
5. (Optional) Add, edit, or delete reports.
   - Cloning an entry in the table
     1. Select an entry in the table.
     2. Click **Clone**. The **Clone** window opens with the information for the entry.
     3. Make changes as required.
     4. When you finish, 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. When you finish, click **Save**. The entry is updated in the table.
   - Deleting a value from the table
     1. Select the entry in the table.
     2. Click **Delete**. A confirmation message displays.
     3. Click **Delete** to remove the entry. The entry is removed from the table.
6. When you finish, 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 timestamped alarm notifications for Policy Management systems. The display is refreshed every ten seconds and appears in the upper right corner of all CMP pages. Alarms remain active until they are reset.

The Active Alarms report provides details about active alarms. To view the Active Alarms report:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.
   The **Alarms** section expands to show the available alarm reports.
2. Select **Active Alarms**.

The **Active Alarms** report opens in the work area.

Figure 21: Sample Active Alarms Report shows a sample active alarm report.

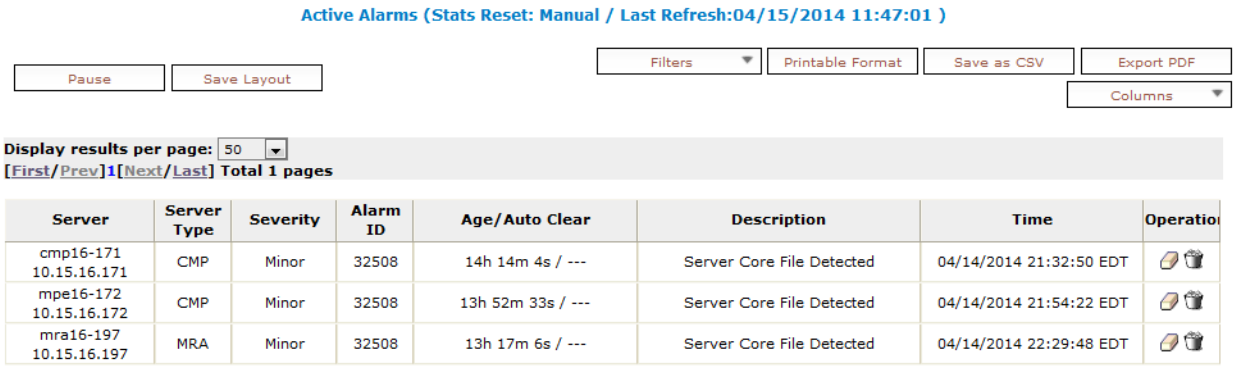


Figure 21: Sample Active Alarms Report

The alarm levels are as follows:

- **Critical** — Service is being interrupted. (Critical alarms are displayed in red.)
- **Major** — Service may be interrupted if the issue is not corrected. (Major alarms are displayed in orange.)
- **Minor** — Non-service affecting fault. (Minor alarms are displayed in yellow.)

Notifications, which have a severity of Info, are not displayed in the Active Alarms report, but are written to the trace log. For more information, see *Viewing the Trace Log*.

Note: Alarms generated by Policy Management systems running software before V7.5 are mapped to these levels as follows: Emergency or Critical map to Critical; Alert or Error map to Major; Warning or Notice map to Minor.

The Age/Auto Clear column shows how long an alarm has been active (that is, how long since it was raised) and how long the alarm will display before being automatically cleared. The Auto Clear time is shown as `---` if the alarm is not automatically cleared.

The following options are available:

- To sort the report on any column, click the column title.
- To display online help for an alarm, click its ID.
- To hide an alarm, click the hide icon (), located to the right of each row. All instances of alarms with that ID reported from that server are hidden from display (but shown in the Hidden Filter, which you can use to restore the display of those alarms).

  Note: Hiding an alarm only affects the current user. Other users will see the alarm if they display the **Active Alarms** page.

- To manually clear an alarm, click the clear icon (trash can), located to the right of each row. You are prompted, `This alarm will be cleared. Are you sure?` Click **OK**.
- To pause the display of alarms, click **Pause**. To resume the display, click **Refresh**.
- To select what information is displayed, click **Columns** and select from the pulldown list.
- To control what alarms and alarm classes are displayed on the page, click **Filters** and select from the pulldown menu:

- The **Search Filter** tab has three controls. The **Server** control lets you display alarms from all servers (the default) or a specific server. The **Server Type** control lets you display alarms from all Policy Management products (the default) or just **CMP**, **MRA**, or **MPE** systems. The **Severity** control lets you display alarms of all severities (the default), critical and major alarms, critical alarms, major alarms, or minor alarms.
- The **Hidden Filter** tab shows alarms, by server and alarm ID, that are currently hidden from display. Click the delete icon, to the right of an entry, to remove it from the list of hidden items and display it in the page again.

- To save your formatting changes to the report page, click **Save Layout**.
- **Printable Format** — The current alarms are displayed in a separate window.
- **Save as CSV** — A comma-separated value (CSV) file named `report.csv` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.
- **Export PDF** — A Portable Document Format (PDF) file named `report.pdf` is generated, suitable for a spreadsheet application, and a standard **File Download** window opens, so you can save or open the file.

Viewing the Alarm History Report

The Alarm History Report displays historical alarm information.

To view the alarm history report:

1. From the **System Wide Reports** section of the navigation pane, select **Alarms**.
   The **Alarms** section expands to show the available alarm reports.
2. Select **Alarm History Report**.
   The Alarm History report opens.

   Note: If you are using Internet Explorer, the window appears behind the main window.

   The window displays up to 50,000 alarms, sorted by age.

   Note: If you wish to view the most recent alarms, and there are more than 50,000 alarms in the database, specify a start date/time that includes the present.

3. To view older alarms, reduce the number of alarms displayed, or locate a specific alarm or group of alarms, you can define filtering criteria using the following fields:
   - **Start Date** — Filter out alerts before a specific date/time. Click the calendar icon to specify a date/time.
   - **End Date** — Filter out alerts after a specific date/time. Click the calendar icon to specify a date/time.
   - **Severity** — Filter alerts by severity level; select a level (the default is **All**) from the list.
   - **Cluster or Server** — Select the cluster or server within the cluster whose alarms you want to view.
   - **Active Alarms** — Select to view only active alarms; the default is to display both active and cleared alarms.
   - **Aggregate** — Select to aggregate alarms that have the same IP address, alarm ID, and severity. (This function is limited to 50,000 alarms.)
4. After entering filtering information, click **Filter** to refresh the display with the filtering applied.
   The alarm list is filtered.

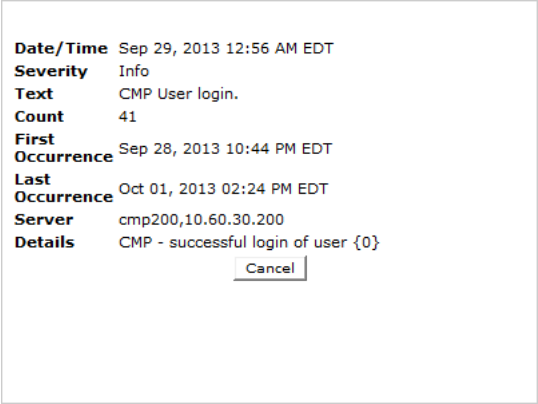
5. When you finish, click **Close** to close the window.

Alarms contain the following information:

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

  Note: Alarms generated by Policy Management systems running software before V7.5 are mapped to these levels as follows: Emergency or Critical map to Critical; Alert or Error map to Major; Warning or Notice map to Minor.
- **Alarm ID** — When clicked, the alarm ID provides online help information.
- **Text** — User-readable text of the alert.
- **OAM VIP** — OAM IP address in IPv4 or IPv6 format.
- **Server** — Name and IP address, in IPv4 or IPv6 format, or FQDN of the device from which this alarm was generated.

To view alert details, click (binoculars icon), located to the right of the alert. A window displays additional information; for example:



Click **Cancel** to close the window.

Viewing Session Reports

To view the session reports, from the **System Wide Reports** section of the navigation pane, select **Sessions**.

The navigation pane displays the available session reports.

Viewing the AF Session Report

The application function (AF) session report shows information on the current and maximum number of AF sessions for each specific radio access technology type (RAT-Type) for each MPE device.

The following RAT-Types are supported:

- WLAN (0) — Wireless local area network
- VIRTUAL (1) — Virtual network
- UTRAN (1000) — Universal Terrestrial Radio Access Network
- GERAN (1001) — GSM EDGE Radio Access Network
- GAN (1002) — Generic Access Network
- HSPA_EVOLUTION (1003) — High Speed Packet Access Evolution
- EUTRAN (1004) — Evolved UTRAN
- CDMA2000_1x (2000)
- HRPD (2001) — High Rate Packet Data
- UMB (2002) — Ultra Mobile Broadband
- EHRPD (2003) — Enhanced HRPD

To view the AF session report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **AF Session Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The available columns are the following:

- **Associated MRA** — The MRA device managing this device, or N/A if no MRA device is managing this device. (If your CMP system is not configured to manage MRA devices, this option is not available.)
- **Server Name** — The name defined for the server.
- **Server Type** — Either **MPE** or **MRA**. All MPE devices managed by an MRA device are displayed together, followed by a row for that MRA device that represents the total counts for all MPE devices managed by that MRA device. Any MRA devices not managed by an MRA device are displayed after the last configured MRA device.
- **WLAN - Current** — The current number of WLAN connections to this device.
- **WLAN - Max** — The highest number of WLAN connections recorded to this device.
- **Virtual - Current** — The current number of Virtual connections to this device.
- **Virtual - Max** — The highest number of Virtual connections to this device.
- **UTRAN - Current** — The current number of UTRAN connections to this device.
- **UTRAN - Max** — The highest number of UTRAN connections recorded to this device.
- **GERAN - Current** — The current number of GERAN connections to this device.
- **GERAN - Max** — The highest number of GERAN connections recorded to this device.
- **GAN - Current** — The current number of GAN connections to this device.

- **GAN - Max** — The highest number of GAN connections recorded to this device.
- **HSPA_EVOLUTION - Current** — The current number of HSPA_EVOLUTION connections to this device.
- **HSPA_EVOLUTION - Max** — The highest number of HSPA_EVOLUTION connections recorded to this device.
- **EUTRAN - Current** — The current number of EUTRAN connections to this device.
- **EUTRAN - Max** — The highest number of EUTRAN connections recorded to this device.
- **CDMA2000_1X - Current** —The current number of CDMA2000_1X connections to this device.
- **CDMA2000_1X - Max** — The highest number of CDMA2000_1X connections recorded to this device.
- **HRPD - Current** — The current number of HRPD connections to this device.
- **HRPD - Max** — The highest number of HRPD connections recorded to this device.
- **UMB - Current** — The current number of UMB connections to this device.
- **UMB - Max** — The highest number of UMB connections recorded to this device.
- **EHRPD - Current** — The current number of EHRPD connections to this device.
- **EHRPD - Max** — The highest number of EHRPD connections recorded to this device.

The first row in the table displays the total for all configured MRA devices.

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (the default), server totals only, or one specific server.
- **Server Type** — Filter in all server types (the default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA** — Filter in all MRA devices (the default), totals only, or one specific MRA device. (If your CMP system is not configured to manage MRA devices, this option is not available.)

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; an **AF Session Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the PDN Connection Report

The PDN Connection Report shows information on the current and maximum number of packet data network (PDN) connections for each specific radio access technology type (RAT-Type) for each MPE device.

The following RAT-Types are supported:

- WLAN (0) — Wireless local area network
- UTRAN (1000) — Universal Terrestrial Radio Access Network
- GERAN (1001) — GSM EDGE Radio Access Network
- GAN (1002) — Generic Access Network

- HSPA_EVOLUTION (1003) — High Speed Packet Access Evolution
- EUTRAN (1004) — Evolved UTRAN
- CDMA2000_1x (2000)
- HRPD (2001) — High Rate Packet Data
- UMB (2002) — Ultra Mobile Broadband
- EHRPD (2003) — Enhanced HRPD
- UNKNOWN (-1)

To view the PDN Connection report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **PDN Connection Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The available columns are the following:

- **Associated MRA** — The MRA device managing this device, or N/A if no MRA device is managing this device. (If your CMP system is not configured to manage MRA devices, this option is not available.)
- **Server Name** — The name defined for the server.
- **Server Type** — Either **MPE** or **MRA**. All MPE devices managed by an MRA device are displayed together, followed by a row for that MRA device that represents the total counts for all MPE devices managed by that MRA device. Any MRA devices not managed by an MRA device are displayed after the last configured MRA device.
- **WLAN - Current** — The current number of WLAN connections to this device.
- **WLAN - Max** — The highest number of WLAN connections recorded to this device.
- **UTRAN - Current** — The current number of UTRAN connections to this device.
- **UTRAN - Max** — The highest number of UTRAN connections recorded to this device.
- **GERAN - Current** — The current number of GERAN connections to this device.
- **GERAN - Max** — The highest number of GERAN connections recorded to this device.
- **GAN - Current** — The current number of GAN connections to this device.
- **GAN - Max** — The highest number of GAN connections recorded to this device.
- **HSPA_EVOLUTION - Current** — The current number of HSPA_EVOLUTION connections to this device.
- **HSPA_EVOLUTION - Max** — The highest number of HSPA_EVOLUTION connections recorded to this device.
- **EUTRAN - Current** — The current number of EUTRAN connections to this device.
- **EUTRAN - Max** — The highest number of EUTRAN connections recorded to this device.
- **CDMA2000_1X - Current** —The current number of CDMA2000_1X connections to this device.
- **CDMA2000_1X - Max** — The highest number of CDMA2000_1X connections recorded to this device.
- **HRPD - Current** — The current number of HRPD connections to this device.
- **HRPD - Max** — The highest number of HRPD connections recorded to this device.
- **UMB - Current** — The current number of UMB connections to this device.

- **UMB - Max** — The highest number of UMB connections recorded to this device.
- **EHRPD - Current** — The current number of EHRPD connections to this device.
- **EHRPD - Max** — The highest number of EHRPD connections recorded to this device.
- **UNKNOWN - Current** — The current number of connections of unclassified type to this device.
- **UNKNOWN - Max** — The highest number of connections of unclassified type recorded to this device.

The first row in the table displays the total for all configured MRA devices.

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (the default), server totals only, or one specific server.
- **Server Type** — Filter in all server types (the default), totals only, MPE devices only, or MRA devices only.
- **Associated MRA** — Filter in all MRA devices (the default), totals only, or one specific MRA device. (If your CMP system is not configured to manage MRA devices, this option is not available.)

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **PDN Connection Count Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the PDN APN Suffix Report

The PDN APN suffix report shows information on PDN connection counts per access point name (APN) suffix.

To view the PDN APN suffix report, from the **System Wide Reports** section of the navigation pane, select **Sessions** and then select **PDN APN Suffix Report**.

