Policy Management
Configuration Management Platform

Wireless User's Guide

910-6402-001 Revision A
June 2012

Table of Contents

List of Figures

List of Tables

Chapter 1

About This Guide

Topics:

About This Guide describes the organization of the document and provides other information that could be useful to the reader.

Introduction

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

Conventions

The following conventions are used throughout this guide:

- **Bold text** in procedures indicates icons, buttons, links, or menu items that you click on.
- *Italic text* indicates variables.
- `Monospace text` indicates text displayed on screen.
- **`Monospace bold text`** indicates text that you enter exactly as shown.

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 Multimedia Policy Engine* provides an overview of the Multimedia Policy Engine (MPE), which manages multiple network-based client sessions; the network in which the MPE operates; policies; and the Configuration Management Platform (CMP), which controls MPE devices and associated applications.
- *Configuring the Policy Management Topology* describes how to set the topology configuration.
- *Managing MPE Devices* describes how to use the CMP to configure and manage the MPE devices in a network.
- *Configuring Protocol Routing* describes how to configure protocol routing.
- *Managing Network Elements* describes how to manage network elements.
- *Managing Application Profiles* describes how to manage application profiles.
- *Managing Match Lists* describes how to manage match lists, which provide whitelist and blacklist functions in the CMP.
- *Managing Quotas* describes how to manage Gx and Gy quotas.
- *Managing Services and Rating Groups* describes how to manage Gy services and rating groups.
- *Managing Traffic Profiles* describes how to manage traffic profiles.
- *Managing Retry Profiles* describes defines how to manage retry profiles.
- *Managing Charging Servers* describes how to manage charging servers.
- *Managing Policy Time Periods* describes how to manage time periods.
- *Managing Serving Gateways to MCCs/MNCs* describes how to map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs).
- *Managing Monitoring Keys* describes how to manage monitoring keys.
- *Managing Third-Party AVPs* describes how to manage attribute-value pair (AVP) data in Diameter messages issued by third-party vendors.
- *Managing Multi-Protocol Routing Agents* describes the Multi-Protocol Routing Agent (MPE), a standalone entity that supports MPE devices and is manageable by the CMP.

- *Managing Subscriber Profile Repositories* describes how to manage subscriber profile repositories (SPRs).
- *Understanding and Creating Policy Rules* describes policy rules, which dynamically control how an MPE device processes protocol messages as they pass through it.
- *Managing Policy Rules* describes how to manage your library of policy rules and policy groups.
- *Managing Policy Tables* describes how to manage policy tables.
- *Managing Subscribers* describes how to manage subscriber tiers and quota usage within the CMP.
- *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.
- *System Administration* describes functions reserved for CMP system administrators.
- The appendix, *CMP Modes*, lists the functions available in the CMP, 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:

- System operators
- System administrators

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

	**DANGER**: (This icon and text indicate the possibility of *personal injury*.)
	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

Phone:

1230-020-555-5468

- **Colombia**

  Phone:

  01-800-912-0537

- **Dominican Republic**

  Phone:

  1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552 (1-888-FOR-TKLC)

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91 124 436 8552 or +91 124 436 8553

    TAC Regional Support Office Hours:

10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

- **Singapore**

  Phone:

  +65 6796 2288

  TAC Regional Support Office Hours:

  9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Related Publications

The following publications provide additional information for the configuration and use of Policy Management products in a wireless environment:

- *Wireless Product Release Notes*
- *Policy Management Troubleshooting*
- *SNMP User's Guide*
- *OSSI XML Interface Definition*

The following documents are useful for reference:

- PCMM specifications PKT-SP-MM-I05
- Internet Engineering Task Force (IETF) RFCs:

  - RFC 4960: "Stream Control Transmission Protocol"
  - RFC 5321: "Simple Mail Transfer Protocol"

- IETF RADIUS-related RFCs:
  - RFC 2865: "RADIUS"
  - RFC 2866: "RADIUS Accounting"
  - RFC 3576: "Dynamic Authorization Extensions to RADIUS"

- IETF Diameter-related RFCs:
  - RFC 3539: "Authentication, Authorization and Accounting (AAA) Transport Profile"
  - RFC 3588: "Diameter Base Protocol"
  - RFC 3589: "Diameter Command Codes for 3GP (Release 5)
  - RFC 4006: "Diameter Credit Control Application (DCCA)"

- 3rd Generation Partnership Project (3GPP) technical specifications:
  - 3GPP TS 23.003: "Numbering, addressing and identification (Release 9.7)"
  - 3GPP TS 23.039: "Interface Protocols for the Connection of Short Message Service Centers (SMSCs) to Short Message Entities (SMEs)"
  - 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)"
  - 3GPP TS 23.203: "Policy and charging control architecture (Release 8.5)"
  - 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 reference point (Release 11.2)"
  - 3GPP TS 29.213: "Policy and Charging Control signalling flows and QoS parameter mapping (Release 9.6)"
  - 3GPP TS 29.214: "Policy and Charging Control over Rx reference point (Release 9.7)"
  - 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 8.12)"
  - 3GPP TS 29.328: "IM Subsystem Sh Interface; Signalling flows and message contents (Release 9.2)"
  - 3GPP TS 29.329: "Sh Interface based on the Diameter protocol (Release 9.2)"

- 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 Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

The Multimedia Policy Engine

Topics:

The Multimedia Policy Engine provides an overview of the Policy Management Multimedia Policy Engine (MPE), which manages multiple network-based client sessions; the network in which the MPE operates; policies; and the Configuration Management Platform (CMP), which controls MPE devices and associated applications.

The Multimedia Policy Engine

The Multimedia Policy Engine (MPE) device provides a policy and charging rules function (PCRF) as defined in 3GPP 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.

Understanding Policy Rules

A policy rule is an if-then style rule that has a set of conditions and actions. If the conditions are met, the actions are performed. You create policy rules within the CMP, using a wizard that contains a large number of conditions and actions to assist you in the construction of policy rules. Once you create policy rules, you deploy them to MPE devices.

You can combine policy rules to provide additional power and flexibility. When there are multiple policy rules, the order in which the policy rules are evaluated can also influence MPE device behavior, so the order of evaluation is also configurable through the CMP. You can also organize policy rules into groups to simplify the management of policy rules. You can cause groups of rules to be executed.

The following are sample scenarios for which you might use policy rules:

- You can modify the contents of protocol messages using policy rules. For example, you could use a policy rule to override the requested bandwidth parameters in a request.
- You can create policy rules that track the use of resources for devices in the network and implement limits on how those resources are used.
- Some protocols allow for the provisioning of default QoS parameters for subscribers. With these protocols, policy rules can implement subscriber tiers where different subscribers have different bandwidth available.
- You can configure policy rules to monitor the reservation of bandwidth on network elements and notify operators when an element exceeds certain threshold levels.

Overview of Major Tasks

The major tasks involved in using MPE devices are configuration, defining manageable elements and profiles, creating and deploying policy rules, managing subscribers and licenses, and administering the authorized CMP users.

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

1. Configure the Policy Management topology, which defines the addresses of Policy Management clusters in your network. This step is described in *Configuring the Policy Management Topology*.
2. Configure protocol routing, which enables a Policy Management device to forward requests to other Policy Management devices for further processing. This step is described in *Configuring Protocol Routing*.

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

1. Create network element profiles, including protocol options, for each network element with which the MPE devices interact. This task is described in *Managing Network Elements*.
2. Specify which MPE device will interact with which network element(s). This task is described in *Managing Network Elements*.
3. Create application profiles, which specify protocol information to associate each request with an application. This task is described in *Managing Application Profiles*.
4. Create match lists, which provide whitelist and blacklist functions. This task is described in *Managing Match Lists*.
5. Create Gx and Gy quotas, which set limits on a subscriber's usage. This task is described in *Managing Quotas*.
6. Create Gy services, which identify a class of traffic and can be collected into rating groups. This task is described in *Managing Services and Rating Groups*.
7. Create traffic profiles, which define default settings for protocol messages. This task is described in *Managing Traffic Profiles*.
8. Create retry profiles, which specify the circumstances under which installation of certain rules is retried in the event of a failure. This task is described in *Managing Retry Profiles*.
9. Define charging servers, which are applications that calculate billing charges for a wireless subscriber. This task is described in *Managing Charging Servers*.
10. Define policy time periods to specify in policy time-of-day conditions. This task is described in *Managing Policy Time Periods*.
11. Map serving gateways to mobile country codes (MCCs) and mobile network codes (MNCs). This task is described in *Managing Serving Gateways to MCCs/MNCs*.
12. Define monitoring keys, which are unique strings that identify the quota profile to be used by certain rules for usage tracking. This task is described in *Managing Monitoring Keys*.
13. Define how policy rules will process attribute-value pairs (AVPs) used in Diameter messages by third-party vendors. This task is described in *Managing Third-Party AVPs*.
14. Configure Multi-Protocol Routing Agents, which are Policy Management devices that can route requests to MPE devices. This task is described in *Managing Multi-Protocol Routing Agents*

The steps to create and deploy policy rules must be done in the following order:

1. Create policy rules on the CMP device. This step is described in *Understanding and Creating Policy Rules*.
2. Deploy the policy rules from the CMP to MPE devices. This step is described in *Managing Policy Rules*.
3. You may decide to consolidate policy rules with similar structures using a policy table. This step is described in *Managing Policy Tables*.

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

- Manage subscriber profiles on subscriber profile repositories (SPRs). This task is described in *Managing Subscriber Profile Repositories*.
- Manage subscriber tiers and quota usage. This task is described in *Managing Subscribers*.
- View reports 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. This task is described in *System Administration*.

- Upgrade software using the Upgrade Manager GUI page. This page is described in *Upgrade Manager*.

The Configuration Management Platform

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

- Configuration and management of MPE, MRA, and 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 MPE and CMP software

Organizing Policy Rules

The CMP includes features to simplify the management of multiple policy rules.

The order in which rules are evaluated is important. The CMP lets you configure the evaluation order of policies. See *Structure and Evaluation of Policy Rules*.

The CMP provides a policy template feature to simplify the creation of multiple policy rules that have similar conditions and actions. Once you create a policy template, you can use it to create additional rules. See *Creating a Policy Template*.

The CMP also provides a policy rule grouping feature. Policy rules can be organized into groups and the groups can be used to simplify the process of deploying policies to MPE devices. See *Creating a Policy Group*. Policy rule groups can be executed with a single action. See *Structure and Evaluation of Policy Rules*.

Policies with similar conditions or actions can be consolidated into tabular form. See *Managing Policy Tables*.

GUI Overview

The CMP uses an intuitive and highly portable Graphical User Interface (GUI) supporting industry-standard web technologies (SSL, HTTP, HTTPS, IPv4, IPv6, and XML). *Figure 1: Structure of the CMP GUI* shows the structure of the CMP GUI.

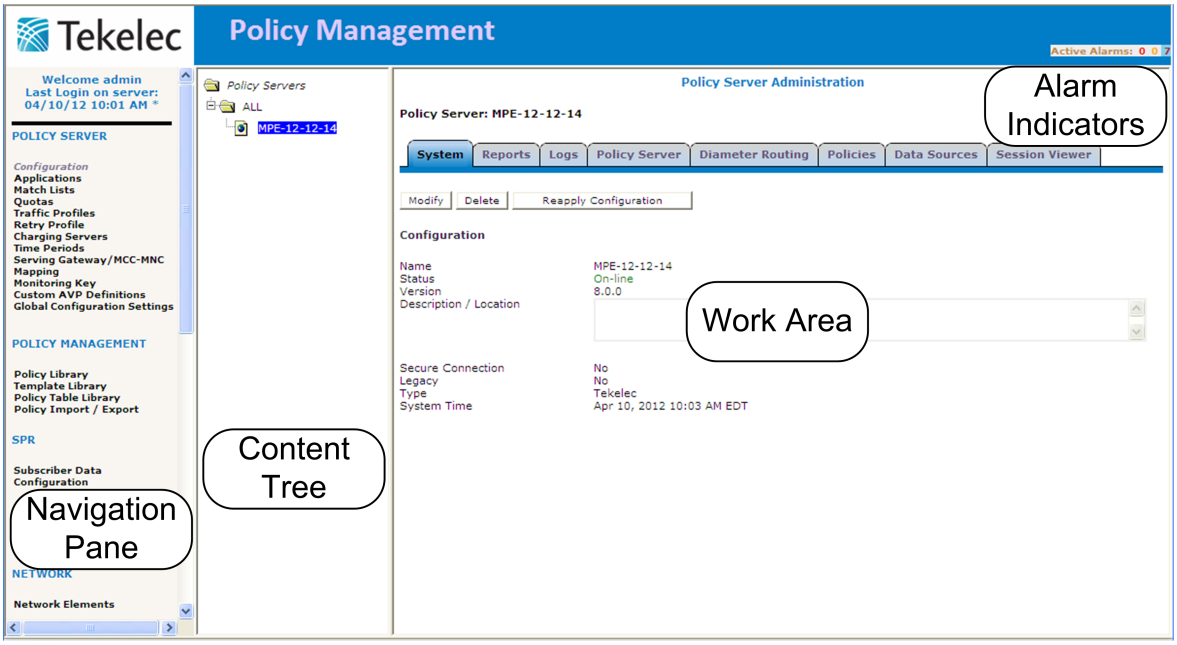


Figure 1: Structure of the CMP GUI

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

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

Specifications for Using the GUI

Tekelec recommends the following:

- **Web Browsers** —
  - Mozilla Firefox release 3.6
  - Microsoft Internet Explorer 8.4 or higher, on Windows XP
- **Monitor** — 1024 x 768 or higher

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

GUI Icons

The CMP provides icons for removing, deleting, or changing the sequential order of items displayed in a list:

 **Remove icon** — When visible in the work area, selecting the Remove icon removes an item from the group it is associated with. The item is still listed in the ALL group and any other group that it is currently associated with. For example, if you remove MPE device PS_1 from policy server group PS_Group2, PS_1 still displays in the ALL group.

 **Delete icon** — When visible in the work area, selecting the Delete icon deletes an item, removing it from the MPE device.

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

 **Move icon** — The up/down arrow icons are displayed when it is possible to change the sequential order of items in a list.

Shortcut Selection Keys

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

- **Shift/click** — selects two or more consecutive items. To do this, select the first item, then Shift/click on a second item to select both items and all items in between.
- **Control/click** — selects two or more non-consecutive items. To do this, hold down the Ctrl key as you click on each item.

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.
3. When you finish, click **Change Password**.

Your password is changed.

Chapter 3

Configuring the Policy Management Topology

Topics:

Configuring the Policy Management Topology describes how to configure the CMP to manage the other Policy Management devices in a network.

About the Policy Management Topology

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

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

Figure 2: 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.

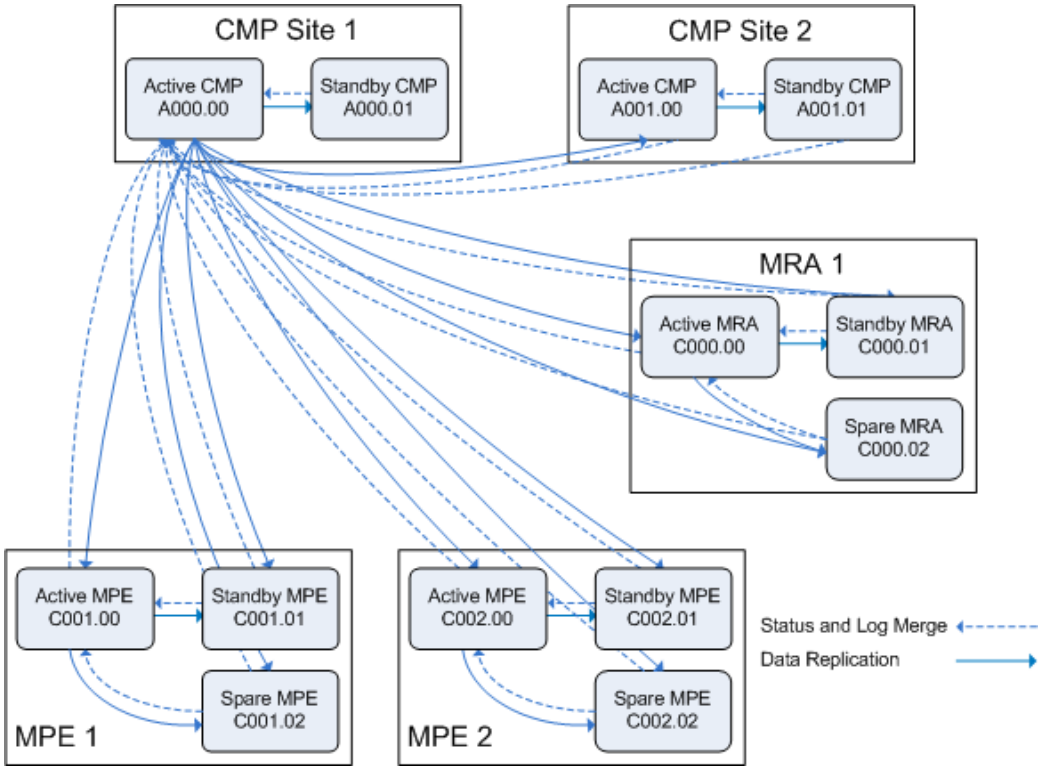


Figure 2: Policy Management Topology

High Availability

High Availability is provided for CMP, MPE, and MRA cluster configurations. High Availability is afforded by using two servers per cluster, an active server and a standby server per cluster. As shown in *Figure 3: 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 through the Operation, Administration, and Management (OAM) network. The servers work collaboratively as follows:

1. The active server establishes a TCP link to the standby server, and uses this link to continuously replicate topology and application configuration to the standby server.
2. The standby server establishes a separate TCP link back to the active server, and uses this link to continuously report events and alarms. The standby server has current data but does not process it.
3. The servers share a virtual IP (VIP) cluster address to support automatic failover.
4. The COMCOL database runtime process constantly monitors the status of both servers in the cluster.
5. If the active server fails, it instructs the standby server to take over and become the active server.

The terms "active" 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 become the active server. (For example, this would occur if the active server became unresponsive.) When this happens, the server that was previously the active server assumes the role or state of the standby server.

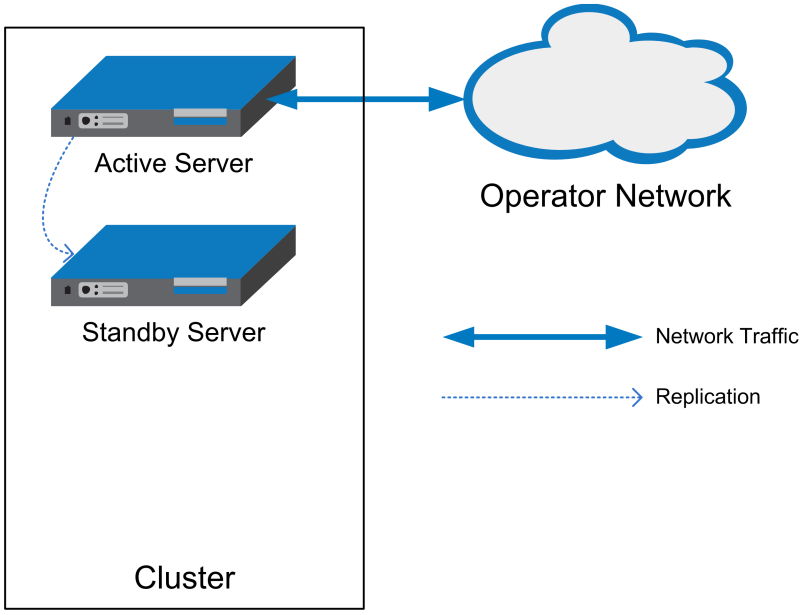


Figure 3: High Availability

MPE and MRA Georedundancy

As shown in *Figure 4: MPE or MRA Cluster with Active, Standby, and Spare Servers*, an MPE or MRA cluster can contain an additional server, called a spare server. The active server will replicate its database to the spare server as well as the standby server. In this configuration, the standby server is first in line to take over from the active server, and the spare is second in line.

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

The additional (spare) server need not be physically close to the active and spare servers. Georedundancy is an optional configuration provided for MPE and MRA clusters in which the spare server is located in a separate geographical location, as shown in *Figure 5: MPE or MRA Georedundant*

Configuration. If the two servers at one site become unavailable, the third server, located at another site, would continue to provide service.

Note: The CMP supports georedundancy as an optional configuration mode. This mode must be configured before your CMP system will display georedundancy options. Contact Customer Support to change an existing CMP system to support georedundant MPE or MRA clusters.

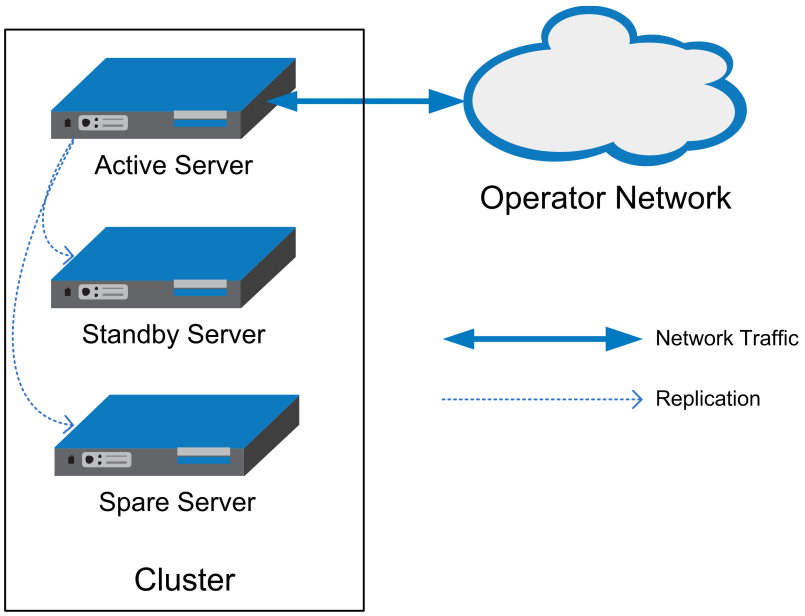


Figure 4: MPE or MRA Cluster with Active, Standby, and Spare Servers

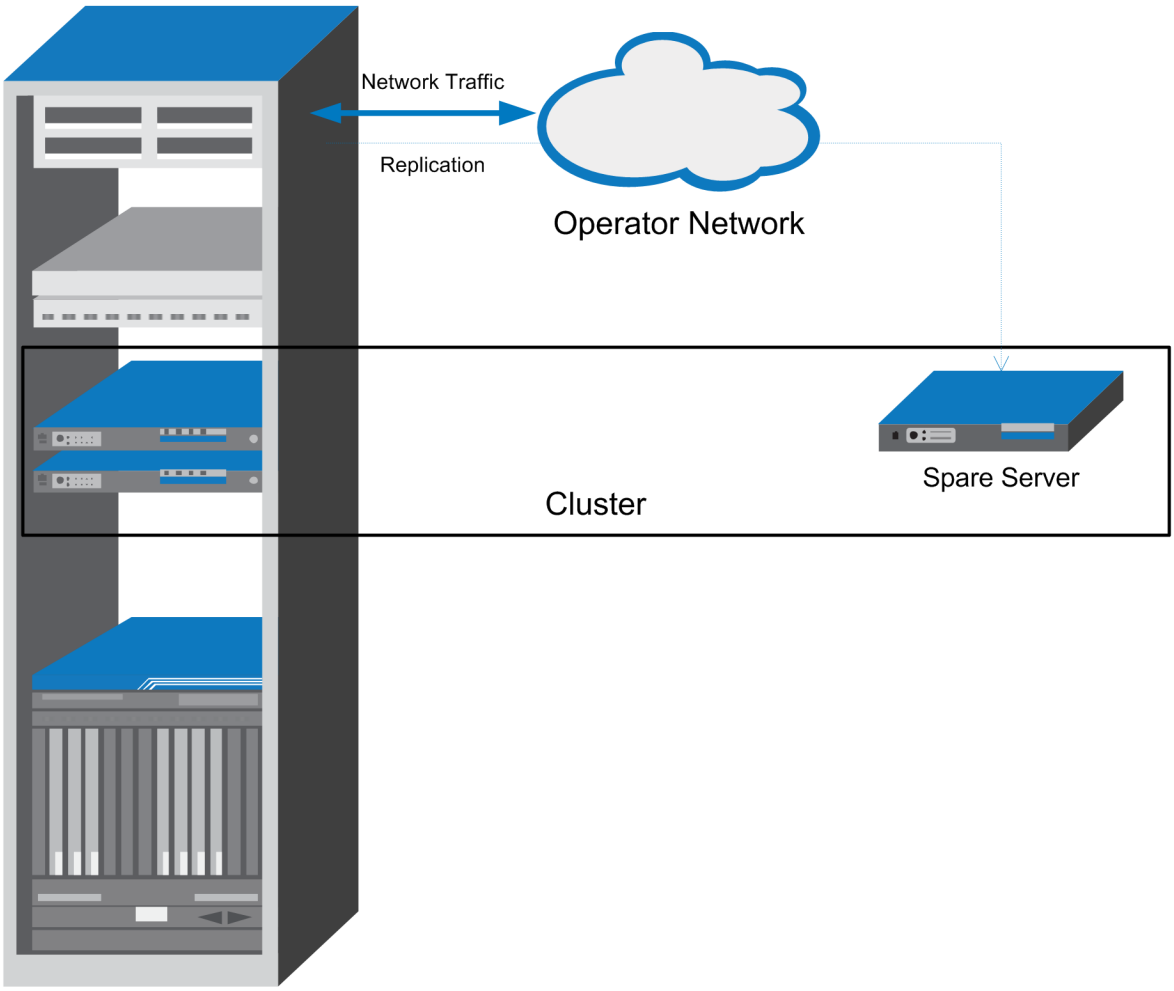


Figure 5: MPE or MRA Georedundant Configuration

CMP Georedundancy

As shown in *Figure 6: CMP Georedundancy*, georedundancy is implemented for CMP clusters by pairing a primary site CMP cluster with a secondary site cluster. The active server from the Site 1 CMP cluster will continuously replicate topology and application data to active server of the Site 2 cluster.