The display is refreshed automatically every ten seconds. To hold the current values, click **Pause**. To resume, click **Refresh**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The available columns are the following:

- **APN** — The access point name.
- **Server Name** — The server name.
- **Server Type** — Either **MPE** or **MRA**.

- **Current** — The current number of PDN connection counts for each suffix that have been matched on each server.
- **Max** — The highest number of PDN connection counts for each suffix that have been matched on each server.

The first row in the table displays the total values for all configured servers.

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

- **APN** — Filter in all APN suffixes (default), all PDN connections without a configured APN suffix match (OtherAPNs), or APN suffix totals only.
- **Server Name** — Filter in all servers (default), server totals only, or one specific server.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **PDN APN Suffix Statistics Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing Other Reports

To view the miscellaneous reports:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select the report to view.

The navigation pane displays the available reports.

Viewing the Connection Status Report

The connection status report provides an aggregate view of connections maintained by managed Policy Management systems. The display is refreshed every ten seconds.

To view the connection status report, from the **System Wide Reports** section of the navigation pane, select **Others** and then select **Connection Status**.

Figure 22: Sample Connection Status Report shows a sample connection status report.

Connection Status (Stats Reset: Interval / Last Refresh: 06/10/2013 17:31:46)

Pause | Save Layout | Columns | Filters | Printable Format | Save as CSV | Export PDF

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	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter PCEF	normal	06/10/2013 10:34:03 EDT	15	1	872	872	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter BBERF	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter TDF	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	mra17-38.camiant	Diameter CTF	normal	06/10/2013 10:34:03 EDT	15	1	0	0	0	0
mpe17-79	MPE	ggsn1	---	down	N/A	---	---	---	---	---	---

Figure 22: Sample Connection Status Report

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The available columns are the following:

- **Server** — name of the associated system
- **Server Type** — **MPE** (Multimedia Policy Engine) or **MRA** (Policy Front End)
- **Remote Identity** — the Diameter ID (if known) or IP address of the remote system
- **Type** — the type of connection
- **Status** — the status of the connection (the possible values are protocol-specific)
- **Up/Down Since** — the timestamp when the connection reached its current state (N/A if the connection has never been established)
- **# Total Connect** — the number of times that the connection has been re-established

  Note: This counter is reset if the cluster is restarted.

- **# Active Connect** — the number of active connections

  Note: This counter is reset if the cluster is restarted.

- **Msgs Sent** — the number of Diameter or RADIUS protocol messages that have been sent to the remote system
- **Msgs Received** — the number of protocol messages that have been received from the remote system
- **Errors Sent** — the number of protocol error messages that have been sent to the remote system
- **Errors Received** — the number of protocol error messages that have been received from the remote system

If a connection is in a non-functional state, the row is displayed in red; if a connection is in a transitional state between functional and non-functional (including when a connection is being established), the row is displayed in yellow.

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

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

- **Type** — Filter in all remote device types (the default) or one specific device type: **Diameter AF**, **Diameter PCEF**, **Diameter BBERF**, **Diameter TDF**, **Diameter SH**, **Diameter CTF**, or **Diameter DRMA**.
- **Status** — Filter in all remote device status values (the default) or one specific status: **down**, **normal**, or **reopen**.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **Connection Status Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the Protocol Errors Report

The protocol errors report provides an aggregate view of connection errors, with one row for each distinct error code or sub-code. The display is refreshed every ten seconds.

To view the protocol errors report, from the **System Wide Reports** section of the navigation pane, select **Others** and then select **Protocol Errors**.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The following columns are available:

- **Server** — name of the associated system
- **Server Type** — **MPE** or **MRA**
- **Remote Identity** — the Diameter ID (if known) or IP address of the remote system
- **Error** — the protocol error
- **# Received** — the number of protocol errors received from the remote system
- **# Sent** — the number of protocol errors sent to the remote system

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

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

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **Connection Status Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Viewing the Policy Statistics Report

The policy statistics report provides an aggregate view of policy statistics, with one row for each policy, letting you gauge the performance of individual policies. The display is refreshed every ten seconds.

To view the policy statistics report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
   The list of available reports displays in the navigation pane.
2. Select **Policy Statistics Report**.
   The Policy Statistics report opens.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The following columns are available:

- **Server Name** — Name of the associated system
- **Server Type** — Either **MPE** or **MRA**
- **Policy Name** — The name of each policy defined and active on the displayed server
- **Evaluated** — The number of times the displayed policy was evaluated for the displayed server
- **Executed** — The number of times the displayed policy was executed for the displayed server
- **Ignored** — The number of times the displayed policy was ignored by the displayed server
- **Total Execution Time (ms)** — The total execution time for each policy, in milliseconds
- **Average Execution Time (ms)** — The average amount of time it takes a policy to execute, in milliseconds
- **Maximum Execution Time (ms)** — The maximum execution time for each policy, in milliseconds

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

- **Server Name** — Filter in all servers (the default) or one specific server.
- **Policy Name** — Filter in all policies (the default) or one specific policy.

You can save formatting changes to the report page. Click **Save Layout**.

You can display the report in a format suitable for printing. Click **Printable Format**; a **Policy Statistics Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

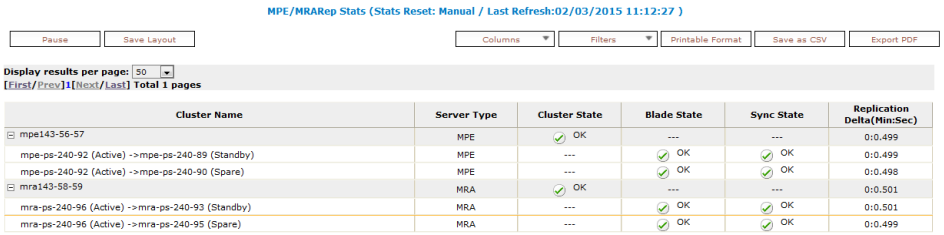
Viewing the MPE/MRA Replication Statistics Report

The MPE/MRA replication statistics report provides a view of database replication statistics, with one row for each replication path in an MPE or MRA cluster. The display is refreshed every ten seconds.

To view the replication statistics report:

1. From the **System Wide Reports** section of the navigation pane, select **Others**.
2. Select **MPE/MRA Rep Stats**.

Figure 23: Sample MPE/MRA Replication Statistics Report shows a sample replication report.



Cluster Name	Server Type	Cluster State	Blade State	Sync State	Replication Delta(Min:Sec)
mpe143-56-57	MPE	OK	---	---	0:0.499
mpe-ps-240-92 (Active) ->mpe-ps-240-89 (Standby)	MPE	---	OK	OK	0:0.499
mpe-ps-240-92 (Active) ->mpe-ps-240-90 (Spare)	MPE	---	OK	OK	0:0.498
mra143-58-59	MRA	OK	---	---	0:0.501
mra-ps-240-96 (Active) ->mra-ps-240-93 (Standby)	MRA	---	OK	OK	0:0.501
mra-ps-240-96 (Active) ->mra-ps-240-95 (Spare)	MRA	---	OK	OK	0:0.499

Figure 23: Sample MPE/MRA Replication Statistics Report

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To pause the display, click **Pause**. To resume the display, click **Refresh**.
- To save the any formatting changes in the page, click **Save Layout**.
- To display another page of the report, click the page number.

You can customize what information is displayed by controlling which table columns appear, using the **Columns** pulldown menu. The following columns are available:

- **Cluster Name** — the name of the cluster and the blades participating in replication as well as their high availability (HA) states.
- **Server Type** — the type of cluster being utilized (**MPE** or **MRA**).
- **Blade State** — displays the state of the blade replicating with the current active blade.

Table 54: 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

Blade Ha State	Value Displayed in the Report	Icon Used in the User Interface
Out of Service	Critical	Red X
Unknown	Critical	Red X

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

Table 55: Sync State Values in MPE/MRA Replication Stats Report

Sync Status	Description	Value Displayed on the CMP	Icon Used in the User Interface
Down	The link is down and there is no current attempt to restore it.	Critical	Red X
DownListening	The incoming link is down awaiting the other side to initiate the connect attempt.	Critical	Red X
Down Connecting	The link is down by this side is trying to connect.	Critical	Red X
DownRejected	The link is down because a connect attempt was rejected in the handshake phase.	Critical	Red X
Down Handshake	The link is connected but not ready for application use (so it is down logically). The links is being validated in a handshake as legitimate.	Critical	Red X
Connected	Connected and ready for use.	Critical	Red X
Connected Reinit	Connected and ready for use, but after an application error where the recovery is start over without either a link drop or a complete application restart.	Critical	Red X
Connected Incompat	Connected but the schema are incompatible and replication cannot run until (1) the schema has the needed upgrade information or (2) problematic tables are excluded from replication.	Critical	Red X
RegisterSent	RegisterSent means the link is exchanging application level credentials and information (such as data dictionary information). In this state, registration has been sent from one side and it is being awaited from the other side.	Critical	Red X
RegisterAcked	In this state, registration has been sent acknowledged from the other side. In most configurations, it is a 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

Sync Status	Description	Value Displayed on the CMP	Icon Used in the User Interface
Inhibited	Inhibited means the link administrative state is inhibited (or disabled), but the applications have exchanged registration messages.	Major	Red Exclamation Mark
AuditWait	The audit is awaiting an `OK to proceed` message from the remote side.	Critical	Red X
AuditQueue	The audit is queued because a limit on the number of simultaneous audits.	Critical	Red X
Audit	Audit means the application is bringing the databases into agreement. It does so by comparing each table one-by-one, and then applying database updates since the audit began.	Major	Red Exclamation Mark
Active	Active means the link is in the normal active steady-state conditions where updates are being transferred to the slave database(s) with a normal and acceptable delay.	OK	Green Check Mark
ActiveBehind	ActiveBehind is the same as Active but the slave database is unacceptably behind for whatever reasons. After an audit, it would be typical to be in the ActiveBehind state until any queued updates are applied to the slave database.	Major	Red Exclamation Mark
ActiveSwitch	A switchover is being attempted without an audit if the states of the databases allow it.	Major	Red Exclamation Mark
ActivePost Audit	The database is coherent but has not caught back up to current after the preceding audit.	Major	Red Exclamation Mark

- **Cluster State** — represents the overall state of the cluster. The Cluster State Column is an aggregation of the Blade State and Sync State columns. The value for the Cluster State is selected based on the maximum severity.

Table 56: Priority Table in MPE/MRA Replication Stats Report

Priority	Value	Icon Used in the User Interface
1	Critical	Red X
2	Major	Red Exclamation Mark
3	Minor	Warning Sign
4	OK	Green Check Mark

You can filter results by controlling which table rows appear, using the **Filters** pulldown menu. You can define filtering criteria using the following fields:

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

You can display the report in a format suitable for printing. Click **Printable Format**; an **MPE/MRA Rep Status Report** window opens.

You can save the report in comma-separated value (CSV) format, suitable for importing into a spreadsheet application. Click **Save as CSV**. A file named `report.csv` is generated, and a standard **File Download** window opens, so you can save or open the file.

You can save the report as a Portable Document Format (PDF) file, suitable for storage or online display. Click **Export PDF**. A file named `report.pdf` is generated, and a standard **File Download** window opens, so you can save or open the file.

Chapter 17

Upgrade Manager

Topics:

The Upgrade Manager allows you to manage upgrade ISOs and perform software upgrades on servers in the topology. During the upgrade process, the **System Maintenance** page displays the upgrade status. Access to these GUI options can be restricted by user role; see *Managing Users* for more information.

For specific steps on performing an upgrade, contact My Oracle Support. See see *My Oracle Support (MOS)* for how to contact My Oracle Support.

About Preparing for an Upgrade

Upgrading a server requires a large amount of preparation. Detailed information about preparing for an upgrade is available at the My Oracle Support website.

CAUTION

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

About ISO Files on Servers

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

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

ISO Maintenance Elements

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

There are three types of elements that appear on the **ISO Maintenance** page: Checkboxes to select servers on which to perform operations, the table of filtered servers, and pulldown menus (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for performing operations. The following list describes all of these elements.

Table 57: ISO Maintenance Elements

Element	Description
☐ (checkbox)	Use this column to select the servers on which an operation is to be performed. If you select a main cluster server, all servers in that cluster are selected. **Note:** At least one server must be selected before you can select an operation from the **Operations** menu.
Name	Displays the server names of all filtered servers. When a server is downloading an ISO file, a special download icon appears next to the name.

Appl Type	Displays the type of application running on each server. The **Filters** menu lets you select the following servers: • **CMP Site1 Cluster** • **CMP Site2 Cluster** • **MPE** • **MRA** • **Mediation Server** • **All** .
IP	Displays the OAM server IP address of each server. The **Filters** menu lets you select only a server with a specific IP address or **All** servers.
Running Release	Displays the current Policy Management software release of each server. The **Filters** menu lets you display a specific release only or **All** releases.
ISO	Displays the ISOs or CD-ROM on each server. Use the checkbox to select the ISO to delete during the Delete ISO operation.
Columns	Use the **Columns** pulldown menu to change the columns that appear in this table. By default, all columns appear. To change which columns appear, uncheck the columns to be removed from the page. The Name column is mandatory.
Filters	Use the **Filters** pulldown menu to select a subset of servers to appear on this page. On this menu are the following filter submenus: • **Appl Type** • **IP** • **Running Release** These filters are set to **All** by default, so all servers appear initially. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	Use the **Operations** menu to select an ISO operation to perform. **Note:** The servers on which the operation is being performed must be selected (in the first column of the table) before that or any operation can be selected. The operations that appear in the menu depend on the state of the servers that are selected; that is, when more than one server is selected, only the operations that are available on all of these servers appear. Possible operations are: • **Push Script** • **Upload ISO** • **Delete ISO** As a protective feature, when a command is executed, a warning message pops up, asking if you are sure you want to execute this operation. When **OK** is clicked, a progress bar displays the status of the command completion in a pop-up window. **Note:** Once the operation is confirmed, it cannot be cancelled.

Viewing the ISO Status of Servers

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

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

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

Pushing a Script to a Server

Before starting this procedure, you must mount the ISO file manually and copy three upgrade scripts to `/opt/camiant/bin` on the CMP system:

- `policyUpgrade.pl`
- `policyUpgradeHelper.pl`
- `qpSSHKeyProv.pl`

Use this procedure to push upgrade scripts to the remote servers receiving a software upgrade. This procedure is required before a software upgrade can occur on a server. An error message displays in the Upgrade Status column until this procedure is complete.

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

The upgrade scripts are downloaded to the selected servers.

Adding an ISO File to a Server

Before adding an ISO file to a server, ensure that only the required ISO is in the directory `/var/TKLC/upgrade` for every server in the cluster.