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

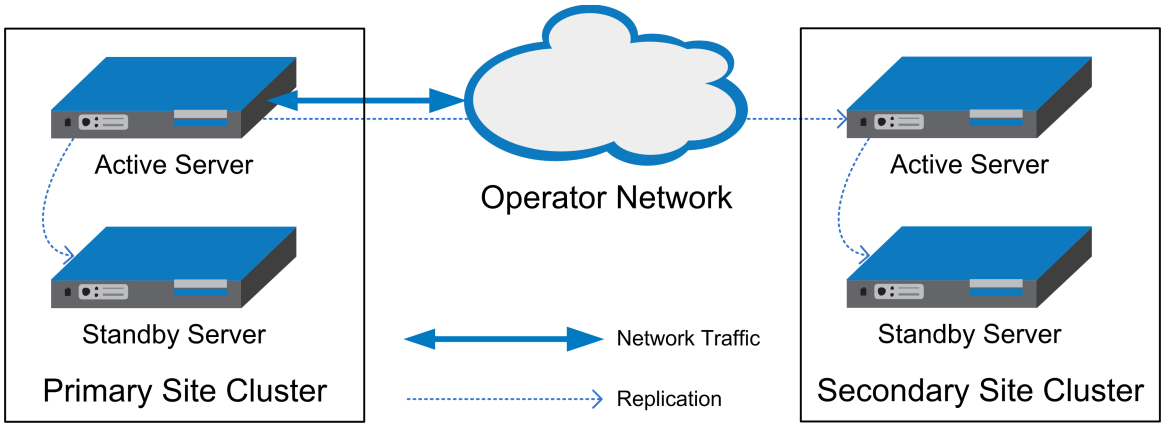


Figure 6: CMP Georedundancy

Primary and Secondary Sites

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

"Secondary" refers to the georedundant backup site, server, and connection. MPE and MRA clusters can be dispersed between a primary site and a secondary site. This dispersal mates the primary and secondary sites together.

If for some reason the active server at a primary site can no longer provide service, the cluster fails over to the standby server at the primary site. The server assuming the service becomes the active server. If and only if no servers are available at a primary site, the cluster fails over to the secondary site, and a server takes over as the active server in the cluster and provides service.

When one of the servers at the primary site is once again able to provide service, then the "active" status transitions back to the server at the primary site.

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

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

Cluster Preferences

When you configure a georedundant MPE or MRA cluster, you initially designate a server as active, standby, or spare. This determines which site initially processes traffic. Once defined, you can reverse this preference, which has the effect of making the spare server the active server and the active server the spare server. This is useful in situations where you need to troubleshoot, service, upgrade, or replace the active server.

The Cluster Settings table on the Cluster Configuration page lists information on MPE or MRA cluster preferences under the heading "Site Preference." A cluster preference is either "Normal," "Reverse," or "N/A" for CMP clusters, which cannot be reversed.

Server Status

The status of a server can be thought of as its current role. The status describes what function the server is currently performing in the cluster. Statuses can change from server to server within a cluster, but no two servers in the same cluster should ever have the same status. (Two servers in the same cluster with the same status is an error condition.)

The status values are as follows:

- **Active:** The active server in a cluster is the server that is the externally connected. The active server is the only server that is handling connections and servicing messages and requests. Only the active server writes to the database. An active server at the primary site remains active unless it cannot provide service. An active server at the secondary site will remain active as long as no server is available to provide service at the primary site.
- **Standby:** The standby server in a cluster is the server that is prepared to immediately take over in the event that the current active server is no longer able to provide service. If the standby server takes over, it becomes the active server. Once the previously active server has recovered, it reverts to its former status of standby 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 demotes itself and reverts to its former status of spare or standby (depending on the availability of the other servers in the cluster).
- **Out of Service:** If a server has failed and is unavailable to assume any of the other roles, then its status is out of service. A server is reported as out of service in two scenarios:
  - The CMP system can reach the server, but the software service on the server is down
  - The CMP system cannot reach the server

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

Setting Up the Topology

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

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

1. Configure the primary CMP cluster — You start to build a topology by logging in to the active CMP server at the primary site. Configure the CMP cluster settings. The settings are replicated (pushed) to the standby CMP server. Together, the two servers form a primary, or Site 1, CMP cluster. This is the primary CMP site for the whole topology network. The primary site cannot be deleted from the topology.
2. Configure the secondary CMP cluster (optional) — Use the primary CMP cluster to configure a secondary, or Site 2, CMP cluster. A secondary CMP cluster can provide georedundancy.

3. Configure MPE and MRA clusters — Enter MPE and MRA cluster settings on the active CMP server on the primary site. You can define the topology before defining the servers themselves. Once defined, the configuration information is replicated as follows:
   a. The active CMP server establishes a TCP link to both the active and standby MPE or MRA servers through the OAM network. The topology configuration, including the cluster settings, is replicated to both servers. These servers form an MPE or MRA cluster based on the topology configuration.
   b. Each MPE or MRA server establishes a separate TCP link back to the active CMP server, and uses this link to continuously report events and alarms.
   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. In a georedundant topology, if both the active and standby servers fail, it instructs the spare server to take over and become the active server.
4. For georedundancy (optional), configure additional sites for MPE and MRA clusters.

Once you define the topology, use the Topology column, on the Reports tab of each server, to determine if there are any topology mismatches. See *Cluster Information Report* 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 at least one server
- The gateway address and default route are properly configured on the CMP server
- The CMP server IP connection is active
- The CMP application is running on at least one server

To set up the primary CMP cluster:

1. Log in to the CMP server.
2. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens. If a primary cluster is not yet defined, you are prompted: "Initial Configuration Detected. Please add CMP Site 1 Cluster."
3. Click **Add CMP Site1 Cluster**.
   The Cluster Settings Page opens. The cluster name and application type are fixed.
4. Enter the following information (*Figure 7: Cluster Settings Page for CMP Cluster* shows an example):
   a) **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).
   b) **Network VLAN IDs** (appears if you selected **C-Class** or **C-Class(Segregated Traffic)**) — 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.

      The VLAN ID must be part of the device name. For example, if a VIP is on a VLAN with ID=230, the device name for this VIP must be "bond0.230." Enter a VLAN ID for each VIP.

c) **OAM VIP** (required) — Enter the IPv4 address and mask of the OAM VIP. The OAM VIP is the IP address the CMP uses to communicate with an MPE or MRA 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.

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.

5. Select **Server-A** and enter the following information for the first server of the cluster:
   a) **IP** (required) — The IP address of the server. Enter the standard dot-formatted IP 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`).
   c) **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.
6. Once you define a Server A, you can select **Server-B** to enter the appropriate information for the second server of the cluster.
7. When you finish, click **Save** (or **Cancel** to discard your changes).
   You are prompted, "Active server will restart and you will be logged out." The active server restarts.

The CMP cluster topology is defined.

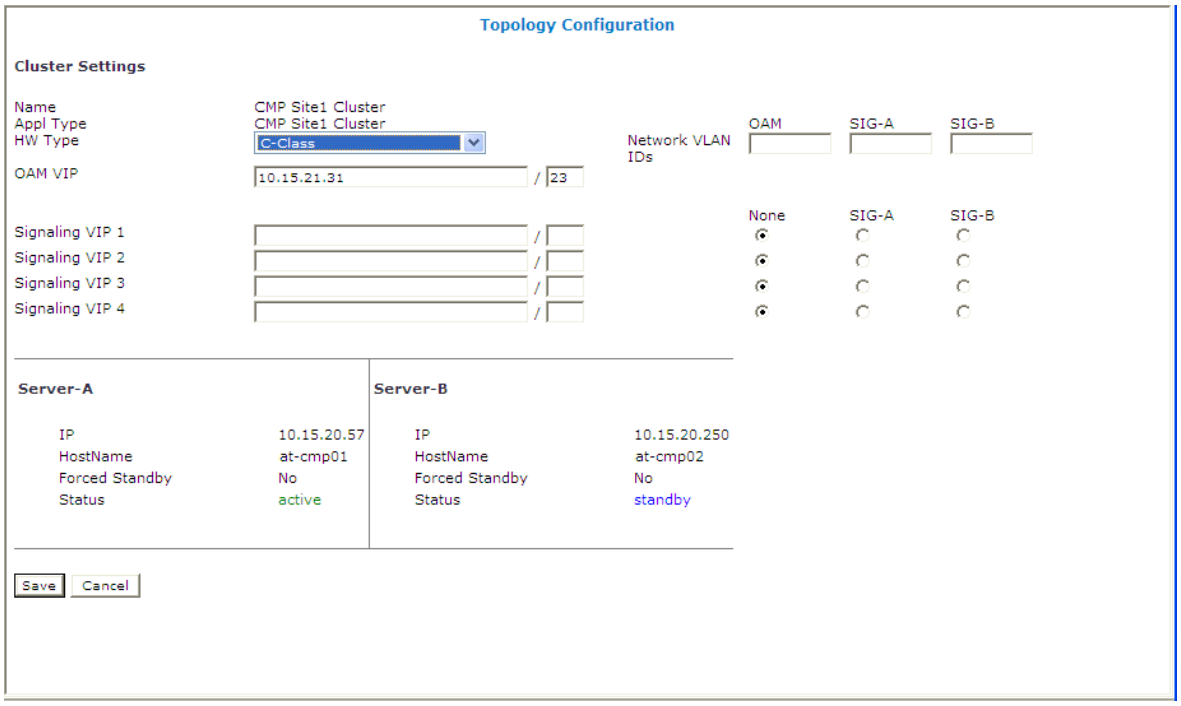


Figure 7: Cluster Settings Page for CMP Cluster

Once the topology is defined, use the Topology column, on the Reports tab, to determine if there are any topology mismatches. See *Cluster Information Report* for more information.

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

Setting Up a Site

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

To set up a site:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens.
2. From the content tree, select the **All Sites** group.
   The Site Configuration page opens.
3. On the Site Configuration page, click **Create Site**.
   The New Site page opens.
4. Enter values for the configuration attributes:
   a) **Name** (required) — The site name. Enter up to 32 alphanumeric characters, underscores (_), or hyphens (-).
   b) **Max Primary Site Failure Threshold** — If the number of MPE or MRA pair failures reaches this threshold, a trace log entry and a major alarm are generated.

      A pair failure is recorded when both servers at a primary site are either out of service or in forced standby. You can optionally enter a number up to the total number of servers provisioned at this site. The default is no threshold.
5. When you finish, click **Save** (or **Cancel** to abandon your request).
   The site configuration is saved in the CMP database.

The site is defined.

If you need to define multiple sites, repeat steps 3 through 5 as necessary.

Setting Up an MPE Cluster

To define an MPE cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens.
2. Click **Add MPE/MRA Cluster**.
   The Cluster Settings 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).
   c) **Site Preference** — Select **Normal** (the default) or **Reverse**.

      This field only appears on the page if the CMP system supports georedundancy.

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

e) **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).

f) **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.

   The VLAN ID must be part of the device name. For example, if a VIP is on a VLAN with ID=230, the device name for this VIP must be "bond0.230." Enter a VLAN ID for each VIP.

g) **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 uses to communicate with the MPE 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.

h) **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, 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 MPE cluster. (To support redundant communication channels, an MPE cluster uses both **SIG-A** and **SIG-B**.) 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 an MPE /MRA cluster, at least one signaling VIP is required (whether it's SIG-A or SIG-B).

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 (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. (Optional) **Secondary Site** — For a georedundant cluster, select the name of a previously defined site. The secondary site name must be different from the primary site name.

   This section only appears on the page if the CMP system supports georedundancy.

7. (Optional) For a georedundant cluster, click **Add Server-C** and enter the appropriate information for the spare server of the cluster.

   This section only appears on the page if the CMP system supports georedundancy. If you define a secondary site, you must define a spare server.

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

The MPE cluster is defined.

Once the topology is defined, use the Topology column, on the Reports tab, to determine if there are any topology mismatches. See *Cluster Information Report* for more information.

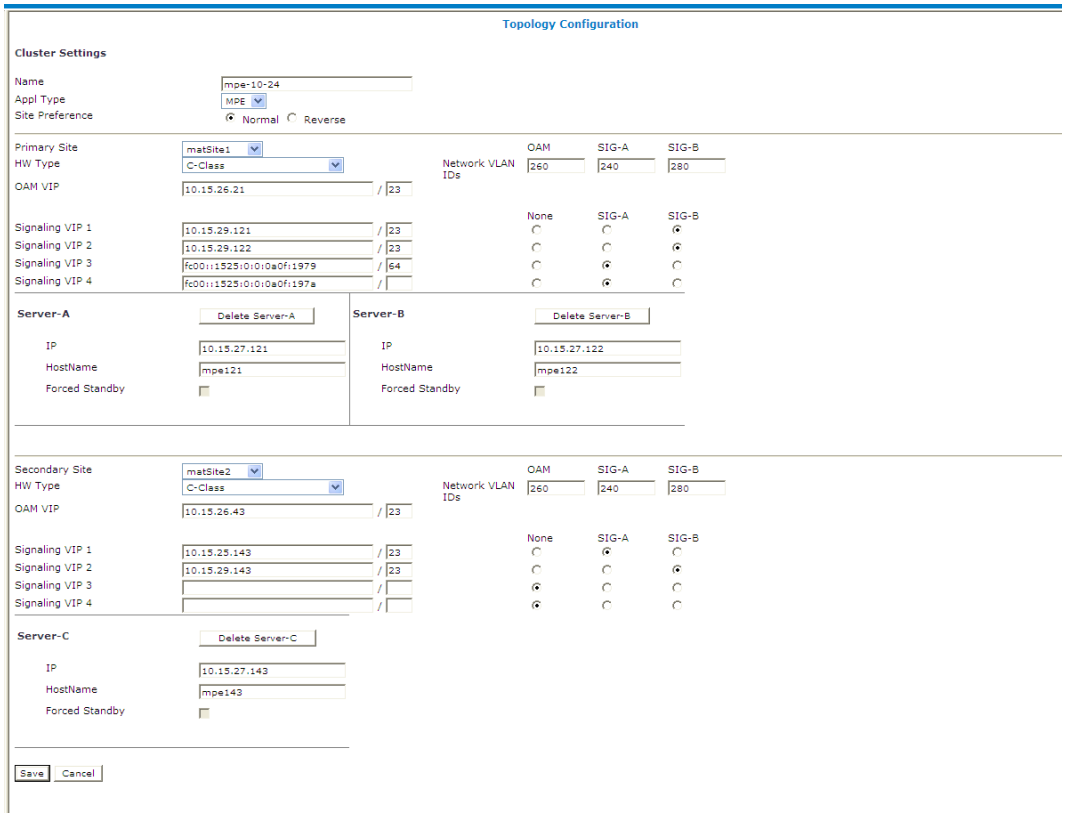


Figure 8: Cluster Settings Page for MPE Cluster

Modifying the Topology

Once the topology is configured, you can change it as necessary, 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, or 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 the topology is described in the following topics:

- *Modifying a Site*
- *Removing a Site from the Topology*
- *Modifying an MPE or MRA Cluster*
- *Modifying a CMP Cluster*
- *Removing a Cluster from the Topology*
- *Reversing Cluster Preference*
- *Demoting a CMP Cluster*
- *Forcing a Server into Standby Status*

Modifying a Site

To modify a site:

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

The site is modified.

Removing a Site from the Topology

You can remove a site from a georedundant topology. You can only remove a site if it is not referenced by an MPE or MRA cluster. Once it is in use by a cluster, if you try to delete it, you are prompted, "*Site* cannot be deleted because it is referred in following clusters: *cluster1*[, *cluster2*[,...]]"

To remove a site from the topology:

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

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

The site is removed from the topology.

Modifying an MPE or MRA Cluster

To modify an MPE or MRA cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens.
2. From the content tree, select the cluster you want to modify.
   The Topology Configuration page opens, displaying information about the cluster.
3. On the Topology Configuration page, 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 Primary Site**.
- To modify the secondary site configuration, click **Modify Secondary Site**.
- To delete the secondary site configuration, click **Delete Secondary Site**.

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 both servers of an MPE or MRA cluster.

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

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

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

Modifying a CMP Cluster

To modify a CMP cluster:

1. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens.
2. From the content tree, select the cluster you want to modify.
   The Topology Configuration page opens, displaying information about the cluster.
3. On the Topology Configuration page, click the appropriate 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 appropriate fields on the Topology Configuration page become editable. For information on configurable fields, see *Setting Up a CMP Cluster*.
4. Make changes as required.

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

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

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

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

Removing a Cluster from the Topology

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

The cluster is removed from the topology.

Reversing Cluster Preference

You can change the preference, or predilection, of the servers in a cluster to be active or spare.

To reverse cluster preference:

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

The cluster preferences are reversed.

Demoting a CMP Cluster

In a two-cluster CMP topology, you can demote the primary cluster (which is typically the Site 1 cluster) to secondary status. You would do this, for example, prior to performing maintenance or an upgrade, or if the primary cluster has failed completely and is unreachable.

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

CAUTION

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

To demote a CMP cluster:

1. Log in to the currently active georedundant CMP cluster.
2. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens, displaying a cluster settings table listing information about the clusters defined in the topology. The name of the primary CMP cluster is marked with "(P)," and the name of the secondary cluster is marked with "(S)." You should see options to **View** and **Demote**.
3. Open a second browser window and log in to the secondary CMP cluster.
   The page displays the message "This server you signed in is the Secondary Active Server."
4. From the **Platform Setting** section of the navigation pane, select **Topology Setting**.
   The Topology Configuration page opens, displaying a cluster settings table listing information about the clusters defined in the topology. You should see options to **View** and **Promote**.

   CAUTION

   CAUTION: If you do not see the same information in both steps 2 and 4, stop this procedure and do not try to change the current active georedundant cluster. Contact Tekelec Support before proceeding.

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

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

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

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

Forcing a Server into Standby Status

You can change the status of an active or spare server in a cluster to Standby. 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 the status or roles of the other servers in the cluster.
- The server continues as part of its cluster, and reports its status as "Forced-Standby."

To force a server into standby status:

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

The server is placed in standby status.

Configuring SNMP Settings

The CMP system provides a screen for configuring SNMP settings for the CMP system and all MPE and MRA servers in the topology network.

Note: SNMP settings configuration must be done on a server that is the Active Server in the Primary Cluster. A banner warning appears if the login is not on the primary/active CMP. SNMP cannot be configured from servers other than the active/primary CMP.

To configure SNMP settings, do the following:

1. Log into the CMP system from its server address as the Administration user.

   The CMP **Navigation Pane** is displayed.
2. Click on the **SNMP Setting** link under **Platform Setting**.

   The SNMP Settings attributes are displayed.
3. Click on the **Modify** button.

The **SNMP Settings** edit screen is displayed.

4. Edit the SNMP Settings attributes that need to be entered or changed.

   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 address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. The field is required to allow the Manager to receive traps. By default, these fields are empty. **Note:** The IPv6 address is not supported.
Enabled Versions	Supported SNMP versions: • SNMPv2c • SNMPv3 • SNMPv2c and SNMPv3 (default)
Traps Enabled	Enable sending SNMPv2 traps (default is box check marked) Disable sending SNMPv2 traps (box not check marked)
Traps from Individual Servers	Enable sending traps from an individual server (box check marked). Sending traps from the active CMP (default is box not check marked)
SNMPv2c Community Name	The SNMP read-write community string. The field is required if SNMPv2c is enabled. The name can contain alphanumeric characters and cannot exceed 31 characters in length. The name cannot be either “private” or “public”. The default value is “snmppublic”.

Field Name	Description
SNMPv3 Engine ID	Configured Engine ID for SNMPv3. 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 Username	The SNMPv3 User Name. The field is required if SNMPv3 is enabled. The name must contain alphanumeric characters and cannot not exceed 32 characters in length. The default value is “TekSNMPUser”.
SNMPv3 Security Level	SNMPv3 Authentication and Privacy options. **1.** “No Auth No Priv” - Authenticate using the Username. No Privacy. **2.** “Auth No Priv” - Authentication using MD5 or SHA1 protocol. **3.** “Auth Priv” - Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol. The default value is “Auth Priv”.
SNMPv3 Authentication Type	Authentication protocol for SNMPv3. Options are: **1.** “SHA-1” - Use Secure Hash Algorithm authentication. **2.** “MD5” - Use Message Digest authentication. The default value is “SHA-1”.
SNMPv3 Privacy Type	Privacy Protocol for SNMPv3. Options are: **1.** “AES”: Use Advanced Encryption Standard privacy. **2.** “DES”: Use Data Encryption Standard privacy. The default value is “AES”.
SNMPv3 Password	Authentication password for SNMPv3. This value is also used for msgPrivacyParameters.

Field Name	Description
	The field is required If SNMPv3 is enabled. The length of the password must be between 8 and 64 characters; it can include any character. The default value is “snmpv3password”.

5. Click **Save** to save the changes, or **Cancel** to discard the changes.

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 **Policy Server** section of the navigation pane, select **Global Configuration Settings**.
   The content tree displays a list of global configuration settings; the initial group is **Precedence Range**.
2. From the content tree, select the **Precedence Range** group.
   The Precedence Range Configuration page opens in the work area.
3. On the Precedence Range Configuration page, click **Modify**.
   The Modify Precedence Range page opens.
4. Enter values for the configuration attributes:
   a) **AF-Triggered** — Enter the minimum and maximum values for rules triggered by Rx requests. The default range is 400 to 899.
   b) **UE-Triggered** — Enter the minimum and maximum values for rules triggered by user equipment-initiated resource requests. This range cannot overlap with the AF range. The default range is 1000 to 1999.
   c) **Default Session** — If no other rules are installed when a Gx eHRPD, E-UTRAN, or GPRS session is established, a default rule is installed. Enter the default session precedence. The default precedence is 3000.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Precedence Range Configuration page closes.

The reserved precedence ranges are configured.

Precedence values not set aside here are available for your use in defining rules. By default, you can use 0–399, 900–999, 2000–2999, and 301–4,294,967,295.

Range changes do not automatically cause deployed rules to be redeployed with new precedence values. Also, range changes do not automatically cause revalidation of defined traffic profiles.

When traffic profiles are imported, they are imported regardless of their configured precedence values. The CMP system displays a message reminding you to check the precedence values of the imported traffic profiles. See *Importing an XML File to Input Objects* for more information.

Setting UE-Initiated Procedures

When enabled, this feature allows the MPE 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, do the following:

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 **UE-Initiated Procedures**.
   The UE-Initiated Procedures page opens in the work area group.
3. On the UE-Initiated Procedures page, 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). 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 1 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 256 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 1 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 256 characters in length. The default name is 3GPP.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The UE-Initiated Procedures page closes.

The UE-initiated attributes are configured.

Setting Stats Settings

You can define when and how measurement statistic values are reset.

To change stats settings, do the following:

1. From the **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 **Stats Settings**.
   The Stats Settings page opens in the work group area.
3. On the Stats Settings page, click **Modify**.
   The Modify Stats Settings page opens.
4. Enter values for the configuration attributes:
   a) **Stats Reset Configuration** — From the pulldown menu, select **Manual** or **Interval**. When in Manual mode, numeric values can only reset when the system restarts (for example, on failover or initial startup) or when you issue a reset command. Manual mode disables the resetting of numeric fields at regular intervals but does not alter historical data collection. When configured for Interval mode, numeric values are reset at regular intervals, controlled by the Stats Collection Period variable. In Interval mode, a reset occurs on the hour and then every 5, 10, 15, 20, 30 or 60 minutes afterwards, depending on the value selected in Stats Collection Period, providing a better idea of the performance of the Policy Management system at specific times of day. Default value is Manual.
   b) **Stats Collection Period** — When the Stats Reset Configuration variable is set to Interval, specify the time interval to use from the pulldown menu. Options are 5, 10, 15, 20, 30, and 60 minutes.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Stats Settings page closes.

The Stats Settings attributes are configured.

Setting Quota Settings

This feature defines the quota pools.

To enable or disable processing of the Quota Settings procedures or to change configuration attributes, do the following:

1. From the **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 **Quota Settings** folder.
   The Quota Settings page opens in the work area.
3. On the Quota Settings page, 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** (or **Cancel** to discard your changes).
   The Quota Settings page closes.

The Quota Setting attributes are configured.

Chapter 4

Managing MPE Devices

Topics:

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

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

Policy Server Profiles

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

The following subsections describe how to manage policy server profiles. For information on deploying defined policies to an MPE device, see *Deploying a Policy or Policy Group to MPE Devices*.

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 policy server groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, click **Create Policy Server**.
   The New Policy Server page opens.
4. Enter values for the configuration attributes:
   a) **Associated Cluster** (required) — Select the cluster with which to associate this MPE device.
   b) **Name** — Name of this MPE device. The default is the associated cluster name. A name is subject to the following rules:
      - Is case insensitive (uppercase and lowercase are treated as the same)
      - Must be no longer than 255 characters
      - Must not contain quotation marks (") or commas (,)
   c) **Description / Location** (optional) — Information that defines the function or location of this MPE device.
   d) **Secure Connection** — Designates whether or not to use the HTTPS protocol.
   e) **Type** — Defines the policy server type:
      - **Tekelec** (the default) — The policy server is an MPE device and can be fully managed by the CMP.
      - **Unmanaged** — The policy server is not an MPE device and therefore cannot be actively managed by the CMP. This selection is useful when an MPE device is routing traffic to a non Tekelec policy server.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The profile appears in the list of policy servers.