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

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
   The **ISO Maintenance** page opens.
2. Select the servers to receive the ISO file.
3. Click **Operations** and select **Upload ISO**.
   An upload window opens.
4. Enter the following information for the ISO file:

Option	Description
Mode	Mode used to transfer file to remote servers. Currently, SCP is available.
ISO Server Hostname/IP	Enter the name or address of the server receiving the ISO file. This field is required.
User	Enter your user name. This field is required.
Password	Enter your password. This field is required.
Source ISO file full path	Enter the location where the ISO file is to be stored on the remote server. This field is required.

5. Click **Add** (or **Back** to abandon your request).
   The transfer process begins to the selected servers. A download icon appears in the Name column for the servers receiving the ISO file during the file transfer process. A progress bar displays during the operation. Once the process completes, the icon disappears.

The ISO file is distributed to the servers.

Deleting an ISO File from a Server

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

1. From the **Upgrade** section of the navigation pane, select **ISO Maintenance**.
   The **ISO Maintenance** page appears.
2. Select the servers.
3. Select the ISO file on the servers that is being removed.
4. Click **Operations** and select **Delete ISO**.
   A confirmation message displays.
5. Click **OK**.
   A progress bar displays the progress of this operation.

The selected ISO files are deleted from the selected remote servers.

About the Upgrade Manager

On the **Upgrade** menu, **Upgrade Manager** is an option. The Upgrade Manager is reserved for future use. Do not use the Upgrade Manager to upgrade a Policy Management system.

About Performing an Upgrade

The information in this section is a general overview of the Upgrade Manager steps you take to upgrade an individual server. Specific details, including the order in which systems are upgraded, are provided by My Oracle Support. See *My Oracle Support (MOS)* for more information.

CAUTION

Caution: Once you begin an upgrade, any changes you make to the configuration during the process (such as creating or editing network elements or policies) may be lost. Subscriber tracing conditions and logs are not preserved. The Subscriber Activity log does not support tracing across mixed-mode systems (that is, systems running different versions of Policy Management software).

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

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

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

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

1. Log in to the active server of the primary-site CMP cluster as **`root`**. The system displays the root-level prompt (**#**).
2. Enter the command **`mount -o loop /var/TKLC/upgrade/`*`iso_name`*` /mnt/upgrade`** (where *iso_name* is the name of the ISO file). The ISO file is mounted.
3. Enter the following commands:

   ```
   cp /mnt/upgrade/upgrade/policyScripts/policyUpgrade.pl /opt/camiant/bin
   ```

   ```
   cp /mnt/upgrade/upgrade/policyScripts/policyUpgradeHelper.pl
   /opt/camiant/bin
   ```

   ```
   cp /mnt/upgrade/upgrade/policyScripts/qpSSHKeyProv.pl /opt/camiant/bin
   ```

   Script files are copied to the target directory on the active server.
4. Enter the command **`umount /mnt/upgrade`**. The ISO file is unmounted.
5. Enter the command **`qpSSHKeyProv.pl --prov --user=admusr`**. SSH keys are provisioned on the active server.

   Note: This step is always required. You need to enter the **`admusr`** password.
6. Enter the command **`logout`**. You are logged out of the active server.
7. Select the forced standby server of the primary-site cluster and apply **Start Upgrade** to begin the upgrade process on that server.
8. Select the primary site and apply **Switch ForceStandby** to make the standby server active and the active server standby. You are logged out of the CMP system.
9. Log in to the CMP system, select the forced standby server, and apply **Start Upgrade** to begin the upgrade process on that server.
10. Select the forced standby server and apply **Cancel Force Standby** to make it active (and the active server standby).

To upgrade an MDF, MPE, or MRA cluster:

1. Select the active server of the cluster and apply **Turn Off Replication** to stop replication traffic.
2. Select the standby server of the cluster and apply **Force Standby**.
3. Select the forced standby server of the cluster and apply **Start Upgrade** to begin the upgrade process on that server.
4. Select the cluster and apply **Switch ForceStandby** to make the standby server active and the active server standby.

5. Select the cluster and apply **Reapply Configuration** (see *Reapplying the Configuration to Policy Management Devices*) to distribute configuration information to it.
6. Select the forced standby server and apply **Start Upgrade** to begin the upgrade process on that server.
7. Select the forced standby server of the cluster and apply **Turn On Replication** to restart replication traffic.
8. Select the standby server and apply **Cancel Force Standby** to make it active (and the active server standby).

Once all servers in all clusters of the Policy Management network are upgraded, select each server and apply **Upgrade Completion**.

System Maintenance Elements

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

There are three types of elements that appear on the **System Maintenance** page:

- Checkboxes to select servers/ISOs on which to perform operations.
- Table of filtered servers.
- Pulldown menus (**Columns**, **Filters**, and **Operations**) for changing what displays in the table and for performing operations.

Table 58: System Maintenance Elements describes all of the elements.

Table 58: System Maintenance Elements

Element	Description
(checkbox)	Use the checkbox column to select the servers on which an operation is to be performed. If you select a main cluster server, all servers in that cluster are selected. **Note:** At least one server must be selected before you can select an operation from the **Operations** list.
Name	Displays the server name of each server. When a server is in the process of being upgraded, a special upgrade icon appears next to the name. Likewise, if a server upgrade has failed, a special failed icon appears next to the name. If current information on a server is unavailable, a (synch broken icon) appears next to the name.
Appl Type	Displays the type of Policy Management application running on each server. The **Filters** list allows you to display **CMP Site1 Cluster**, **CMP Site2 Cluster**, **MPE**, **MRA**, **Mediation Server**, or **All**.
IP	Displays the IP address of each server. The **Filters** list allows you to display only the server with a specific IP address or All servers.

Element	Description
Server State	Displays the state of each server. The server state can appear in different colors, depending on the state displayed. The **Filters** list allows you to display the following states: • **Active** • **Standby** • **Out-Of-Service** • **Force Standby** • **All** (default)
ISO	Displays the ISOs or CD-ROM on each server. Use the checkbox to select an ISO to use during an upgrade on that server.
Prev Release	Displays the previous Policy Management software release of each server, if known. The **Filters** list allows you to display a specific release only or **All** releases.
Running Release	Displays the current Policy Management software release of each server. The **Filters** list allows you to display a specific release only or **All** releases.
Replication	Displays whether replication is On or Off.
Upgrade Status	Displays details of last upgrade performed on each server.
Columns	Use the **Columns** list to change the columns that appear on this page. By default, all columns appear. To change which columns appear, uncheck the columns to be removed from the page. The Name column is mandatory.
Filters	Use the **Filters** list to select a subset of servers to appear on this page. On this menu are the following filter submenus: • **Appl Type** • **IP** • **State** • **Prev Release** • **Running Release** These filters are set to **All** by default, so all servers appear initially. Selecting another option from one or more of these filters reduces the number of servers displayed.
Operations	Use the **Operations** list to select an upgrade operation to perform. **Note:** At least one server must be selected before you can select an operation from the **Operations** list. The operations that appear in the list depend on the state of the servers that are selected. In other words, when more than one server is selected, only the operations that are applicable to all selected servers appear. See *Table 59: System Maintenance Operations* for the possible operations. As a protective feature, when a command is executed, a warning message displays, asking if you are sure you want to execute this operation. When

Element	Description
	you **OK**, a progress bar displays the status of the command completion in a pop-up window. **Note:** Once the operation is confirmed, it cannot be cancelled.

Table 59: System Maintenance Operations

Operation	Description
Push Script	Pushes script to remote server. Upgrade Manager uses the script to communicate with the remote server and to perform the upgrade or backout.
Upload ISO	Adds ISO to the specified Policy Management products.
Force Standby	Forces the selected server(s) into standby status. CAUTION **Caution:** Setting Force Standby for all servers in a cluster effectively removes the cluster from service. **Note:** You cannot force both servers of a CMP cluster into Standby status.
Prepare Upgrade	Turns off COMCOL replication of database tables.
Upgrade Completion	Turns off legacy replication.
Undo Upgrade Completion	Prepare for a backout of a software upgrade. This process turns on legacy replication for all the clusters.
Switch ForceStandby	Switches the upgraded server to active and the previously active server to forced standby in order to upgrade it.
Cancel Force Standby	Cancels the Force Standby status.
Start Upgrade	Begins the upgrade with selected ISO on each server.
Accept Upgrade	Removes backout information. Once the upgrade is accepted for any server in a cluster, the cluster cannot be rolled back. The status of the server must be Force Standby and the upgrade status must be Pending. Clears alarm 32532 (Upgrade Pending Accept/Reject). If the upgrade results in a conversion of the file system, the server restarts. **Note:** If a server fails after an upgrade is accepted, you must accept the upgrade again for the replacement server.
Backout	Initiates a backout on the selected server(s).

Viewing Upgrade Status of Servers

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

1. From the **Upgrade** section of the navigation pane, select **System Maintenance**.

The **System Maintenance** page appears.

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

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

About Rolling Back an Upgrade

It is possible to roll back, or back out, the Policy Management software to the previous version in a production environment.

Note: Before beginning a rollback, contact My Oracle Support and inform them of your plans.

Before backing out a Policy Management upgrade, remove all new feature advanced device settings. (See *Configuring Advanced Device Settings* for more information.)

CAUTION

Caution: Any Gx or Rx sessions created on version 9.7.3 MPE systems will be lost after backout to version 9.7.2.

For a complete Policy Management deployment, the sequence of backing out an upgrade is the reverse of installing the upgrade:

1. Back out one or several MPE clusters
2. Back out MRA clusters
3. Back out any remaining MPE clusters
4. Back out MDF clusters
5. Back out CMP clusters
6. Reapply the configuration to MDF, MPE, and MRA systems

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

The procedure for rolling back a CMP cluster is different from the procedure for rolling back other Policy Management clusters.

Rolling Back an Upgrade

To roll back an MDF, MPE, or MRA cluster:

1. Select the standby server of the cluster and apply **Turn Off Replication** to turn off replication on that server.
2. Select the standby server of the cluster and apply **Force Standby**.
3. Select the forced standby server of the cluster and apply **Backout** to begin the rollback process on that server.
4. Select the cluster and apply **Switch ForceStandby** to make the standby server active and the active server standby.

5. Select the forced standby server and apply **Backout** to begin the rollback process on that server.
6. Select the active server of the cluster and apply **Turn On Replication** to turn on replication for that server.
7. Select the forced standby server and apply **Cancel Force Standby** to make it active (and the active server standby).

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 **Replication** column shows **On**.

Rolling Back a CMP Cluster

If you are rolling back an entire Policy Management network, you must roll back aCMP cluster last. This rollback procedure is different from the rollback procedure for other clusters.

Note: You cannot begin this operation until all other Policy Management clusters are rolled back.

Note: Before beginning a rollback, contact My Oracle Support and inform them of your plans.

To roll back a CMP cluster:

1. Select the standby server of the cluster and apply **Force Standby**.
2. Select the forced standby server of the cluster and apply **Backout** to begin the rollback process on that server.
3. Select the cluster and apply **Switch ForceStandby** to make the standby server active and the active server standby.
4. Select the forced standby server and apply **Backout** to begin the rollback process on that server.
5. Select the forced standby server and apply **Cancel Force Standby** to make it active (and the active server standby).

The CMP cluster is rolled back to the previous release.

Chapter 18

Global Configuration

Topics:

This section describes how to configure the global settings in the CMP system.

Defining Global Configuration Settings

This section describes how to configure global CMP settings.

Setting the Precedence Range

When overlapping policy and charging control (PCC) quality of service (QoS) rules apply to the same Gx or Gxx Diameter session, precedence is applied to determine which rule is installed on the gateway. In the case of an overlap, the rule with the lower precedence value is installed. Some vendor gateways require unique precedence, or else reject rules. You can configure MPE devices to maximize the probability that all rules have unique PCC rule precedences. This is a global configuration setting that affects all MPE devices managed by this CMP system.

Note: This does not guarantee rule precedence uniqueness. Operator-defined rules are not validated to ensure precedence uniqueness; if you define such rules, you must track their precedence values yourself.

To set the precedence range, do the following:

1. From the **Global Configuration** section of the navigation pane, select **Global Configuration Settings**.
   The content tree displays a list of global configuration settings.
2. From the content tree, select the **Precedence Range** group.
   The **Precedence Range Configuration** page opens in the work area.
3. Click **Modify**.
   The fields become editable.
4. Enter values for the configuration attributes:
   a) **AF-Triggered** — Enter the minimum and maximum values for rules triggered by Rx requests. The default range is 400 to 899.
   b) **UE-Triggered** — Enter the minimum and maximum values for rules triggered by user equipment-initiated resource requests. This range cannot overlap with the AF range. The default range is 1000 to 1999.
   c) **Default Session** — If no other rules are installed when a Gx eHRPD, E-UTRAN, or GPRS session is established, a default rule is installed. Enter the default session precedence. The default precedence is 3000.
5. When you finish, click **Save**.

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 values in the following ranges:

- 0–399
- 900–999
- 2000–2999
- 3001–4,294,967,295

Range changes do not automatically cause deployed rules to be redeployed with new precedence values. Also, range changes do not automatically cause revalidation of defined traffic profiles.

When traffic profiles are imported, they are imported regardless of their configured precedence values. The CMP system displays a message reminding you to check the precedence values of the imported traffic profiles. See *Importing an XML File to Input Objects* for more information.

Setting UE-Initiated Procedures

When enabled, this feature allows an MPE device to trap UE-Init resource modification requests and reject them using the specified parameters. This feature applies to Gx and Gxx (Gxa, Gxc) interfaces.

To enable or disable processing of UE-Initiated procedures or to change configuration attributes:

1. From the **Global Configuration** section of the navigation pane, select **Global Configuration Settings**.
   The content tree displays a list of global configuration settings.
2. From the content tree, select the **UE-Initiated Procedures**.
   The **UE-Initiated Procedures** page opens in the work area group.
3. Click **Modify**.
   The **Modify UE-Initiated Procedures** page opens.
4. Enter values for the configuration attributes:
   a) **Reject UE-Initiating Request** — Select to enable this feature to reject UE-Initiated resource modification requests gracefully, or leave unchecked to process normally with no impact (by ignoring specific AVPs relevant to the UE-Initiated procedure request). The default is unchecked (disabled).
   b) **Experimental Result Code** — Enter the numeric value that is returned in the Experimental-Result-Code AVP as part of the CCA message (if no configured code exists). Enter an integer between 0 and 2,147,483,647. The default value is 5144.
   c) **Experimental Result Code Name** — Enter the description of the error that is returned in the Experimental-Result-Code AVP as part of the CCA message. Enter a string value up to 255 characters in length. The default name is DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED.
   d) **Experimental Result Code Vender Id** — Enter the vender ID that is included in the Experimental-Result-Code AVP as part of the CCA message. Enter an integer between 0 and 2,147,483,647. The default ID is 10415.
   e) **Experimental Result Code Vendor Name** — Enter the vender name that is included in the Experimental-Result-Code AVP as part of the CCA message. Enter a string value up to 255 characters in length. The default name is 3GPP.
5. When you finish, click **Save**.