You have defined the policy server profile.

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

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

Configuring or Modifying a Policy Server Profile

To configure or modify a policy server profile:

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

   The Policy Server Administration page opens in the work area.

   The page contains the following tabs:

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

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

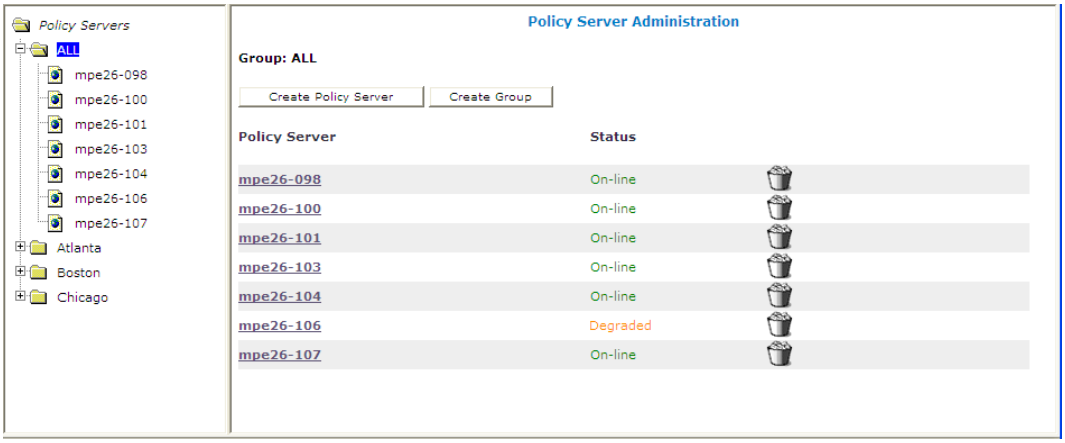
Deleting a Policy Server Profile

Deleting an MPE device profile from the ALL group also deletes it from any associated group.

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 the **Delete** icon 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; the System tab opens. Click **Delete**.

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

The policy server profile is deleted.

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. On the Policy Server Administration page, select the **Policy Server** tab.
   The current configuration options are displayed.
4. Click **Modify** and define options as necessary.
   Table 3: Policy Server Protocol Configuration Options defines available options. (The options you see may vary depending on the mode in which your system is configured.)
5. When you finish, click **Save** (or **Cancel** to discard your changes).

Table 3: Policy Server Protocol Configuration Options

Attribute	Description
Associations	

Attribute	Description
Applications	The application profiles associated with this MPE device. To modify this list, click **Manage**. For more information on application profiles, see *Managing Application Profiles*.
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*.
Configuration	
Subscriber Indexing	Select the appropriate index(es) in the SPR: **Index by Username** (account ID), **Index by NAI** (network access ID), **Index by E.164 (MSISDN)** (E.164 phone number), **Index by IMSI** (IMSI number), or **Index by IP Address**. **Note:** The indexing parameters to use depend on how Sh is used. If you are unsure which indexing method(s) to configure, contact Tekelec Support.
Time of Day Triggering	Select **Enable** or **Disable** (the 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 *Managing Policy Time Periods*.
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 Savings Changes	If selected, the MPE device observes Daylight Savings Time for the configured Billing Time Zone.
Default Local Time Mode	Select the time used within a user's session from the pulldown menu: **System Local Time** to use the local time of the MPE device (the 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, all subscribers' full monthly quota is granted for the billing cycle following a quota reset. If enabled, all subscribers'

	monthly quota is prorated for the billing cycle following a quota reset, based on the value of the **Billing Date Effective** field in the subscriber's profile. This is a global setting affecting all subscribers. (If the field value is null, usage will not be prorated.)
Billing Date Effective Name	Enter the name of the custom field in subscriber profiles to use for the SPR variable **NewBillingDateEffective**. The default is null. This is a global setting affecting all subscribers. To specify a local time in the SPR, the field must be in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*; to specify a time zone (UTC offset), the field must be in the format *yyyy-mm-dd*T*hh*:*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 will combine the updates (PURs), resulting from a single user request into a single PUR update to the SPR. The PUR will contain both the quota usage and state updates for the user. This reduces the number of transactions between the MPE and SPR.
Cache Quota Usage	If enabled, the MPE device caches the quota usage objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.
Cache Entity State	If enabled, the MPE device caches the entity state objects locally for as long as the user session exists. If disabled, objects are cached for a default of 60 seconds.
Subscribe Quota Usage	Subscribe to receive notifications from the SPR for any changes to the quota.
Subscribe Entity State	Subscribe to receive notifications from the SPR for any changes to the entity state.
RADIUS-S	

RADIUS Shared Secret	Authenticates RADIUS messages received from external gateways (that is, PDSN or HA). This field must be configured with a value or the RADIUS-S protocol will not work. Also, each gateway must be configured to use this value when sending messages to the MPE device, or the messages received from that gateway will be dropped.
Untiered Plan Name	When the MPE device is set to RADIUS-S mode, this attribute indicates that a matching plan name does not participate in any tiered service plan. On a successful lookup for a given subscriber, the plan name returned by LDAP is compared to the Untiered Plan Name configured for the MPE device via the Policy Server tab. If they match, no default QoS values are sent to the gateway for the subscriber. If the Untiered Plan Name is null, this only matches if the subscriber has an entry in LDAP with no value for the associated attribute. The default value is null.
Default Downstream Profile Default Upstream Profile	Define the upstream and downstream bandwidth parameters that are used when establishing a default traffic profile using RADIUS-S. You can override these parameters by configuring policy rules that apply different profiles. If a default profile is not configured, and the policy rules do not set the bandwidth parameters, a default traffic profile is sent to the Gateway to disable policing.
Index by Username	Select if the RADIUS database is indexed by subscriber account ID.
Index by NAI	Select if the RADIUS database is indexed by subscriber network address ID.
Index by Calling Station ID	Select if the RADIUS database is indexed by subscriber calling station ID.
Index by IP Address	Select if the RADIUS database is indexed by subscriber IP address.
Diameter	
Diameter Realm	The domain of responsibility (for example, `galactel.com`) for the MPE device.
Diameter Identity	The fully qualified domain name (FQDN) of the MPE device (for example, `mpe3.galactel.com`).
Default Resource Id	The bearer used if a GGSN does not send any bearer information in a Credit-Control Request (CCR). Enter an alphanumeric string of up to 100 characters. The default is no resource ID (that is, no bearer).
Correlate PCEF sessions	If selected, the primary PCEF Gx session will share information with all secondary sessions that share an IP address within the same IP-CAN session. Up to 10 different Gx sessions can be correlated to one subscriber. By default, PCEF sessions are not correlated, and do not share information.
Validate user	If enabled, sessions for unknown users are rejected.

Diameter PCEF Default Profile	Select the default traffic profile from the list that will be applied during PCEF session establishment using the Gx or Ty protocols, or if no other SCE traffic profile is applied as a result of a policy being triggered.
Diameter AF Default Profiles	
	Define the bandwidth parameters that are used when a request from an Application Function (AF) does not contain sufficient information for the MPE device to derive QoS parameters. These profiles are defined per media type: **Default**, **Audio**, **Video**, **Data**, **Application**, **Control**, **Text**, **Message**, and **Other**. (The **Default** profile is used when a profile for a media type is not defined.) To specify values, create Diameter profiles in the general profile configuration.
Default Charging Servers	
Primary Online Server	FQDN of the primary online charging server (used, for example, for prepaid accounts).
Primary Offline Server	FQDN of the primary offline charging server (used, for example, for billed accounts).
Secondary Online Server	FQDN of the secondary (backup) online charging server.
Secondary Offline Server	FQDN of the secondary (backup) offline charging server.

SMPP Configuration	
SMPP Enabled	Select to enable Short Message Peer to Peer (SMPP) messaging to subscribers. To send an SMS message to a subscriber, an MSISDN must be present in the subscriber's profile. Messages can be up to 254 characters long.
(Primary) SMSC Host	Enter the FQDN or IP address of the primary Short Messaging Service Center store-and-forward server, which accepts SMS messages from the relay server.
SMSC Port	Enter the port number on which the primary Short Messaging Service Center store-and-forward server is listening for SMS messages. The default port is 2775.
ESME System ID	Enter the system ID of the primary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source. **Note:** This value must be configured on the primary SMPP server.
ESME Password	Enter the password of the primary External Short Messaging Entity. Sending the ID and password values authenticates the relay server as a trusted source. **Note:** This value must be configured on the SMPP server.

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

SMTP Configuration	
SMTP Enabled	Select to enable Simple Mail Transport Protocol (SMTP) messaging (email) to subscribers. SMTP notifications are triggered from policy action and sent through an SMS Relay (SMSR) function to an external mail transfer agent (MTA). **Note:** There is no delivery receipt for the SMTP messages sent from the SMSR, only confirmation that it reached the configured MTA.
MTA Host	Enter the FQDN or IP address of the Mail Transfer Agent server, which accepts SMTP messages from the SMSR function.
MTA Port	Enter the port number on which the MTA server is listening for SMTP messages. The default port is 25.
MTA Username	Enter the system ID of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. **Note:** This value must be configured on the MTA.
MTA Password	Enter the password of the SMSR function. Sending the ID and password values authenticates the SMSR function as a trusted source. **Note:** This value must be configured on the MTA.
Confirm MTA Password	Re-enter the password for verification. **Note:** This is a new configuration setting for the SMTP connection.
Default From Address(es)	Enter the source address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none. **Note:** The total number of To, CC, and BCC addresses is limited to five.
SMTP Connections	The number of SMTP connections. They range from 1-10. **Note:** SMTP connections can be increased to support a higher throughput.
Default Reply-To Address(es)	Enter the email address automatically inserted into the To field when a user replies to an email message. For most email messages, the From and Reply-To fields are the same, but this is not necessarily so. If no Default Reply-To is specified here, the From

	address is used. Optionally enter a static email address to use for Reply-To. The default is none.
Default CC Address(es)	Enter the copy address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none. **Note:** The total number of To, CC, and BCC addresses is limited to five.
Default BCC Address(es)	Enter the blind copy recipient address for an SMTP message. Enter up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile. The default is none. **Note:** The total number of To, CC, and BCC addresses is limited to five.
Default Signature	Enter the text that appears as a signature in an SMTP message. The default is none.

RADIUS Configuration	
Default Passphrase	If the source IP address of a received RADIUS message does not match any of the IP addresses configured for a NAS device, and no passphrase is defined for the NAS device, then the MPE device will attempt to decode the message using this default passphrase. Enter the passphrase to use. The default is **radius**.
Load Shedding Configuration	
Enabled	Select to enable load shedding on the Diameter interface, or the RADIUS accounting interface between a NAS or RADIUS Proxy, and the MPE device. The default is enabled.

Configuring MPE Advanced Settings

The Advanced configuration page provides access to attributes that are not normally configured, including session cleanup and configuration key settings. To configure an advanced setting 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. On the **Policy Server Administration** page, select the **Policy Server** tab.
   The Policy Server configuration settings are displayed.
4. Click **Advanced**.

Advanced configuration settings are displayed and can be edited.

- **Session Clean Up Settings**

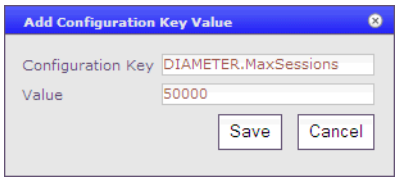
Table 4: Session Clean Up Options

Attribute	Description
Enable Session Clean Up	Select to turn on session clean up. Default value is selected (check marked).
Max Session Cleanup Rate (sessions/sec)	Define the rate (in sessions/sec) at which the cleanup task attempts to clean stale sessions. Default value is 50 sessions/sec. Valid range is 1-50 sessions/sec. This setting should not be modified without consulting Tekelec Customer Service.
Max Session Iteration Rate (sessions/sec)	Define the maximum rate (in sessions/sec) at which the cleanup task iterates through the sessions database. Default value is 1000. Valid range is 1-1000. This setting should not be modified without consulting Tekelec Customer Service.
Max Duration For Session Iteration (hours)	Define the maximum duration, in hours, to iterate through the sessions. Default value is 2 hours. Valid range is 1-2 hours. This setting should not be modified without consulting Tekelec Customer Service.
Session Cleanup Start Time	Define the time of day when the cleanup task occurs. Specify either Start Time or Interval for defining when session cleanup occurs by clicking the associated radio button and entering/selecting a value. Time can be specified in 24-hour format from the pulldown menu. No default value is defined.
Session Cleanup Interval (hours)	Define the interval, in hours, at which the cleanup task occurs. Specify either Start Time or Interval for defining when session cleanup occurs by clicking the associated radio button and entering/selecting a value. Default value is 6 hours. Valid range is 0-6 hours. Note that a value of 0 disables cleanup. This setting should not be modified without consulting Tekelec Customer Service.
Session Validity Time (hours)	The amount of time in seconds after which all sessions except Rx sessions are declared as stale. Default CMP value is 24 hours.
Max Session Validity Time (hours)	Define the maximum amount of time, in hours, after which the session is cleaned up after an error. Default value is 48 hours. Valid range is 1-48.
Override Cleanup Audit	Select to turn override clean up audit on. When selected, the cleanup task bypasses the audit process and deletes all sessions that are stale for the session validity time. Default value is deselected (not check marked).
Cleanup Stale RX Sessions	This flag determines whether the DiameterSessionCleanUp task should clean up Rx sessions. Default value is true.

Audit RX Sessions	This flag determines whether the DiameterSessionCleanUp task should audit Rx sessions before purging them from the database. Default value is false.
RX Session Validity Time (hours)	The amount of time in seconds after which an Rx session is declared as stale. Default CMP value is 24 hours.

- **Other Advanced Configuration Settings**— Configuration Key changes are made using this table.
  - **To add a key to the table** — Click **Add**; the Add Configuration Key Value window opens. Enter the following values:
    - **Configuration Key** — The attribute to set
    - **Value** — The attribute value

    For example:

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

    CAUTION

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

  - **To clone a key in the table** — Select an existing key in the table and click **Clone**; the Clone Configuration Key Value window opens with that key's information filled in. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
  - **To edit a key in the table** — Select an existing key in the table and click **Edit**; the Edit Configuration Key Value window opens with that key's information. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
  - **To delete a key from the table** — Select an existing key in the table and click **Delete**; you are prompted, "Are you sure you want to delete the selected Configuration Key Value(s)?" Click **Delete** to remove the key (or **Cancel** to cancel your request).

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

Configuring Data Source Interfaces

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

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

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

2. From the content tree, select the desired policy server.
   The Policy Server Administration page opens.
3. On the Policy Server Administration page, select the Data Sources tab.
   The current data sources are displayed, listing the administrative state, subscription state, type, primary address, and secondary address.
4. To modify the list of data sources, click **Modify**.

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

   - **To add a data source to the table** — Select the data source type from the Add pulldown list; the appropriate Add Data Source window opens. Configure values as appropriate.
   - **To clone a data source in the table** — Select an existing data source in the table and click **Clone**; the Clone Data Source window opens with that data source's information filled in. Make changes as required.
   - **To edit a data source in the table** — Select the data source in the table and click **Edit**; the Edit Data Source window opens, displaying the data source's information. Change the configuration values as required.
   - **To delete a data source from the table** — Select the data source in the table and click **Delete**; you are prompted, "Are you sure you want to delete the selected data source(s)?" Click **Delete** to remove the data source entry (or **Cancel** to cancel your request).
   - **To change the order of the list** — If you define multiple data sources, they are searched in the order displayed in this list. To change the order, select a data source and click the Up or Down arrows.

   When you finish, click **Save** (or **Cancel** to discard your changes).
5. The following general settings are available:

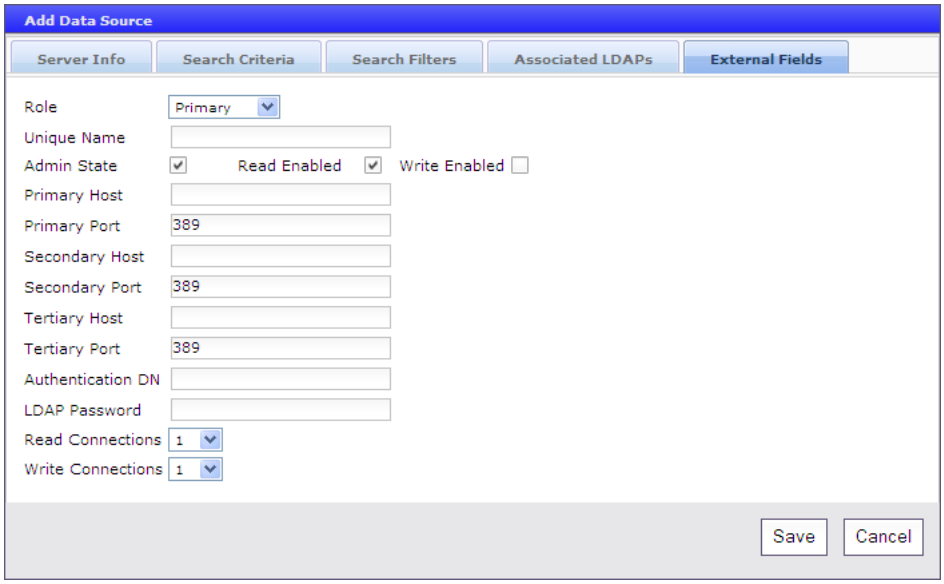
   - **Merge Search Results** — If you define multiple data sources and a search returns results from more than one source, the results are displayed in source order. To display one sorted list instead, select this option.
   - **Subscription Enabled Via Policy Only** — For detailed information, see the SPR documentation.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

Configuring an LDAP Data Source

For LDAP, you can configure connections to up to three servers. The Add Data Source window contains the following tabs: Server Info, Search Criteria, Search Filters, Associated LDAPs, and External Fields.

Server Info Tab

On the Server Info tab, enter the following:



- **Role**— Data source attribute with a value of either Primary or Secondary.
  - **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, in order to be used in a subscriber lookup.
- **Unique Name** — Name given to the 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. A typical port number is 389. 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:

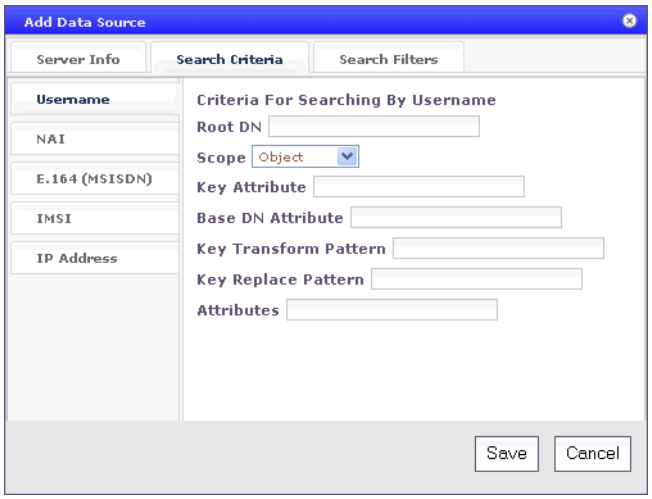
  `cn=PolicyServer,ou=galactel,o=galactel.com`
- **LDAP Password** — Provides read-only access to the LDAP directory. The MPE device must bind to the LDAP server with the DN and password to access the database. Example: `tekelec`.
- **Read Connections** — Enabled for data sources set in the Secondary role.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

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 a LDAP data source role of *primary*.

     Note: The field is blank.

   - **Username** — The database is indexed by user name (account ID).
   - **NAI** — The database is indexed by NAI (network access ID).
   - **E164 (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** (default) — restrict the scope of the LDAP search to the specified object.
   - **One-Level** — 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:

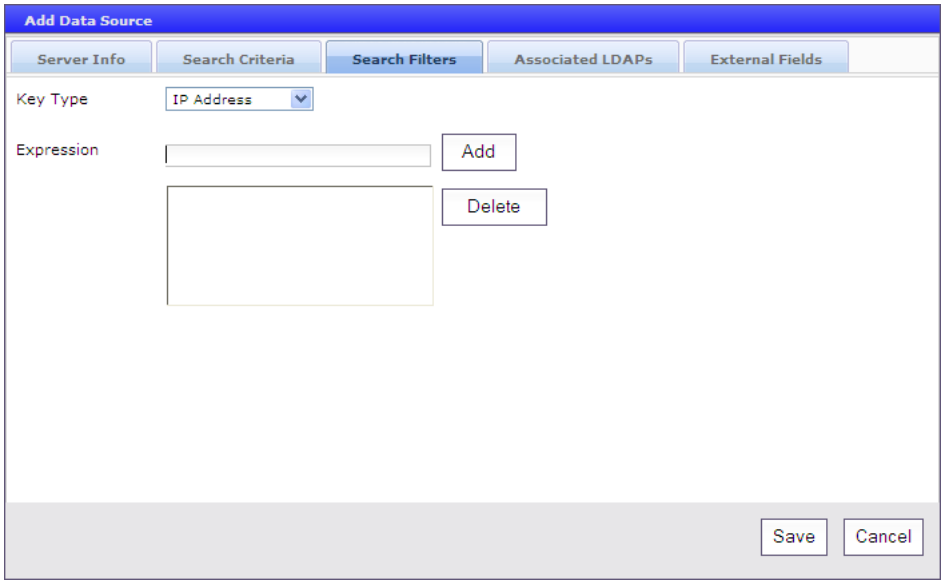
   - *attr* — a field is saved with the same name and value as the specified attribute
   - *field=attr* — a field with the specified name is saved with the value of the specified attribute
   - *field=attr*[*from*:*to*] —a field with the specified name is saved with a substring of the value of the specified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

   The substring is determined by the *from* and *to* values. A value of 0 in *from* indicates the beginnning 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. Tekelec recommends ordering 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:

   - **Username** — User name (account ID)
   - **NAI** — Network address ID
   - **E164 (MSISDN)**— E.164 phone number
   - **IMSI** — International Mobile Subscriber Identity
   - **IP Address** (default) — IP address

2. **Expression** — Enter a regular expression.

   For example:

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

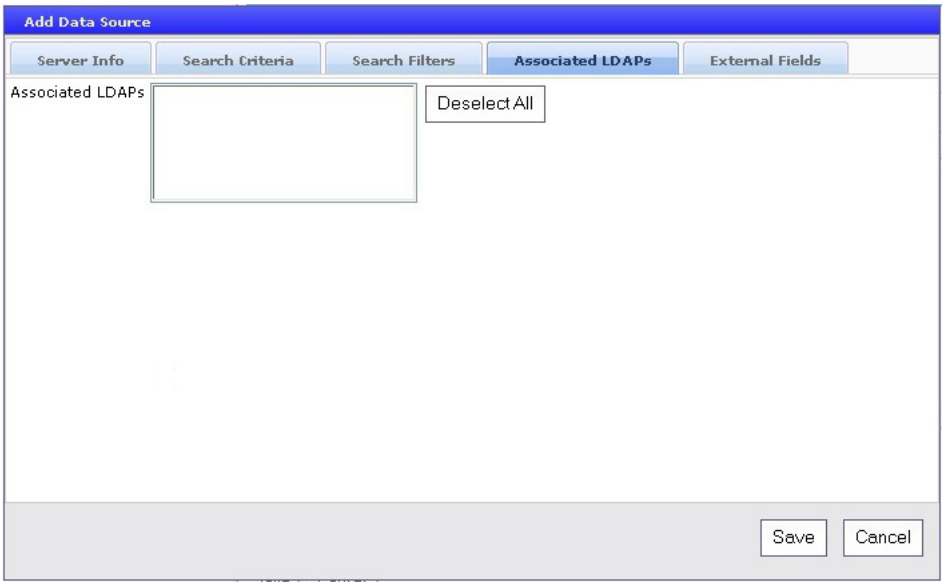
   To add the expression to the list, click **Add**. To remove an expression from the list, select it in the list and click **Delete**.

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

The LDAP data source filters are defined.

Associated LDAPs Tab

On the Associated LDAPs tab, enter the following:



- **Associated LDAPs** — A list of associated secondary LDAP data sources. The list is displayed on the Priority order of the secondary data sources. For example:

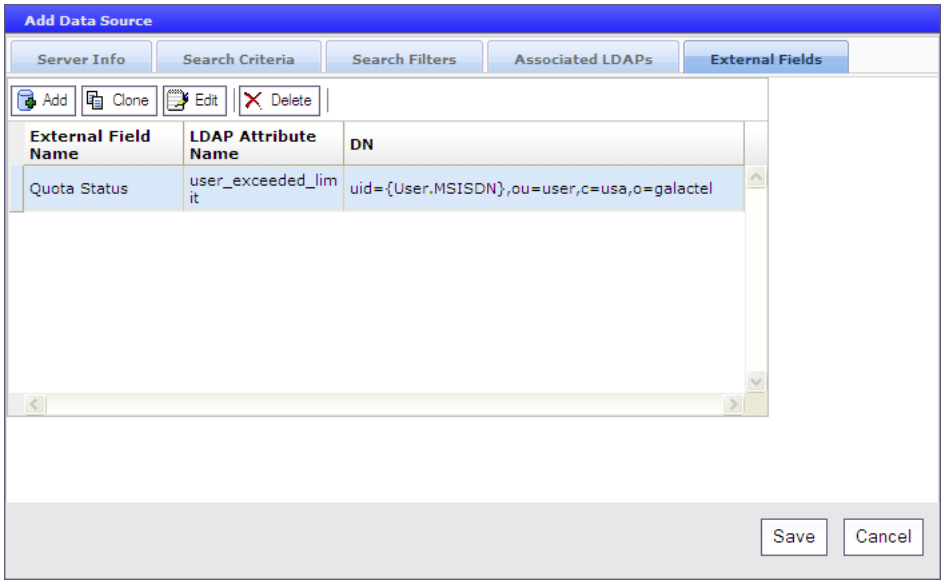
  ```
  LDAP1.AssociatedLDAPs=1234567890111111, 123456789022222
  ```

Note: Select **Deselect All** if you want to deselect your Associated LDAP 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 atributes per data source.