The UE-initiated attributes are configured.

Setting Stats Settings

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

CAUTION

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

To change stats settings, do the following:

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

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

     When in Interval mode, numeric values are reset at regular intervals, controlled by the Stats Collection Period variable. During Interval mode, a reset occurs on the hour and then every 5, 10, 15, 20, 30 or 60 minutes afterwards, depending on the value selected in **Stats Collection Period**, providing a better idea of the performance of the Policy Management system at specific times of day. The default value is Manual.
5. Set the **Stats Collection Period**. When **Stats Reset Configuration** is set to Interval, specify the time interval after which stats are written to the Policy Management devices from the pulldown menu. Options are minutes.
   - 5
   - 10
   - 15 (default)
   - 20
   - 30
   - 60
6. When you finish, 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 **Modify Quota Settings** page opens.

4. Enter values for the configuration attributes:
   a) **Enable subscriber pools** — The global configuration setting for a pooled quota is enabled if the box is checked.
   b) **Enable pooled quota usage tracking** — This allows you to have both individual quota usage tracking and pool quota usage tracking occurring simultaneously.
   c) **Enable pooled entity state** — A defined policy which allows you to update individual entity states and/or pool entity states.

   Note: A subscriber can only be associated with one pool.

5. When you finish, 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 pulldown list. The default is **Enable**.
   c) **Preemption Vulnerability** — Defines whether a service data flow can lose the resources assigned to it so that a service data flow with a higher priority level can be admitted. Select **Enable** or **Disable** from the pulldown list. The default is **Disable**.
5. When you finish, click **Save**.

The eMPS ARP Settings attributes are configured.

Setting PDN APN Suffixes

Access point name (APN) suffix matching on the MPE device is performed by reading the APN suffixes configured on the CMP system. An APN is considered a match based on the longest suffix it has in common after a case-insensitive comparison.

The MPE device dynamically creates a new stats object the first time it receives a new APN suffix match for a PDN connection. Once it is created, each new PDN connection for that APN updates the current object. If a stats object has not been created for an APN suffix, the stats object is not displayed in the APN reports page.

If the MPE device receives a PDN connection without a configured APN suffix match, then the connection is added to a stats object called OtherAPN.

PDN connections per APN suffix are shown in the PDN APN suffix report. See *Viewing the PDN APN Suffix Report* for more information.

Up to 25 different APN suffixes can be configured. Each suffix is limited to 64 characters.

To configure PDN APN suffixes:

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**. The content tree displays a list of global configuration settings.
2. From the content tree, select the **PDN APN Suffixes** folder.
   The **PDN APN Suffix Administration** page opens in the work area, listing the configured PDN APN suffixes.
3. Click **Create PDN APN Suffix**.
4. Enter the following values:
   a) **Name** — Enter the name of the APN suffix.
   b) **Value** — Enter a value for the APN suffix.
   c) **Description** — Enter descriptive text.
5. When you finish, click **Save**.

The PDN APN suffix is created.

Configuring the Activity Log

The Activity Log allows the real-time tracing activity of Gx, SOAP, TCP provisioning, Sh, and Rx protocol messages to be performed for a specific subscriber from multiple MPE devices.

After activation, traces for subscriber protocol messages are merged from all MPE devices in the network to the CMP system. Messages are selected for tracing based on subscriber identification.

Up to 60 subscriber IDs can be configured in the subscriber configuration window with tracing enabled or disabled. Tracing can be enabled for up to 20 subscribers.

After tracing is enabled, the following associated tasks can be performed:

- Modify subscriber tracing configuration settings and add subscribers for tracing
- Activate and deactivate trace log backup
- View and export historical trace log data
- View and export real-time trace data for up to 10 subscribers

See *Subscriber Activity Log* for information on performing these tasks.

To enable subscriber tracing, do the following:

1. From the **Global Configuration** section of the navigation pane, select **Global Configuration Settings**.
   The content tree displays a list of global configuration settings.
2. From the content tree, select **Activity Log Configuration**.
   The **Activity Log Configuration** page opens in the work area.
3. Click **Modify**
   The fields become editable.
4. Enter the number of subscribers for which tracing can be performed in the **Max Subscriber Trace Count** field. The subscriber trace count can be a value of 1 to 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. When you finish, 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 DIAMERTER.ENF.AFDirectReply setting on a per APN basis.

When the DIAMERTER.ENF.AFDirectReply setting is set to true, all Rx processing can be synchronous for specific APNs.

The **Custom APNs Configuration** display has three screens:

- **Synchronous APNs**
- **Session Recovery APNs**— allows a session recovery.
- **Session Synch APNs**—allows you to enable/disable Gx Session-Sync on a per APN per MPE basis.

1. From the **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
2. From the content tree, select the **Custom APNs Configuration** folder.
3. Click **Modify**.
4. Managing Synchronous APNs
   a) On the **Custom APNs Configuration** page, select the **Synchronous APNs** section.
   b) Enter a **Synchronous APN** (for example, `xyz1.oracle.com`).
   c) Click **Add** to add the new APN to the list. To delete an APN, highlight the APN in the list and click **Delete**.
   d) Click **Save**.
5. Managing 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 recover APN. To delete a Session Recovery APN, highlight the APN in the list and click **Delete**.
6. Adding a Session Synch APN
   a) On the **Custom APNs Configuration** page, select the **Session Synch APNs**section.

b) Enter a **Session Synch APN**.
c) Click **Add**. To delete a Session Synch APN, highlight the APN in the list and click **Delete**.

Defining the Data Source Selection

Defining the Data Source Selection describes how to associate data sources with a subscriber, using the IMSI for the subscriber. Associating the subscriber with the data source also associates the subscriber with the relevant SPRs. The association is created on the CMP GUI, then distributed to the MPE devices. For more information, see *Message Distribution Function Reference*.

Chapter 19

System Administration

Topics:

System Administration describes functions reserved for CMP system administrators.

Note: Some options are visible only when you are logged in with administrative rights to the CMP system. However, the **Change Password** option is available to all users.

Configuring System Settings

Within the CMP system you can define the settings that control system behavior.

To define system settings:

1. From the **System Administration** section of the navigation pane, select **System Settings**.
   The **System Settings** page opens in the work area, displaying the current system settings.
2. Click **Modify**.
   The **System Settings** page opens.
3. In the **Configuration** section, define the following:
   a) **Idle Timeout (minutes; 0=never)** — The interval of time, in minutes, that a session is kept alive.

      The default value is 30 minutes; a value of zero indicates the session remains active indefinitely.

   b) **Account Inactivity Lockout (days; 0=never)** — The maximum number of days since the last successful login after which a user is locked out.

      If the user fails to log in for the defined number of days, the user is locked out and cannot gain access to the system until an administrator resets the account. The default value is 21 days; a value of zero indicates no limit (the user is never locked out for inactivity).

   c) **Maximum Concurrent Sessions Per User Account (0=unlimited)** — The maximum number of times a defined user can be logged in simultaneously. A value of zero indicates no limit.

      If more than the configured number of concurrent users try to log in (for example, a second user if this value is set to 1), they are blocked at the login page with the message `Your account already has the maximum number of concurrent sessions`.

   d) **Password Expiration Period (days; 0=never)** — The number of days a password can be used before it expires. Enter a value from 7 to 365, or 0 to indicate that the password never expires.
   e) **Password Expiration Warning Period (days; default=3)** — The number of days before a password expires to begin displaying a window to users after login warning that their password is expiring.
   f) **Admin User Password Expiration** — By default, the password for the admin user never expires.

      If you select this option, the **admin** user is subject to the same password expiration policies as other users.

   g) **Block users when password expires** — By default, once a password expires, the user must immediately change it at the next login.

      If you select this option, if their password expires, users cannot log in at all. (If you select **Admin User Password Expiration** and the **admin** user's password expires, the user can still log in but must immediately select a new password.)

   h) **EMS Shared Secret**— Field provided to support third-party single sign-on architectures.
   i) **Minimum Password Length** — The minimum allowable length in characters for a password, from 6 to 64 characters.

      The default is six characters.

   j) **Login Banner Title** — The title that displays at the top of the login page. The default is **`Welcome`**. You can enter up to ten 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 GUI menu. Default value is 0.

4. In the **Invalid Login Threshold** settings section, define the following:

   a) **Enable** — Enables login threshold control.

   By default, this feature is enabled; clear the check box to disable this feature.

   b) **Invalid Login Threshold Value** — Defines the maximum number of consecutive failed logins after which action is taken.

   Enter a value from 1 through 500; the default is 3 attempts.

   c) **Action(s) upon Crossing Threshold** — The system action to take if a user reaches the invalid login threshold:

   - **Lock user** — prevents users from logging in if they reach the invalid login threshold.
   - **Send trace log message** — If a user account reaches the threshold, an incident is written to the trace log, including the username and the IP address (in IPv4 or IPv6 format) from which the login attempts were made. The default level is **Warning**; to change the event level, select a different level from the list.

5. The **Password Strength Settings** section lists four character categories: lowercase letters, uppercase letters, numerals, and non-alphabetic characters. You can specify a password strength policy that requires users to create passwords by drawing from these categories:

   - **Require at least categories below** — By default, this setting is 0 (disabled). Select it to require users to include password characters from between one to four of the categories.
   - **Require at least lower-case letter(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 lowercase letters in their passwords.
   - **Require at least upper-case letter(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 uppercase letters in their passwords.
   - **Require at least numeral(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 numerals in their passwords.
   - **Require at least non-alphabetic character(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 nonalphabetic characters in their passwords.
   - **Force users with weak password to change password at their next login** — By default, this setting is 0 (disabled). Select it to require users to conform to a new password policy effective the next time they log in.

6. When you finish, click **Save**.

The system settings are configured.

Figure 24: Sample Password Strength Policy shows an example of settings that establish a password strength policy requiring user passwords to contain at least one uppercase letter, four numerals, and one non-alphabetic character. (A password that would satisfy this policy is P@ssword1357.) Users whose passwords do not meet these requirements will be forced to change their passwords the next time they log in.

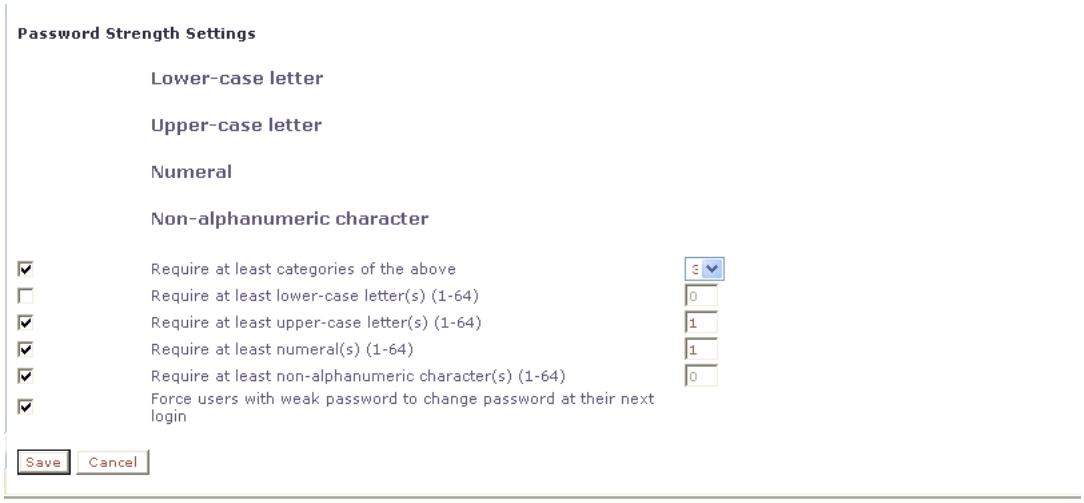


Figure 24: Sample Password Strength Policy

Importing and Exporting CMP Configurable Objects

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

Using the OSSI XML Interface

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

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

The OSSI XML interface includes the following:

- **Topology Interface** — Allows you to query and manage network elements within the system
- **Operational Measurements (OM) Interface** — Allows you to retrieve statistical data from the system
- **AVP definitions** — Allows you to define, save, and restore third-party AVP definitions within the system
- **Policy Tables** — Allows you to export policy tables, and import them to add, edit, replace or delete a table

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

Importing an XML File to Input Objects

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

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

Oracle recommends that you export the existing database of objects before starting an importation operation to ensure that you can recreate the previous state if necessary (see *Exporting Audit Log Data*).

To use an XML file to input defined objects:

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

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

2. Enter the file name of the XML import file, or click **Browse** and, from the standard file open window that appears, locate it.
3. Select the type of import: * (specifies import all types), **Network Elements**, **Tiers**, **Serving Gateway/MCC-MNC Mapping**, **Traffic Profiles**, **Retry Profiles**, **Quotas**, **Quota Conventions**,**Match Lists**, **Services, Charging Servers**, **Time Periods**, **Applications**, **Monitoring key**, **Custom AVP Definition**, **Policy Table**, **KTSp Selection**, **Roles**, **Scopes**, or **Users**. * is the default value.
   If you select **Network Elements**, additional filtering fields are available to help you manage the volume of data being imported. You can filter by network element name and Diameter identifier. Each additional field accepts a string that can include the wildcard characters * (to represent any string) and ? (to represent any character). By default, all elements matching the filter are included. For each field you can select the operators **AND**, **OR**, **AND NOT**, or **OR NOT**; if you select an operator, an additional statement field appears. You can specify up to six logical combinations of filtering statements.

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

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

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

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

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

When traffic profiles are imported, they are imported regardless of their configured precedence values. The CMP system displays a message reminding you to check the precedence values of the imported traffic profiles. See *Setting the Precedence Range* for more information.

Exporting an XML File

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

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

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

2. Select the type of export:

   - **Network Elements** (default)
   - **Tiers**
   - **Serving Gateway/MCC-MNC Mapping**
   - **Traffic Profiles**
   - **Retry Profiles**
   - **Quotas**
   - **Quota Conventions**
   - **Match Lists**
   - **Charging Servers**
   - **Time Periods**
   - **Monitoring key**
   - **Custom AVP Definition**
   - **Policy Table**
   - **Applications**
   - **Roles**
   - **Scopes**
   - **Users**

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

   The role LIadmin cannot be exported.

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

   - **AND**
   - **OR**

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

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

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

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

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

The Manager Report

The Manager Report provides information about the CMP cluster itself. This information is similar to the Cluster Information Report for MPE and MRA clusters. The display is refreshed every ten seconds.

To view the Manager Report, select **Reports** from the **System Administration** section of the navigation pane.

The fields that are displayed in the Manager Report section include the following:

- **Cluster Name and Designation** — The name of the cluster, and also whether it is the primary (P) or secondary (S) site.
- **Cluster Mode** — The status of the cluster:
  - **Active**: The cluster is managing the Policy Management network.
  - **Standby**: The cluster is not currently managing the Policy Management network.