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



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

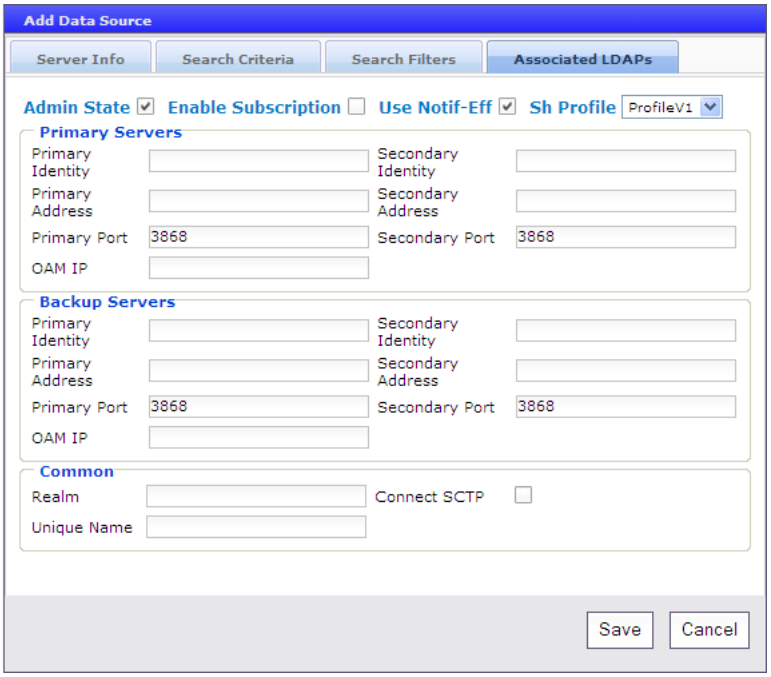
Configuring an Sh Data Source

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

You can receive subscription notifications as changes are implemented to the Quota and Entity state, when adding a configured data source and selecting **Enable Subscription**.

Server Info Tab

On the Server Info tab, enter the following:



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

   Selected by default.

2. **Enable Subscription** — Enable the Sh subscribe/notify function to manage dynamic profile changes. The data is returned in one XML response. If disabled, separate lookups are used.
3. **Use Notif-Eff** — Enable reads of multiple user data blocks (subscriber, quota, and entity state).
4. **Sh Profile** — Select **ProfileV1** (the default) for using third-party HSS, **ProfileV2** for an HSS/Sh (7.5 or earlier version), or **Profile V3** for using SPR (8.0 or later version).

   Note: ProfileV2 supports reading and writing quota and entity state data. **Profile V3** supports retrieving pool information for a subscriber and pool quota usage/pool state from the SPR.

5. **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.

6. **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.

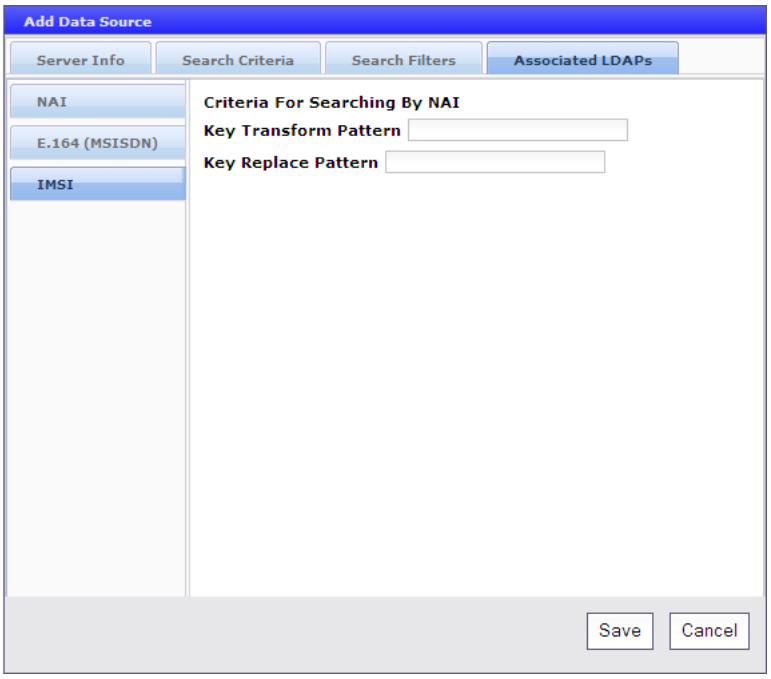
d) **Secondary Identity** — Secondary backup servername.
e) **Secondary Address** — IP address, in IPv4 or IPv6 format, of the secondary backup server.
f) **Secondary Port** — Secondary backup server port number.
The default is 3868.
g) **OAM IP** — The SPR feature queries and edits data from the Sh data source via RESTful API.

Note: An OAM IP is needed for CMP to access the SDM server. CMP is unable to access the SDM server diameter Sh service address due to being in different networks.

7. **Common** :
   a) **Realm**— Server realm; for example, `galactel.com`.
   b) **Unique Name**— The unique name assigned to the server.
   c) **Connect SCTP**— Indicates whether the Sh data source can support SCTP protocol. If checked, MPE can communicate with the Sh data source in SCTP.
8. When you finish, click **Save** (or **Cancel** to abandon your changes).

Search Criteria Tab

On the Search Criteria tab, enter the following:



1. Select how the database is indexed:
   - **NAI** — The database is indexed by NAI (network access ID).
   - **E164 (MSISDN)** — The database is indexed by E.164 (E.164 phone number).
   - **IMSI** —The database is indexed by International Mobile Subscriber Identity.
2. **Key Transform Pattern** — Regular expression (regex) pattern to use to transform a key.

3. **Key Replace Pattern** — Replacement string to use to transform the key.

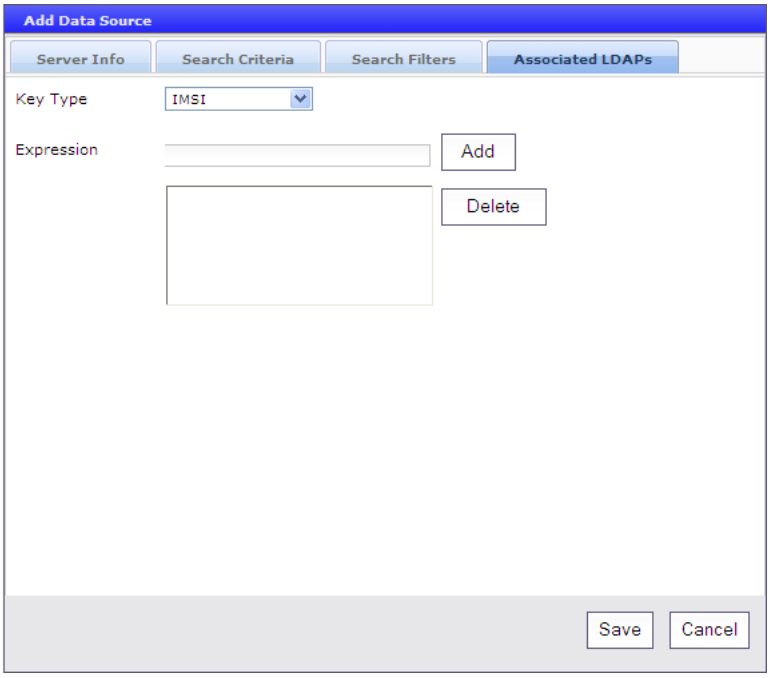
   For example, `17$2` means the new string starts with "17" and is followed by the group 2 ($2) pattern.

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

Search Filters Tab

You can configure any number of filters per search type per data source. For example, if a data source supports searching by MSISDN and IMSI, you can define multiple MSISDN and IMSI filters. Tekelec recommends ordering 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
   - **E164 (MSISDN)** — E.164 phone number
   - **IMSI** (the default) — International Mobile Subscriber Identity

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

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

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

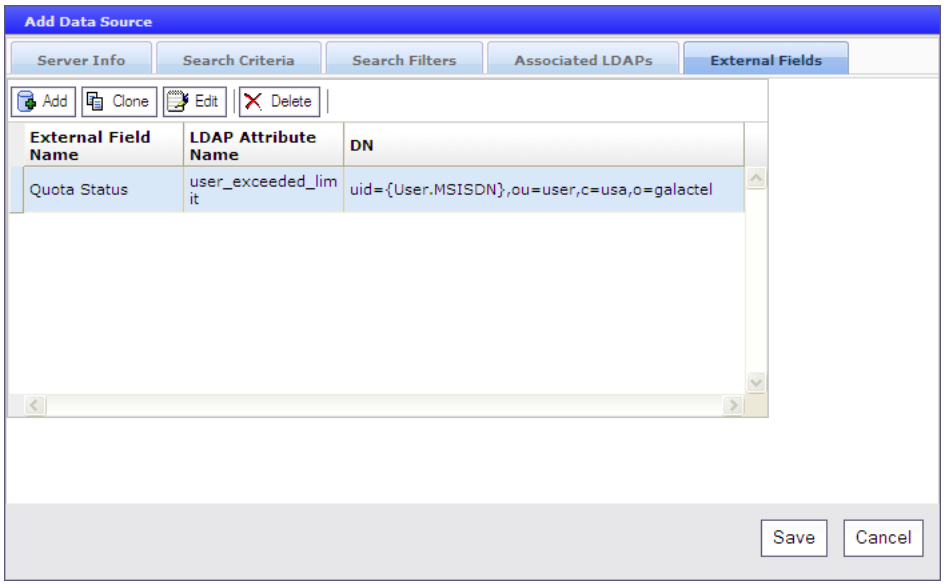
3. When you finish, click **Save** (or **Cancel** to discard your changes).

The Sh data source filters are defined.

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 atributes per data source.

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



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

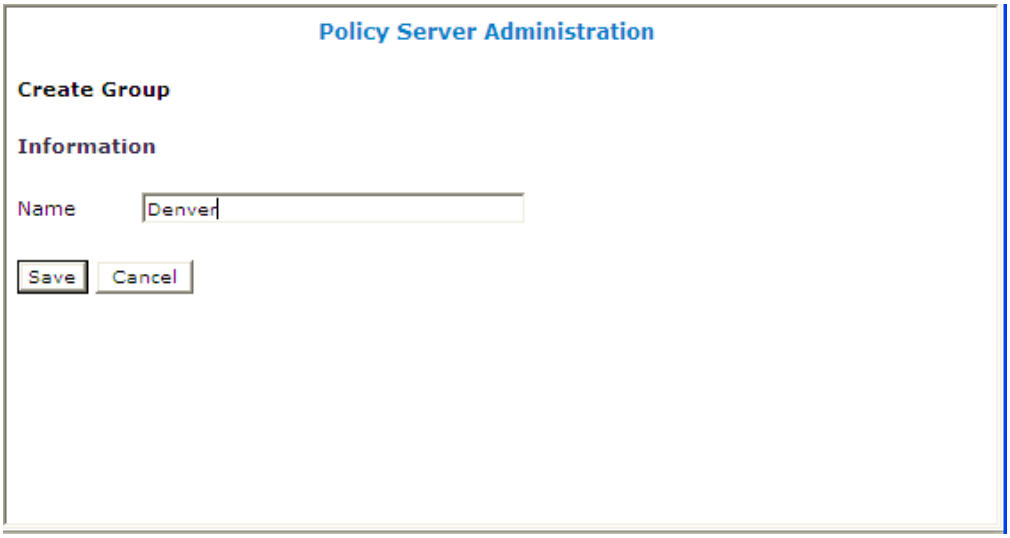
Policy Server Groups

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 groups.

Creating a Policy Server Group

To create a policy server group:

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



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

You have created a policy server group.

Adding a Policy Server to a Policy Server Group

To add a policy server to a policy server group:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the desired policy server group.
   The Policy Server Administration page opens in the work area, displaying the contents of the selected policy server group.
3. On the Policy Server Administration page, click **Add Policy Server**.
   The Add Policy Server page opens, displaying the policy servers not already part of the group.
4. Click on the policy server you want to add; use Ctrl or Shift-Ctrl to select multiple policy servers.
5. When you finish, click **Save** (or **Cancel** to cancel the request).