  To pause refreshing the display, click **Pause**. To resume refreshing, click **Resume**. To reset the display counters, click **Reset All Counters**.
- **Cluster Status** — The status of the servers within the cluster:
  - **On-line**: If one server, it is active; if two servers, one is active and one is standby.
  - **Degraded**: One server is active, but the other server is not available.
  - **Out-Of-Service**: Neither server is active.
  - **No Data**: The CMP system cannot reach the server.

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

- **Overall** — Displays the current topology state (Active, Standby, or Forced-Standby), number of server (blade) failures, and total uptime (time providing active or standby GUI service). For the definitions of these states, see *Server Status*.

- **Utilization** — Displays the percentage utilization of disk (of the /var/camiant filesystem), average value for the CPU utilization, and memory.

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

The Trace Log

The Trace Log is part of system administration records notifications for management activity on the CMP system. For information on configuring the severity level of messages written to the Trace Log, see *Configuring Log Settings*.

To view log information using the Trace Log Viewer:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The **Trace Log** page opens in the work area.
2. Click **View Trace Log**.

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

   All events contain the following information:

   - **Date/Time** — Event timestamp. This time is relative to the server time.
   - **Code** — The event code. For information about event codes and messages, see the *Policy Management Troubleshooting Guide*.
   - **Severity** — Severity level of the event. Application-level trace log entries are not logged at a higher level than Error.
   - **Message** — The message associated with the event. If additional information is available, the event entry shows as a link. Click on the link to see additional detail in the frame below.

   By default, the window displays 25 events per page. You can change this to 50, 75, or 100 events per page by selecting a value from the **Display results per page** pulldown list.

   Events that occur after the Trace Log Viewer starts are not visible until you refresh the display. To refresh the display, click one of the following buttons:

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

3. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search**.
   The trace log for the selected server displays.
4. When you finish, click **Close**.
   The **Trace Log Viewer** window closes.

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

Filtering the Trace Log

The Trace Log can contain a large number of messages. To reduce the number, the log can be filtered using several different fields.

To filter the log information using the Trace Log Viewer:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The **Trace Log** page opens in the work area.
2. Click **View Trace Log**.
   The **Trace Log Viewer** window opens. While the data is being retrieved, the progress message `Scanning Trace Logs` appears.
3. To view the trace log for a different server, select from the **Trace Log Viewer for Server** and click **Search**.
   The trace log for the selected server displays.
4. Specify the filtering parameters using any of the following fields.
   - **Start Date/Time** — Click (calendar icon), specify a date and time, and then click **Enter**.
   - **End Date/Time** — Click (calendar icon), specify a date and time, and then click **Enter**.
   - **Trace Code(s)** — Enter one or a comma-separated list of trace code IDs. Trace code IDs are integers up to 10 digits long.
   - **Use timezone of remote server for Start Date/Time** — Select to use the time of a remote server (if it is in a different time zone) instead of the time of the CMP server.
   - **Severity** — Filter by severity level. Events with the selected severity and higher are displayed. For example, if the severity selected is **Warning**, the trace log displays events with the severity level Warning.
   - **Contains** — Enter a text string to search for. For example, if you enter **`connection`**, all events containing the word connection display. 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 that appeared in events last month and this month, only results from this month appear.
5. Click **Search**.
   The filtered log displays.
6. When you finish, click **Close**.
   The **Trace Log Viewer** window closes.

Configuring the Trace Log

You can configure the severity level of messages written to the Trace Log.

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The **Trace Log** page opens in the work area.
2. Click **Modify**.
   The **Modify Trace Log Settings** page opens.
3. Select the Trace Log Level.

This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:

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

CAUTION

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

4. When you finish, click **Save**.
   The Trace log level is set.

Modifying the Trace Log Configuration

To configure the trace log display:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The Trace Log page opens in the work area, displaying the current trace log configuration.
2. Click **Modify**.
   The Modify Trace Log Settings page opens.
3. Define the settings.
   For a description of the settings, see *Configuring Log Settings*.
4. When you finish, click **Save**.

The trace log configuration is modified.

Viewing the Audit Log

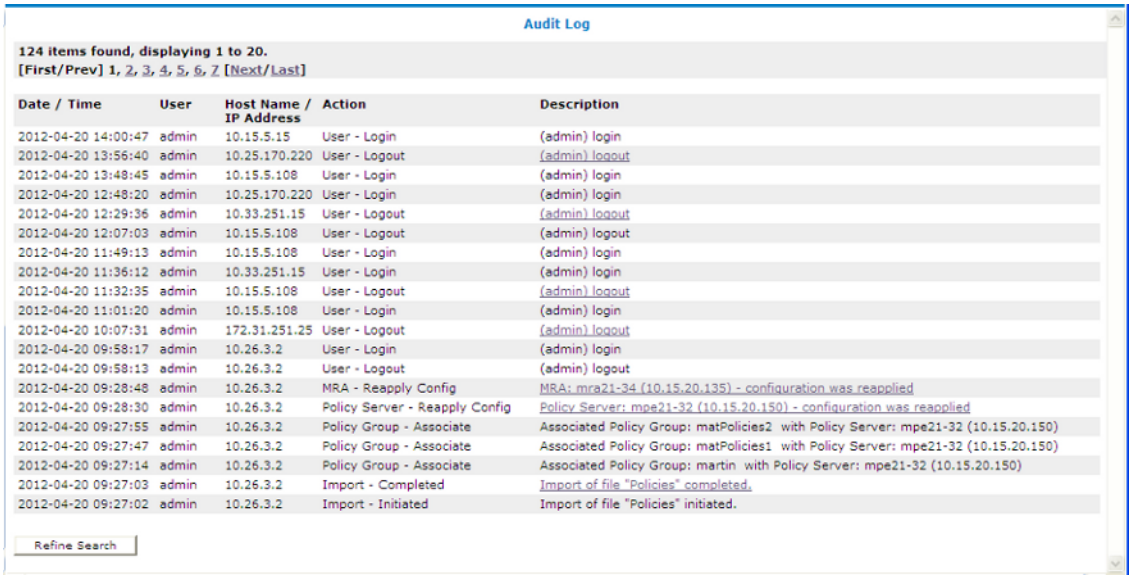
You can track and view configuration changes within the CMP system. Using the audit log, you can track and monitor each configuration event, affording you better system control. The audit log is stored in the database, so it is backed up and can be restored.

To display the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.

The **Audit Log** page opens in the work area.

2. On the **Audit Log** page, click **Show All**.
   The Audit Log opens. (*Figure 25: Audit Log* shows an example.)



Audit Log

124 items found, displaying 1 to 20.
[First/Prev] 1, 2, 3, 4, 5, 6, 7 [Next/Last]

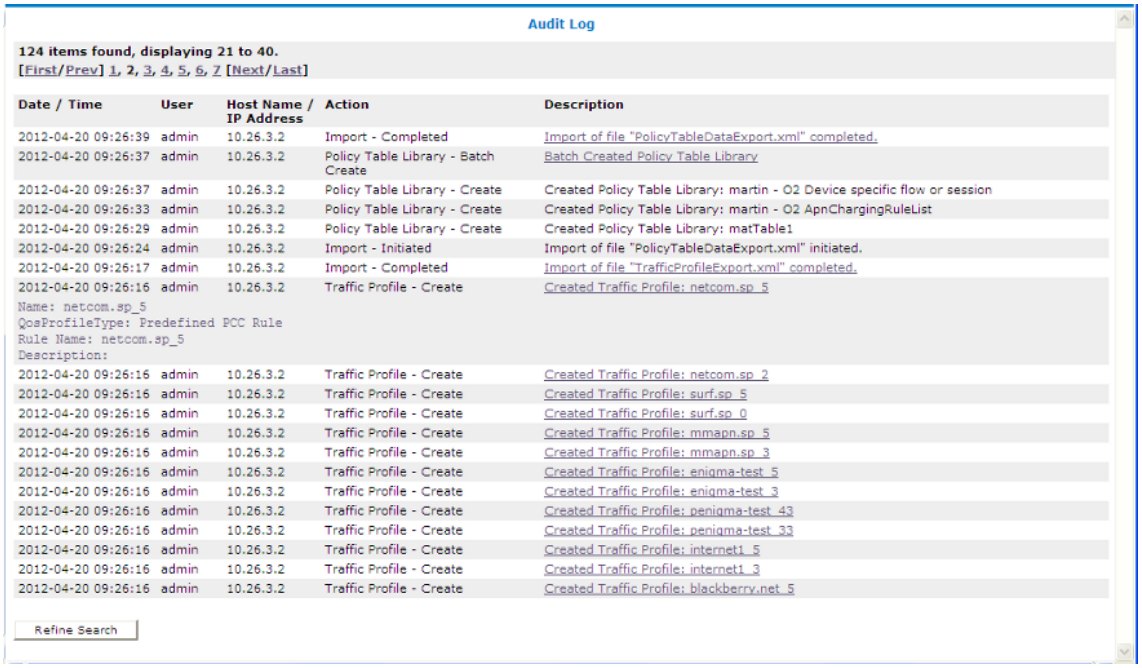
Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 14:00:47	admin	10.15.5.15	User - Login	(admin) login
2012-04-20 13:56:40	admin	10.25.170.220	User - Logout	(admin) logout
2012-04-20 13:48:45	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 12:48:20	admin	10.25.170.220	User - Login	(admin) login
2012-04-20 12:29:36	admin	10.33.251.15	User - Logout	(admin) logout
2012-04-20 12:07:03	admin	10.15.5.108	User - Logout	(admin) logout
2012-04-20 11:49:13	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 11:36:12	admin	10.33.251.15	User - Login	(admin) login
2012-04-20 11:32:35	admin	10.15.5.108	User - Logout	(admin) logout
2012-04-20 11:01:20	admin	10.15.5.108	User - Login	(admin) login
2012-04-20 10:07:31	admin	172.31.251.25	User - Logout	(admin) logout
2012-04-20 09:58:17	admin	10.26.3.2	User - Login	(admin) login
2012-04-20 09:58:13	admin	10.26.3.2	User - Logout	(admin) logout
2012-04-20 09:28:48	admin	10.26.3.2	MRA - Reapply Config	MRA: mra21-34 (10.15.20.135) - configuration was reapplied
2012-04-20 09:28:30	admin	10.26.3.2	Policy Server - Reapply Config	Policy Server: mpe21-32 (10.15.20.150) - configuration was reapplied
2012-04-20 09:27:55	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: matPolicies2 with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:47	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: matPolicies1 with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:14	admin	10.26.3.2	Policy Group - Associate	Associated Policy Group: martin with Policy Server: mpe21-32 (10.15.20.150)
2012-04-20 09:27:03	admin	10.26.3.2	Import - Completed	Import of file "Policies" completed.
2012-04-20 09:27:02	admin	10.26.3.2	Import - Initiated	Import of file "Policies" initiated.

Refine Search

Figure 25: Audit Log

For a detailed description of an item, click the underlined description. The details of the event display. (*Figure 26: Audit Log Details* shows an example.)

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



Audit Log

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

Date / Time	User	Host Name / IP Address	Action	Description
2012-04-20 09:26:39	admin	10.26.3.2	Import - Completed	Import of file "PolicyTableDataExport.xml" completed.
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Batch Create	Batch Created Policy Table Library
2012-04-20 09:26:37	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 Device specific flow or session
2012-04-20 09:26:33	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: martin - O2 ApnChargingRuleList
2012-04-20 09:26:29	admin	10.26.3.2	Policy Table Library - Create	Created Policy Table Library: matTable1
2012-04-20 09:26:24	admin	10.26.3.2	Import - Initiated	Import of file "PolicyTableDataExport.xml" initiated.
2012-04-20 09:26:17	admin	10.26.3.2	Import - Completed	Import of file "TrafficProfileExport.xml" completed.
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: netcom.sp_5
Name: netcom.sp_5 QosProfileType: Predefined PCC Rule Rule Name: netcom.sp_5 Description:				
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: netcom.sp_2
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: surf.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: surf.sp_0
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmapn.sp_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: mmapn.sp_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_5
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: enigma-test_3
2012-04-20 09:26:16	admin	10.26.3.2	Traffic Profile - Create	Created Traffic Profile: 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

Refine Search

Figure 26: Audit Log Details

Searching for Audit Log Entries

To search for entries in the Audit Log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. Click **Search**.
   The **Audit Log Search Restrictions** page opens.
3. Define the following items, depending on how restrictive you want the audit log search to be:
   - **From/To** — Enter the start and end dates and times for this search.
   - **Action by User Name(s)** — Enter the name of the user or users to audit.
   - **Action on Policy Server(s) / MRA(s)** — Enter the name of the Policy Management device to audit.
   - **Audit Log Items to Show** — Specifies a category of items to audit for display:
     - **Policy Server**
     - **Network Element**
     - **Network Element Group**
     - **Application**
     - **MRA**
     - **Policy**
     - **Policy Group**
     - **Account**
     - **Tier**
     - **Entitlement**
     - **Alert**
     - **User**
     - **Audit**
     - **Alarm**
     - **OM Statistics**
     - **Quota**
     - **Quota Convention**
     - **Charging Server**
     - **Time Period**
     - **MPE Manager**
     - **Upgrade Manager**
     - **Topology Setting**
     - **Global Configuration Settings**
     - **Trending Report**
     - **User Layout**
     - **Upsync Log Alarm Threshold**

     When you select some categories, a **Name** field appears, which lets you enter a search string; leave the field blank to include all items. When you select any category, an **Action(s)** link appears, which lets you select individual audit log items within the category. By default all items in the category are selected, but you can select individual items instead. By default you can specify three item categories; click **More Lines** to add an additional item category.

- **Results Forms** — Specifies the number of items per page to display, along with which data to display (most recent or oldest items).

4. When you finish defining the search parameters, click **Search**.
   The Audit Log displays search results.

Exporting or Purging Audit Log Data

You can export the audit log to a text file; the default filename is `AuditLogExport.txt`.

Exporting Audit Log Data

You can export audit log data to a text file. The filename is `AuditLogExport.txt`.

To export data from the audit logs:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. Click **Export/Purge**.
   The **Export and Purge Audit Log Items** page opens.
3. In the **Items to Export** section, select one of the following options:
   a) **Export All Items** — Writes all audit log entries.
   b) **Export Through Date** — Click (calendar icon), and select a date.
4. When you finish, click **Export**.
   A standard File Download window opens; you can open or save the export file.

The audit log is exported.

Purging Audit Log Data

To purge data from the audit log:

1. From the **System Administration** section of the navigation pane, select **Audit Log**.
   The **Audit Log** page opens in the work area.
2. Click **Export/Purge**.
   The **Export and Purge Audit Log Items** page opens.
3. In the **Items to Purge** section, click (calendar icon) and select a date.
4. When you finish, click **Purge**.
   You are prompted with a confirmation message.
5. Click **OK**.

The data is purged from the audit log.

Managing Scheduled Tasks

The CMP system runs batch jobs to complete certain operations. These tasks are scheduled to run at regular intervals, with some tasks scheduled to run in a certain order. You can change the scheduling of these tasks to better manage network load or to propagate a network element change to the Policy Management devices on demand. You can also abort a running task.

CAUTION

Caution: Oracle recommends that you follow the order in which scheduled tasks are listed. Serious system problems can occur if the order is changed. Consult My Oracle Support 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.
OM Statistics	Periodically retrieves Operational Measurement (OM) statistics from all MPE devices. The Operational Measurements XML interface retrieves operational counters from the system. The OM interface requires that the OM Statistics scheduled task be running on the CMP system. After the specified Stats Collection Period, this task collects the operational counters from the Policy Management devices in the network and records them in the CMP database; the data is then available for query via the OM XML interface. You can configure the task to poll at intervals between 5 minutes and 24 hours, with a default value of 15 minutes; the system keeps the data available for query for 1 to 30 days, with a default value of 7 days. The recommended settings for this task will vary depending on the volume of data you are collecting. When you request OM statistics, the data for the response is taken from the information that has been collected by this task. You must gather data using

the OM Statistics scheduled task if you want data available for subsequent OM queries.

Most values returned as part of the response are presented as the positive change between the start time and end time. To calculate a response, you must have a minimum of two recorded values available; thus you must run the OM Statistics task at least twice in a given time period before you can obtain any statistical data from the OSSI XML interface. The *OSSI XML Interface Definitions Guide* describes the OM Interface and the OM Statistics in detail.

Stats File Generator Generates statistics files by extracting the data from the CMP database using the OSSI XML interrface. This task is also responsible for cleaning up the statistics files. The available settings for this task are: Local Repository directory (the default is `/var/camiant/stats_export`); Maximum age to keep files, in hours (default is 72 hours); File Format, either XML (default) or CSV; and Stats Type, which lets you select the statistics group(s) to extract. For information on the individual statistics in each available group, see the *OSSI XML Interface Definitions Guide*.

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.

OSSI Distributor Task (optional) Reads from the database topology and subscriber data that has entered the CMP database using the OSSI Interface.

Subnet SNMP Collector Collects all subnet information residing on the CMTS devices by polling, via SNMP, all CMTS devices for all subnets and then stores them in the local database.

Service Class SNMP Collector Polls, using SNMP, all CMTS devices for the configured service classes and then stores them in the local database.

Subscriber SNMP Collector Polls, using SNMP, all CMTS devices for the configured subscribers and then stores them in the local database.

CMTS Distributor Reads CMTS topology data from the CMP database and then distributes it to the appropriate Policy Management devices within the system.

Subscriber Distributor Reads subscriber data from the CMP database and then distributes it to the appropriate Policy Management devices within the system.

CMTS MA Collector (optional) Polls all of the MAs in the system for subnet and service class data on each CMTS.

PCMM Routing Distribution Detects changes in the CMTS subnet information, and then forwards this information to any upstream MPE devices configured in a routing hierarchy.

Replication Statistics Generates replication statistics for MPE and MRA servers.

Note: The run interval should be the same as the Stats Collection Period. For more information, see *Setting Stats Settings*.

Configuring a Task

To configure an individual task:

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

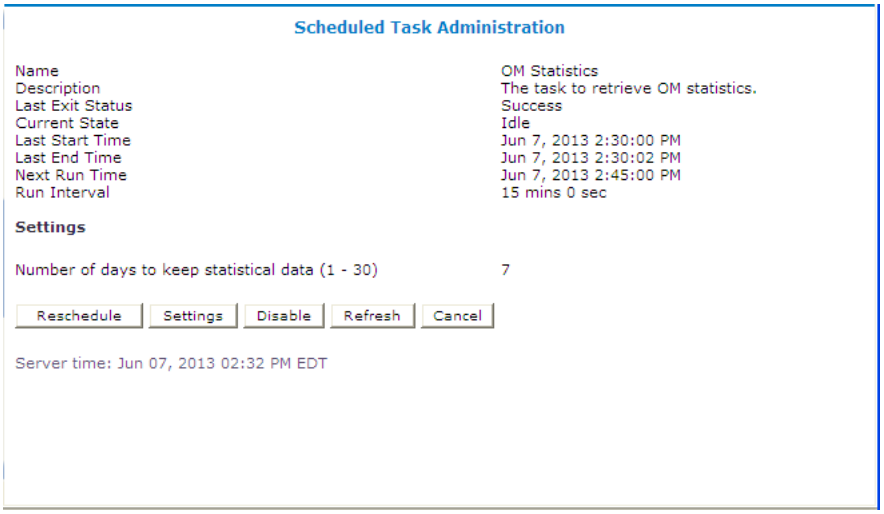
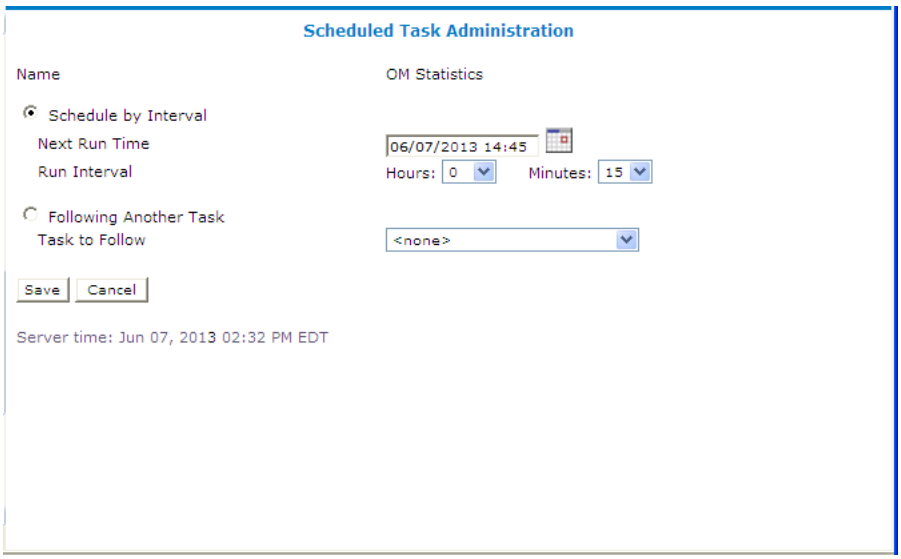


Figure 27: Schedule Task Administration

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



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

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

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

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

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

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

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

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

4. The available options for a scheduled task are as follows:

Managing Users

The CMP system lets you configure the following user attributes:

Roles	What a user can do within the CMP system. See *About User Roles* for details.
Scopes	What network element groups and Policy Management device groups a user can control, which provides a context for a role. See *About User Scope* for details.
Users	Once you define roles and scopes, you can apply them to user profiles. See *About User Profiles* for details.
External Authentication	Lets the CMP system authenticate users using RADIUS or SANE Authentication. These users must match the RADIUS Server account information before access is permitted. See *External Authentication* for details.

Creating a Customer User Management System Profile

To support identity management (IDM), the CMP system can accept HTTP or HTTPS connection requests from an external Customer User Management system to create, update, query, and delete user accounts. Requests and responses consist of XML documents. You must define a user profile for the external system. The profile is a regular CMP user profile with specific roles and scope.

Assign the profile a role that includes the following privileges:

- Show privilege for XML Import/Export
- Read-Write privilege for User Management

For information on creating a user profile, see *Creating a User Profile*. For more information on the XML application programming interface, see the *OSSI XML Interface Definitions Guide*.

About User Roles

The CMP system uses roles to configure what a user can do within the CMP system. Assigning roles to the various users that access the CMP system lets you control who can configure and access features within the CMP system. The default roles are:

Administrator	Permits full read/write access to all functions. You cannot delete the Administrator role.
Operator	Permits full read/write access to all Policy Management device management and configuration functions. Access is also permitted to all system administration functions except user administration.
Viewer	Permits read-only access to functions associated with Policy Management device management and configuration. Full access is also permitted to some of the system administration functions, such as Change Password.

The CMP system allows you to perform the following role management actions:

- *Creating a New Role*
- *Modifying a Role*
- *Deleting a Role*

Creating a New Role

To create a new role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
   The **Role Administration** page opens in the work area, displaying existing roles.
3. On the **Role Administration** page, click **Create Role**.
   The **New Role** page opens. By default, all privileges' accesses are set to either **Hide** (that is, the functions do not appear to users of the role, so access must be explicitly granted) or **Read-Only** (that is, information can be displayed but not changed).
4. Enter the **Name** for the new role.

   Maximum of 64 characters.
5. Enter a **Description/Location** (optional).

   Free-form text.
6. **Policy Server Privileges** — Defines access to the following MPE device management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Configuration**
   - **Configuration Template**
   - **Applications**
   - **Match Lists**
   - **Quota Profiles & Conventions**
   - **Services & Rating Groups**
   - **Policy Counter ID**
   - **Traffic Profiles**

- **Roaming Profile**
- **Protocol Timer Profile**
- **Retry Profiles**
- **Charging Servers**
- **Time Periods**
- **Monitoring Key**
- **Serving Gateway/MCC-MNC Mapping**
- **Customer Vendor**
- **Global Configuration Settings**
- **Bulk Operation**

7. **Subscriber Privileges** — Defines access to the subscriber functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Entitlements**
   - **Tiers**
   - **Quota Usage**
8. **SPR Privileges** — Defines access to the SPR functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Subscriber Data**
9. **Network Privileges** — Defines access to the network management functions (with the access **Hide**, **Read-Only**, or **Read-Write**):
   - **Network Elements**
   - **Topology** (not supported)
10. **MRA Privileges** — Defines access to the MRA Configuration functions:
    - **Configuration** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Bulk Operations** (with the access **Hide** or **Show**)
    - **Configuration Template**
11. **Policy Management Privileges** — Defines access to the policy management functions:
    - **Policy Library** (with the access **Hide**, **Read-Only**, **Read and Deploy**, or **Read, Deploy, and Write**)
    - **Template Library** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Policy Table Library** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Policy Checkpoint** (with the access **Hide**, **Read-Only**, or **Read-Write**)
12. **System Wide Reports Privileges** — Defines access to the system-wide reports functions:
    - **System Wide Reports Configuration** (with the access **Hide**, **Read-Only**, or **Read-Write**)
13. **Platform Setting Privileges** — Defines access to the platform setting functions:
    - **Platform Configuration Setting** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Topology Settings** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **SNMP Settings** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Server Operation** (with the access **Hide** or **Read-Write**)

14. **Upgrade Manager Privileges** — Defines access to software upgrade functions:
    - **ISO Maintenance** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Upgrade Manager** (with the access **Hide**, **Read-Only**, or **Read-Write**)
15. **System Administration Privileges** — Defines access to system administration functions:
    - **Import / Export** (with the access **Hide** or **Show**)
    - **Operational Measurements** (with the access **Hide** or **Read-Only**)
    - **User Management** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Scheduled Tasks** (with the access **Hide** or **Read-Write**)
    - **Trace Log of CMP** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Subscriber Activity Log** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Audit Log** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Audit Log User Info** (with the access **Hide** or **Show**)
    - **Alarms** (with the access **Hide**, **Read-Only**, or **Read-Write**)
    - **Password Strength** (with the access **Read-Only** or **Read-Write**)
    - **Push Method for Statistics** (with the access **Read-Only** or **Read-Write**)

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

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

      Task Settings

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

    New tasks are created to synchronize stats files. These tasks will retry if a remote server is unreachable. The following fields are displayed for the Stats Files Synchronization setting:

    - **Remove Server Information**
      - **Host Name/IP Address**
      - **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. When you finish, click **Save**.

Privileges are assigned to the role.

Modifying a Role

To modify a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
   The **Role Administration** page opens in the work area, displaying existing roles.
3. Select the role to modify.
   The **Role** page opens.
4. Click **Modify**.
   The **Modify Role** page opens.
5. Modify role information as necessary.
   See *Creating a New Role* for a description of the fields contained within this page.
6. When you finish, click **Save**.

The role is modified.

Deleting a Role

You can delete any role except the Administrator role. You cannot delete a role that is in use.

To delete a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, select the **Roles** group.
   The **Role Administration** page opens in the work area, displaying existing roles.
3. Delete the role using one of the following methods:
   - From the work area, click the Delete icon located next to the role to delete.
   - From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

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

The role's information is deleted from the CMP database.

About User Scope

Scope defines which network element groups and Policy Management device groups that a user has access to, which provides operational context for a role.

The CMP system allows you to perform the following scope management actions:

- *Creating a New Scope*
- *Modifying a Scope*
- *Deleting a Scope*

Creating a New Scope

You can configure scopes that contain selections of network element groups and Policy Management device groups that provide a context for a role. This lets you control what areas or devices in a network a user can manage. The default scope, **Global**, contains all items defined within the CMP database. Once you define a scope you can assign it to users.

To configure a new scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. In the content tree, click **Scopes**.
   The **Scope Administration** page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. Click **Create Scope**.
   The **New Scope** page opens.
4. Enter the **Name**

   The name for the scope (up to 64 characters).
5. Enter the **Description/Location** (optional).

   Free-form text.
6. Select the policy server groups included in this scope.
7. Select the network element groups included in this scope.
8. Select the MRA groups included in this scope.
9. When you finish, click **Save** to create the scope.

The scope is created.

Modifying a Scope

To modify a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. In the content tree, click **Scopes**.
   The **Scope Administration** page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. On the **Scope Administration** page, select the scope you want to modify.
   The scope description opens.
4. Click **Modify**.
   The **Modify Scope** page opens. *Creating a New Scope* describes the fields on this page.
5. Modify scope information as necessary.
6. When you finish, click **Save**.

The scope is modified.

Deleting a Scope

You can delete any scope except **Global**. To delete a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
2. From the content tree, click **Scopes**.
   The **Scope Administration** page opens in the work area, displaying existing scopes.
3. Delete the scope using one of the following methods:
   - From the work area, click (trash can icon) located to the right of the scope to delete.
   - From the content tree, select the scope to delete (scope information displays in the work area), then click **Delete**.

   A confirmation message appears.
4. Click **OK**.

The scope is deleted.

About User Profiles

A user profile defines a user with a role and one or more scopes.

The CMP system allows you to perform the following scope management actions:

- *Creating a User Profile*
- *Modifying a User Profile*
- *Deleting a User Profile*

Creating a User Profile

The User Management functions include the tools necessary to create, modify, or delete system user profiles.

The CMP system is configured initially with the following default user profiles and passwords:

- admin/policies (you cannot delete this profile)
- operator/policies
- viewer/policies

Each default user profile has an associated role assigned to it. The **admin** user is the only profile that cannot be deleted or have its username modified. Also, the **admin** user is the only user who can create, modify, or delete other users. The password assigned to the **admin** user can be changed. For security reasons, it is recommended that you change this value from the default value as soon as the system is installed.

Note: When logging in, the username is not case sensitive; however, the password is case sensitive.

To create a new user profile:

1. Log into the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.

   Note: The **Log Out All Users** button is visible only to the **admin** user.

4. Click **Create User**.
   The **New User** page opens.
5. Define the following information:
   a) **Username** — Assign a name to the user profile of up to 64 characters (this value is not case sensitive).
   b) **Description/Location** (optional) — Free-form text.
   c) **Password** — Assign a password to the user profile.
   This value is case sensitive and must contain at least six characters; alphabetic, numeric, and special characters are allowed. This value must conform to the password strength rules.
   d) **Confirm Password** — Re-enter the password to confirm the value entered above.
   e) **Password Expiration Period(days; 0=never)** — The number of days a password can be used before it expires. (This overrides the system setting.)

      Enter a value from 7 to 365, or 0 to indicate that the password never expires. The default is the system setting.
   f) **Force to Change Password** — If selected, this user must change passwords when he or she next logs in.
   g) **Role** — Select a role from the drop list to assign to the user profile.
   h) **Scopes** — Select one or more scopes to assign to the user profile.
6. When you finish, click **Save**.

The user profile is created and stored in the **Users** group.

Modifying a User Profile

To modify a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Select the user profile from the content tree.
   The profile information page opens.
5. Click **Modify**.
   The **Modify User** page opens.
6. Modify the user profile.
   For field descriptions, see *Creating a User Profile*.
7. When you finish, click **Save**.

The user profile is modified.

Deleting a User Profile

You can delete any user profile except **admin**. To delete a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.

3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Delete the user profile using one of the following methods:
   - From the work area, select the ×(X icon), located to the right of the profile you want to delete.
   - From the content tree, select the user profile that you want to delete (profile information displays in the work area), then click **Delete**.

   A confirmation message displays.
5. Click **OK** to delete the user profile.

The user profile is deleted.

Creating a Customer User Management System Profile

To support identity management (IDM), the CMP system can accept HTTP or HTTPS connection requests from an external Customer User Management system to create, update, query, and delete user accounts. Requests and responses consist of XML documents. You must define a user profile for the external system. The profile is a regular CMP user profile with specific roles and scope.

Assign the profile a role that includes the following privileges:

- Show privilege for XML Import/Export
- Read-Write privilege for User Management

For information on creating a user profile, see *Creating a User Profile*. For more information on the XML application programming interface, see the *OSSI XML Interface Definitions Guide*.

About Locking and Unlocking User Accounts

A user is locked out after exceeding the login failure threshold, or if the **admin** user locks the user out. A locked-out user sees the following message on the login page when attempting to log in: `Your account is locked. Please contact the Administrator`.

Note: The **admin** account cannot lock the **admin** account.

The CMP system allows you to perform the following actions:

- *Locking an Account*
- *Unlocking an Account*

Locking an Account

To lock a user account:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Select the user profile from the content tree.
   The **User Administration** page opens.
5. Click **Lock**.
   A confirmation message appears.

6. Click **OK**.
   The account is locked. The page displays the message `User account locked successfully`. The **Lock** button becomes an **Unlock** button. On the **User Administration** page, the Locked Status for the user shows `Locked`.

Unlocking an Account

To unlock a user account:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. Select the user profile from the content tree.
   The **User Administration** page opens.
4. Click **Unlock**.
   A confirmation message appears.
5. Click **OK**.
   The account is unlocked. The page displays the message `User account unlocked successfully`. The **Unlock** button becomes a **Lock** button. On the **User Administration** page, the Locked Status for the user shows `Unlocked by Admin`.

Logging Out All Users

You can log out all users (except the **admin** account) from the CMP system. To log out all users:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. In the content tree, click **Users**.
   The **User Administration** page opens in the work area, displaying existing users.
4. Click **Log Out All Users**

   A confirmation message appears.
5. Click **OK** to log out all users.

Users are logged out.

External Authentication

In addition to the built-in authentication functions, you can configure external authentication, RADIUS authentication, and SANE authentication of CMP users.

The CMP system allows you to manage the following external authentication methods:

- *RADIUS Authentication and Accounting*
- *SANE Authentication*

RADIUS Authentication and Accounting

The CMP system supports RADIUS authentication and accounting. You can configure the CMP system to operate in a network environment including multiple authentication servers, one authentication

server, or no servers. If both primary and secondary authentication servers are defined, the authentication process is as follows:

1. The CMP system contacts the primary RADIUS server.
   If it responds with Accept or Reject, that action is followed.
2. If the primary server does not respond within a specified number of retries or before a timeout value, the CMP system contacts the secondary RADIUS server (if defined).
   If it responds with Accept or Reject, that action is followed.
3. If the secondary server does not respond, the CMP system authenticates against its local database (if enabled).
4. If local authentication is not enabled, authentication fails.
5. The user **admin** is always authenticated locally, regardless of configuration settings.

This process provides a fail-safe mechanism for accessing the CMP system even in the face of misconfiguration or network problems that cause the RADIUS servers to become inaccessible.

RADIUS configuration involves three steps:

1. *Configuring the RADIUS Server* to accept authentication (and accounting, if used)
2. *Defining CMP Users to the RADIUS Server* and *Associating Roles and Scopes* on the CMP system
3. *Defining the CMP System as a RADIUS Client* to work with RADIUS

Configuring the RADIUS Server

The RADIUS server must be configured to authenticate clients and users on the CMP system. Some of the configuration values must be consistent with configuration parameters on the CMP system. (The RADIUS administrator is aware of the names and locations of the configuration files.) See *Enabling and Configuring RADIUS on the CMP System* for details.

Defining the CMP System as a RADIUS Client

The client file identifies the systems that use the RADIUS server to authenticate user access. A client should be defined as a single device; for example:

```
client 10.0.10.22 {
        secret = oracle
        shortname = MPE5
}
client 10.0.10.23 {
        secret = oracle
        shortname = CMP56
}
```

The best practice is to define IP addresses rather than FQDNs. If a netmask is not given, the default is **`/32`**. The shared secret (in this example, **`oracle`**) 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.

Defining CMP Users to the RADIUS Server

RADIUS can use either a database or a simple flat file as its repository of user information. The following example uses a flat file to demonstrate a minimum user configuration. The users file contains authentication and configuration information for each user. It begins with the username and the

authentication (password) that is required from the user. The user/password line is followed by indented lines that are attributes to be passed back to the requesting server.

When RADIUS has authenticated a user, it sends back various attributes with the authentication acceptance message. The CMP system uses these attributes to determine what the user can do. The best practice is to use a vendor-specific attribute (VSA) dictionary file to define what attributes to send back to the client. *Figure 28: Sample VSA Dictionary File For RADIUS* shows a sample file. The local RADIUS administrator is responsible for incorporating the VSA dictionary file onto the RADIUS server.

```
========== dictionary. ====================
# Oracle Communications VSA's, from RFC 2548
# The filename given here should be an absolute path.
#
# Place additional attributes or $INCLUDEs here.

VENDOR Oracle 21274
BEGIN-VENDOR Oracle
ATTRIBUTE Oracle-MI-role 1 string
ATTRIBUTE Oracle-MI-scope 3 string
END-VENDOR Oracle
======================
```

Figure 28: Sample VSA Dictionary File For RADIUS

The attributes **`Oracle-MI-role`** and **`Oracle-MI-scope`** are for access to the CMP system. Both a scope and a role are associated with a user. The responses sent back from the RADIUS server should match what is configured in the CMP system. The defaults for the role, in ascending order of capability, are **`Viewer`**, **`Operator`**, and **`Administrator`**, but the system administrator can create other roles or remove any role except that of **`Administrator`**.

The default scope is **`Global`**, and the administrator can create other scopes within the CMP system.

Associating Roles and Scopes

The CMP system assigns two attributes to a user, a role and a scope. Users that authenticate against a RADIUS server are assigned roles and scopes by matching against the attribute values returned by the RADIUS server.

It is easiest to provide role and scope values using the VSA dictionary, by defining the attributes **Oracle-MI-role** and **Oracle-MI-scope**. The flexibility of roles and scopes can be supported by RADIUS if the VSA dictionary is integrated.

The following example defines users who have access at different role levels:

```
Jeff      Cleartext-Password:="garbage"
          Class="Administrator",
          Oracle-MI-role="Administrator",
          Oracle-MI-scope="Global"

Paul      Cleartext-Password:="apr6279"
          Class="Viewer",
          Oracle-MI-role="Viewer",
          Oracle-MI-scope="Global"
```

However, if Oracle VSAs are not included in the RADIUS dictionary, then they cannot be defined in the user file, and only a **Class** attribute can be returned on a RADIUS authentication. The CMP system can use the Class attribute for RADIUS authentication.

To accept the Class attribute for CMP login, define a scope and a role that matches what the RADIUS server returns as the Class attribute. The CMP system uses the Class attribute for both required credentials. For example, consider this user defined in RADIUS:

```
Dawn      Cleartext-Password:="kkmk4813"
          Class="Viewer"
```

Dawn can get access to the CMP system if you have defined both a role named Viewer and a scope named Viewer; the GUI matches the one returned value to both of the required credentials.

Enabling and Configuring RADIUS on the CMP System

By default, RADIUS Authentication is disabled in the CMP system. Enabling authentication requires admin privileges. The user **admin** is always authenticated against the local database account; thus, the admin user is best suited to setting up RADIUS authentication (see *Creating a User Profile*).

Two configuration parameters must match with the configuration that was put on the RADIUS server:

- **Source of User Credentials** must match up with the user configuration in the RADIUS server, but this will also depend on what is configured in the next parameter.
- If **Action if missing credentials** is set to **Use following defaults**, then a user will be authenticated as long as the password is correct. This user could log in even though the class is not valid:

```
test      Cleartext-Password := "2931txy"
          Class = "noone"
```

If **Action if missing credentials** is set to **Reject**, then the configuration of the user will depend on the configuration of **Source of user credentials**.

To enable RADIUS authentication and accounting:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.
3. From the content tree, select **External Authentication**.
   The **External Authentication** page opens, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**.
   The modify page opens.
5. In the **Configuration** section, select **Enable RADIUS Authentication**.
   Configuration and RADIUS Services configuration fields appear.
6. Edit the following fields:
   a) **Enable RADIUS Accounting** — Enables RADIUS accounting on the CMP system.
   This feature is disabled by default. When enabled, the CMP system sends an Accounting-Start message to the accounting server when a user logs in, and an Accounting-Stop message when the user logs out. These messages contain a session ID attribute that uniquely identifies the user session so that it can be matched between Start and Stop.
   b) **Destination for Accounting Messages** — Choose the following from the list:

- **Both Primary and Secondary** (the default) — Specifies that accounting messages generated for each user session are sent to both the primary and (when configured) secondary RADIUS servers.
- **Primary (Secondary on error)** — Accounting messages are sent only to the primary server, as long as it is reachable. If the primary accounting server is unreachable, messages are sent to the secondary accounting server.

c) **NAS IP Address** (required) — IP address, in IPv4 or IPv6 format, of the network access server. By default, this is the local host address.

d) **Use local authentication** — Choose when to use local authentication:

- **When RADIUS servers timeout**
- **When both RADIUS servers timeout or reject**
- **Never** — Fallback to local authentication is never used (however, the user **admin** is always authenticated locally)

e) **Source of User Credentials** — Choose the following from the list:

- **RADIUS Class** — The value of the Class attribute returned by the server determines both the role and scope.

f) **Action if Missing Credentials:**

- **Reject** — If you select this option, a user whose login credentials are missing is not logged in.
- **Use following defaults**:
  1. **Default Role** — Role assigned if the user credentials are missing or mismatched. The default is **Viewer**.
  2. **Default Scope** — Scope assigned if the user credentials are missing or mismatched. The default is **Global**.

7. In the **RADIUS Services** section, edit the following fields:

a) **Primary RADIUS Authentication Server**

- **Server** — FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary authentication server.

  Note: To disable the primary server, delete its IP address.

- **Port** — IP port number of the primary server. The default is port 1812.
- **Timeout (seconds)** — How long the CMP system waits for a response from the server. The default is 3 seconds.
- **Retries** — How many times the CMP system tries to send a message to the server. The default is 3 times.
- **Shared Secret** — A password-like string that must exactly match between the CMP system and the secret configured in the entry for this CMP system in the clients.conf file in the RADIUS server. If it does not match, the server ignores all messages from the CMP system.

b) **Secondary RADIUS Authentication Server**

If configured, the secondary authentication server uses the same fields as the primary server.

c) **Primary RADIUS Accounting Server**

- **Server** — FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary accounting server.
- **Port** — IP port number of the primary server. The default is port 1813.
- **Timeout (seconds)** — How long the CMP system waits for a response from the server. The default is 3 seconds.
- **Retries** — How many times the CMP system tries to send a message to the server. The default is 3 times.
- **Shared Secret** — A password-like string that must exactly match between the CMP system and the secret configured in the entry for this CMP system in the clients.conf file in the RADIUS server. If it does not match, the server ignores all messages from the CMP system.

d) **Secondary RADIUS Accounting Server**

If configured, the secondary accounting server uses the same fields as the primary server.

8. When you finish, click **Save**.
   The window closes.

RADIUS Authentication and Accounting is configured.

SANE Authentication

The CMP system supports Secure Access to Network Elements (SANE) authentication and authorization. You can configure the CMP system to operate in a SANE network environment such that a user elsewhere in the network can gain single sign-on (SSO) access. When the CMP system is configured to authenticate using SANE, users can log in using a SANE client. (Usage of a SANE client is outside the scope of this document.) See *Enabling and Configuring SANE Authentication on the CMP System* for details.

The **admin** account is treated separately. An admin user enters the CMP URL in any supported browser to log in.

The authentication process is as follows:

1. From a SANE client GUI, the user selects the CMP system. A web browser session is launched. An encrypted SANE authentication artifact is sent to the CMP system through the browser.
2. The CMP system forwards the artifact to a SANE server (the SANE responder).
3. If the SANE server verifies the artifact, it returns an assigned role and scope for the user, and the CMP system allows the user to log in accordingly. Otherwise, the CMP system rejects the login request.
4. The user **admin** is always authenticated locally, regardless of configuration settings. (That user clicks on the **Login** link.)

Enabling and Configuring SANE Authentication on the CMP System

By default, SANE Authentication is disabled in the CMP system. Enabling authentication requires admin privileges. The user **admin** is always authenticated against the local database account; thus, the admin user is best suited to setting up SANE authentication (see *Creating a User Profile*).

To enable SANE authentication:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the **User Management** group.

3. From the content tree, select **External Authentication**.
   The **External Authentication** page opens, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**.
   The modify page opens.
5. In the **Configuration** section, select **Enable SANE Authentication**.
   Additional fields appear.
6. Edit the following fields:
   a) **Artifact Parameter Name** — Name of the artifact parameter. Enter an alphanumeric string. The default is **artifact**.
   b) **Verification for Account** — Choose the following from the list:
      - **On login only** (default) — The CMP system authenticates the user once, on login. The user is considered authenticated until logout.
      - **On each request** — The CMP system authenticates the user on login, and then again for each HTTP or HTTPS request. If any request is not authenticated, the user is immediately logged out.
   c) **Action if Missing Credentials:**
      - **Reject** — If you select this option, a user login is rejected even if the authentication is successful.
      - **Use following defaults** — If you select this option, a user with missing credentials is allowed to log in, but the system assigns a default role and scope:
        1. **Default Role** — Default role assigned to the user. The default role is **Viewer**.
        2. **Default Scope** — Default scope assigned to the user. The default scope is **Global**.
7. In the **SANE Servers** section, edit the following fields:
   a) **SAML Service Name** — Name of the Security Assertion Markup Language service registered with the UDDI server. Enter an alphanumeric string.
   b) **UDDI Inquiry URL** — Universal Description, Discovery and Integration URL, in HTTP or HTTPS format, for the inquiry.
8. When you finish, click **Save**.

SANE authentication is configured on the CMP system.

Changing a Password

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

Note: The **admin** user can change any user's password.

If a system administrator has configured your account for password expiration, you will receive a warning when you log in that you will need to change your password.

To change your password:

1. From the **System Administration** section of the navigation pane, select **Change Password**.

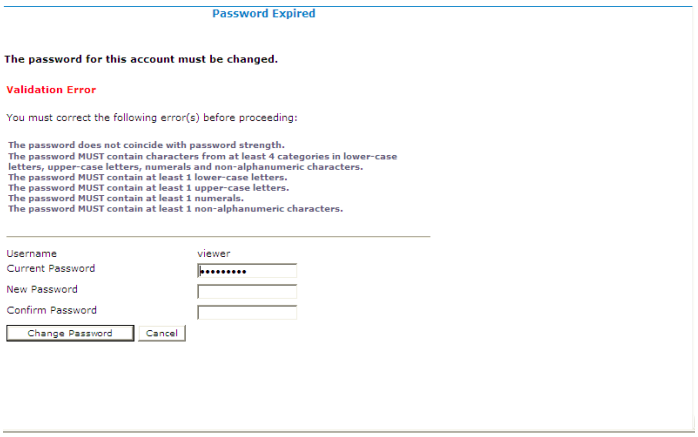
The **Change Password** page opens. If your account is set up with a password expiration period, the expiration date is displayed.

2. Enter the following information:
   a) **Current Password** — The present value of the password.
   b) **New Password** — The value of the new password.

      This value is case sensitive and must conform to the password strength rules. The password cannot contain the user name.

   c) **Confirm Password** — Enter the new password value again.

      If your new password does not conform to the password strength rules, a validation error message appears; for example:



      Enter and confirm another password that conforms to the rules.

3. When you finish, click **Change Password**.

Your password is changed.

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

Appendix A

CMP Modes

Topics:

The functions available in the CMP system are determined by the operating modes and sub-modes selected when the software is installed. Functions that can change include:

- Items on the navigation pane
- Tabs on the **Policy Server Administration** page
- Protocols supported
- Configuration options
- Policy options available in the policy wizard
- Reports available

Normally, servers are pre-configured before delivery. However, if it becomes necessary to replace a server or reinstall the software in the field, the mode selection screen becomes visible, and you must reset the operational modes as appropriate for your environment before you can use the product.

This appendix briefly describes the modes and sub-modes available.

CAUTION

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

The Mode Settings Page

When you use a web browser to connect to a CMP system after the software is first installed, the **Mode Settings** page opens (*Figure 29: Mode Settings Page*). Select modes, functions, and management options, and then click **OK**. The browser page closes and you are automatically logged out. When you next log in, the CMP system reopens in the selected mode.

The modes and functions available are:

Cable Mode Enables support of a cable carrier environment. Functions are described in the *Configuration Management Platform Cable User's Guide*.

Table 60: Cable Functions

Function	Description
PCMM	Supports PacketCable MultiMedia functions.
DQOS	Supports Dynamic Quality of Service functions.
Diameter AF	Supports Diameter AF functions.

Wireless Mode Enables support of a wireless carrier environment. Functions are described in the *Configuration Management Platform Wireless User's Guide*.

Table 61: Wireless Functions

Function	Description
Diameter 3GPP	Supports Diameter 3GPP protocol.
Diameter 3GPP2	Supports Diameter 3GPP2 protocol.
PCC Extensions	Supports Policy and Charging Control functions.
Quotas Gx	Supports a subscriber quota environment using the Diameter Gx protocol. The Gx protocol supports deep packet inspection (DPI) devices.
Quotas Gy	Supports a subscriber quota environment using the Diameter Gy protocol
LI	Supports Lawful Intercept functions. Described in the *Configuring Lawful Intercept Application Note*.
SCE-Gx	Supports the Cisco Service Control Engine Gx protocol. If this mode is selected, Diameter 3GPP and RADIUS

Function	Description
	must also be selected, and other Gx sub-modes must not be selected.
Gx-Lite	Supports the Gx-Lite protocol, a simplified version of 3GPP Gx for use by non-GGSN PCEF vendors that do not have access to network-level information.
Cisco Gx	Supports the Cisco Gx protocol.
DSR	Supports Policy Management network segmentation using a Diameter Signaling Router.
KT	Supports the KT custom features.

SMS Mode Enables support of SMS servers. Functions are described in the *Configuration Management Platform Wireless User's Guide*.

Table 62: SMS Mode functions

Function	Description
SMPP	Supports SMS using SMPP protocol.
XML	Supports SMS using XML.

SPR Mode Enables support of subscriber database management. Select only one sub-mode. Functions are described in the Subscriber Data Management documentation.

Table 63: SPR Mode functions

Function	Description
Subscriber Profiles	Supports subscriber profile functions.
Quota	Supports subscriber quotas.

Wireline Mode Enables support of a wireline carrier environment. Functions are described in the *Configuration Management Platform Wireline User's Guide*.

SPC Mode Enables the COPS Application Manager product, which accepts service provisioning requests from a Session Border Controller over the Common Open Policy Service (COPS) protocol. Functions are described in the *Service Provisioning over COPS Application Manager User's Guide*.

RADIUS Mode Enables support of RADIUS AAA.

The management options are as follows:

- **Manage Policy Servers** — Manage MPE devices

- **Manage SIP-AM Servers** — Manage Session Initiation Protocol Application Manager (SIP-AM) servers
- **Manage MA Servers** — Manage Management Agent servers
- **Manage Policies** — Enable the policy wizard
- **Manage MRAs** — Manage Multi-Protocol Routing Agent servers
- **Manage SPR Subscriber Data** — Manage Subscriber Profile Repository servers
- **Manage Mediation Servers** — Manage Message Distribution Function servers
- **Manage Geo-Redundant MPE/MRA/BoD** — Manage georedundant MPE, MRA, or BoD clusters
- **Manager is HA (clustered)** — Enable High Availability features
- **Manage Analytic Data** — Enable output of policy event records

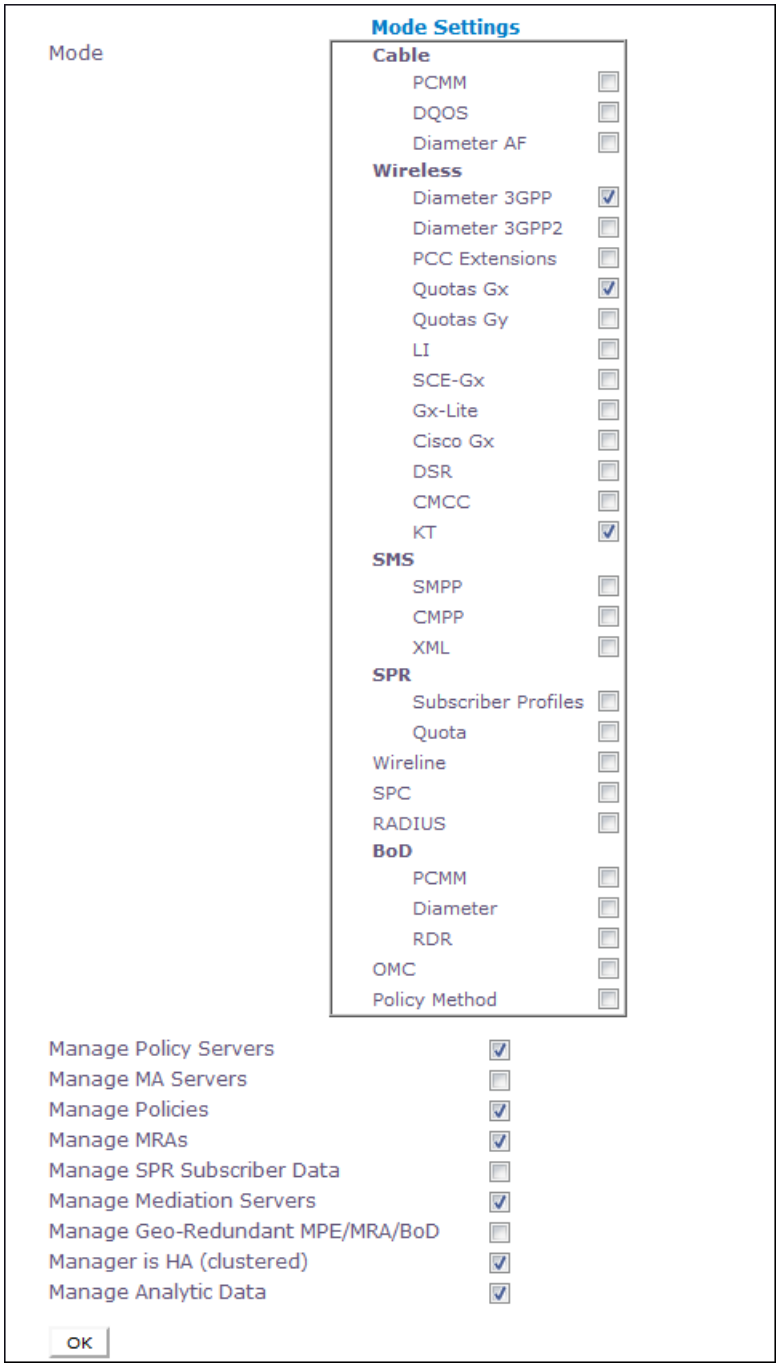


Figure 29: Mode Settings Page

Glossary

#

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

A

AAA	Authentication, Authorization, and Accounting (Rx Diameter command)
APN	Access Point Name The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.

C

charging server	An application that calculates billing charges for a wireless subscriber
CMP	Configuration Management Platform A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.

C

COMCOL	Communications Core Object Library A suite of re-usable C++ libraries, as well as processes and procedures available for use in Tekelec products. Many of its features are focused toward the communications area of software developments, although it purpose is not intended to restrict its functionality to any particular area
CPU	Central Processing Unit

D

Diameter	Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment.
Distinguished Name	A unique name for an entry in a directory service.
DNS	Domain Name System A system for converting Internet host and domain names into IP addresses.
DPI	Deep Packet Inspection is a form of packet filtering that examines the data and/or header part of a packet as it passes an inspection point. The MPE device uses DPI to recognize the application for

D

establishing QoS or managing quota. See also packet inspection.

dynamic quota

Allows modification of an existing quota. A dynamic quota consists of a pass or top-up.

E

E.164

The international public telecommunication numbering plan developed by the International Telecommunication Union.

event

In Policy Management, an expected incident that is logged. Events can be used for debugging purposes.

F

FQDN

Fully qualified domain name

The complete domain name for a specific computer on the Internet (for example, www.oracle.com).

A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GPRS

General Packet Radio Service

A mobile data service for users of GSM mobile phones.

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

G

Gx	The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.

H

HA	High Availability High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.
HTTP	Hypertext Transfer Protocol

I

IMSI	International Mobile Subscriber Identity A unique internal network ID identifying a mobile subscriber.
IP-CAN	Internet Protocol Connectivity Access Network Collection of network entities and interfaces that provide the underlying IP transport connectivity between the user equipment (UE) and the core network or backbone entities. An example IP-CAN is GPRS. An IP-CAN session can incorporate one or more IP-CAN bearers.
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

L

LDAP	Lightweight Directory Access Protocol A protocol for providing and receiving directory information in a TCP/IP network.
Lightweight Directory Access Protocol	See LDAP.

M

MCC	Mobile Country Code A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.
MNC	Mobile Network Code A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.
MPE	Multimedia Policy Engine A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization.

M

MRA	Multi-Protocol Routing Agent Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.
Multimedia Policy Engine	See MPE.

N

NAI	Network Access Identifier The user identity submitted by the client during network authentication.
network topology	A map of physical equipment or logical entities in a network.

O

OCS	Online Charging Server
OFCS	Offline Charging Server
OSSI	Operation Support System Interface An interface to a “back-end” (office) system. The Configuration Management Platform includes an OSSI XML interface.

P

packet inspection	Packet inspection (or shallow packet inspection) is a form of packet filtering that checks the header portion of a packet. See also deep packet inspection.
PCC	Policy and Charging Control

P

PCEF	Policy and Charging Enforcement Function Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.
PCRF	Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.
PDN	Packet Data Network A digital network technology that divides a message into packets for transmission.
policy and charging rules function	See PCRF.

Q

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

R

RADIUS	Remote Authentication Dial-In User Service

R

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

realm

A fundamental element in Diameter is the realm, which is loosely referred to as domain. Realm IDs are owned by service providers and are used by Diameter nodes for message routing.

S

SANE

Secure Access to Network Elements

Verizon Wireless's central authentication and auhorization system for network elements. It provides single-sign-on capability to network elements, for user of the SANE GUI client, and it allows network element vendors to use open-source, open-protocol methodologies to integrate clients int he Verizon Wireless security infrastructure.

SCTP

The transport layer for all standard IETF-SIGTRAN protocols.

SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

S

Secure Access to Network Elements	See SANE.
server	Any computer that runs TPD. Could be a Rack Mount Server or a Blade Server. In Policy Management, a computer running Policy Management software, or a computer providing data to a Policy Management system.
session	A Diameter session between the MPE and an external device (e.g., a Gx, Gxa, Gx-Lite or Rx session). Subscribers can maintain multiple sessions at any given time.
SGSN	Serving GPRS Support Node
SMPP	Short Message Peer-to-Peer Protocol An open, industry standard protocol that provides a flexible data communications interface for transfer of short message data.
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol

S

	arranges managed objects into groups.
SSO	Single sign-on
Subscriber Profile Repository	See SPR.

U

UE	User Equipment

X

XML	eXtensible Markup Language A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.