The policy server is added to the selected group.

Creating a Policy Server Sub-group

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

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

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

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

   The Policy Server Administration page opens in the work area, displaying the contents of the selected policy server group.

3. On the Policy Server Administration page, click **Create Sub-Group**.

   The Create Group page opens.

4. Enter the name of the new sub-group.

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

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

   The sub-group is added to the selected group.

Renaming a Policy Server Group

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

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

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

5. When you finish, click **Save** (or **Cancel** to cancel the request).
   The group is renamed.

Removing a Policy Server Profile from a Policy Server Group

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

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

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the desired 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 desired 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; the System tab opens. 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 desired policy server group or sub-group.
   The Policy Server Administration page opens in the work area, displaying the contents of the selected policy server group or sub-group.
3. On the Policy Server Administration page, click **Delete**.
   You are prompted, "Are you sure you want to delete this Group?"
4. Click **OK** to delete the group (or **Cancel** to cancel the request).

The policy group is deleted.

Reapplying the Configuration to a Policy Server

The CMP lets you reapply the configuration to each MPE device. When you reapply the configuration, the CMP reconfigures the corresponding MPE device completely with topology information (such as network elements and links), ensuring that the MPE device configuration matches that within the CMP. This action is not needed during normal operation but is useful in the following situations:

- When both servers of a cluster are replaced, the new servers come up initially with default values. (The *Policy Management Platform Configuration User's Guide* describes how to restore both single-server and clustered configurations.) Reapplying the configuration lets you redeploy the entire configuration rather than reconfiguring the MPE device field by field. You should also apply the Rediscover Cluster operation to the CMP to re-initialize the Cluster Information Report for the device, thereby clearing out the failed servers' status.
- After upgrading the software on an MPE device, Tekelec recommends that you reapply the configuration from the CMP to ensure that the upgraded MPE device and the CMP are synchronized.
- There are situations in which it is possible for an MPE device configuration to go out of synchronization with the CMP; for example, when a break in the network causes communication to fail between the CMP and the MPE device. If such a condition occurs, the CMP displays the MPE device status as "Configuration Mismatch." In this case, reapplying the configuration brings the MPE device back into synchronization with the CMP.

To reapply the configuration associated 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 **ALL** group.
   The Policy Server Administration page opens in the work area.
3. From the group **ALL**, select the desired MPE device.
   The Policy Server Administration page displays information for that device.
4. On the Policy Server Administration page, select the System tab and click **Reapply Configuration**.
   The profile information is saved to the MPE device.

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

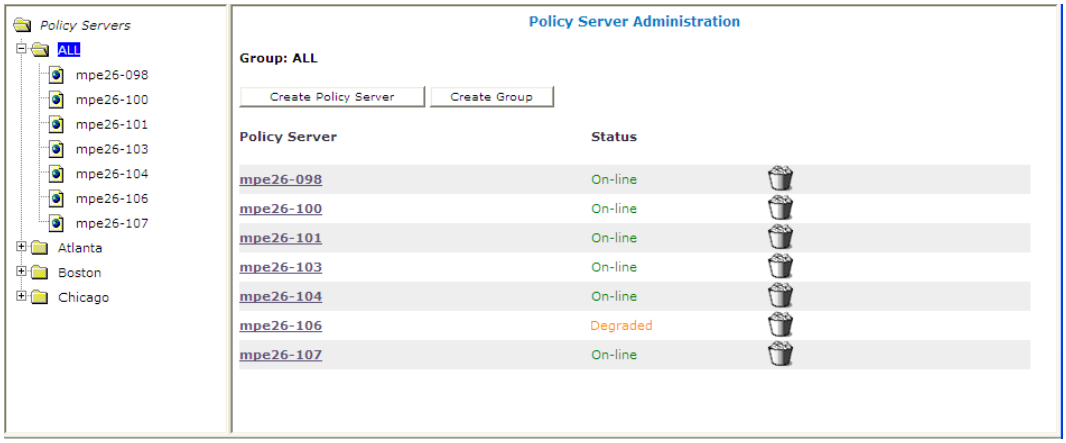


Figure 9: Group View

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

Policy Server Reports

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

Each report page provides 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 All Counters** — Resets all counters under Policy Statistics and Protocol Statistics back to initial values except for "Session count" and "Downstream Bandwidth" under Network Elements.
  - **Rediscover Cluster** — Rediscovers the cluster, deleting any failed servers that have been removed from service.
  - **Pause/Resume** — Stops or restarts automatic refreshing of displayed information. The refresh period is 10 seconds.
  - **Cancel** — Returns to previous page.

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

- **Cluster Information** — 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.
- **Profile Statistics** — Information about quota profiles and traffic profiles.
- **Session Cleanup Statistics** — Information about removal of stranded subscriber sessions.

- **Policy Statistics** — Information about the execution of policy rules.
- **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, and SPR activity.
- **KPI Interval Statistics** — Information about the configured reporting interval for key performance indicator (KPI) statistics.

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.
- **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), CPU, and memory.

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

Time Period

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

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

Policy Statistics

The Policy Statistics section summarizes policy rule activity within the MPE device. This is presented as a table of statistics for each policy rule that is configured for the MPE device.

The following statistics are included:

- **Name** — Name of the policy being polled.
- **Evaluated** — Number of times the conditions in the policy were evaluated.
- **Executed** — Number of times policy actions were executed. This implies that the conditions in the policy evaluated to be true.
- **Ignored** — Number of times the policy was ignored. This can happen because the policy conditions refer to data which was not applicable given the context in which it was evaluated.

To see statistics per policy, click the (details...) hyperlink. 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 on the Policy Name. In addition to Evaluated, Executed, and Ignored, the following details are displayed:

- **Total Execution Time (ms)** — The summary of all execution durations, where execution duration is measured starting at the beginning of the policy conditions evaluation until the execution finishing.
- **Maximum Execution time (ms)** — The longest execution duration of the policy.
- **Average Execution time (ms)** — The average of all execution durations of the policy.
- **Processing Time Statistics** - number of policies processed per time range, in ms. Ranges include 0-20, 20-40, 40-60, 60-80, 80-100, 100-150, 150-200, 200-250, and >250.

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.

Figure 10: Sample Protocol Statistics shows a sample.

Protocol Statistics

Name	Connections	Total client messages in / out	Total messages timeout
Diameter			
Diameter AF Statistics	1	0 / 0	0
Diameter PCEF Statistics	1	7090 / 7090	0
Diameter CTF Statistics	1	0 / 0	N/A
Diameter BBERF Statistics	1	0 / 0	0
Diameter TDF Statistics	1	0 / 0	0
Diameter Sh Statistics	1	0 / 0	0
Diameter DRMA Statistics	1	4 / 4	0

Figure 10: 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 *Related Publications*).

Note: 1. Statistical information is returned from the MPE device as a series of running "peg counts." To arrive at interval rate information, such as session success and failure counts, two intervals are needed to perform the difference calculation. Also, statistical information, such as session activation counts, is kept in memory and is therefore not persisted across the cluster. After a failover, non-persistent metrics must be repopulated based on resampling from the newly active primary server. Therefore, when an MPE device is brought on line, or after a failover, one or more sample periods will display no statistical information.

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

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.

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 11: 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 11: 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.

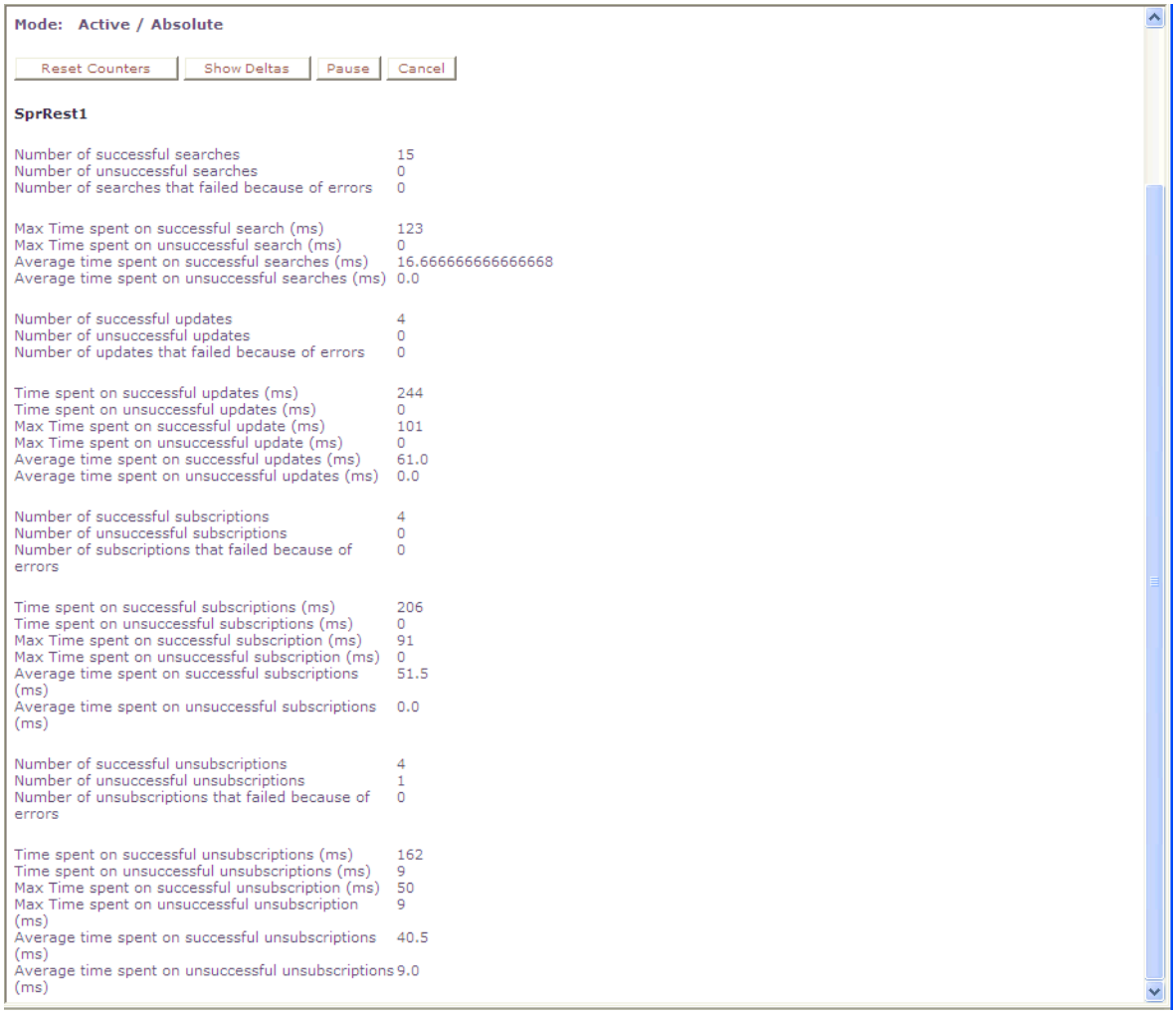
Sh Statistics

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**
- **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, *Figure 12: SPR Data Source Statistics* shows an example of the statistics collected.



Mode: Active / Absolute

Reset Counters | Show Deltas | Pause | Cancel

SprRest1

Number of successful searches	15
Number of unsuccessful searches	0
Number of searches that failed because of errors	0
Max Time spent on successful search (ms)	123
Max Time spent on unsuccessful search (ms)	0
Average time spent on successful searches (ms)	16.666666666666668
Average time spent on unsuccessful searches (ms)	0.0
Number of successful updates	4
Number of unsuccessful updates	0
Number of updates that failed because of errors	0
Time spent on successful updates (ms)	244
Time spent on unsuccessful updates (ms)	0
Max Time spent on successful update (ms)	101
Max Time spent on unsuccessful update (ms)	0
Average time spent on successful updates (ms)	61.0
Average time spent on unsuccessful updates (ms)	0.0
Number of successful subscriptions	4
Number of unsuccessful subscriptions	0
Number of subscriptions that failed because of errors	0
Time spent on successful subscriptions (ms)	206
Time spent on unsuccessful subscriptions (ms)	0
Max Time spent on successful subscription (ms)	91
Max Time spent on unsuccessful subscription (ms)	0
Average time spent on successful subscriptions (ms)	51.5
Average time spent on unsuccessful subscriptions (ms)	0.0
Number of successful unsubscriptions	4
Number of unsuccessful unsubscriptions	1
Number of unsubscriptions that failed because of errors	0
Time spent on successful unsubscriptions (ms)	162
Time spent on unsuccessful unsubscriptions (ms)	9
Max Time spent on successful unsubscription (ms)	50
Max Time spent on unsuccessful unsubscription (ms)	9
Average time spent on successful unsubscriptions (ms)	40.5
Average time spent on unsuccessful unsubscriptions (ms)	9.0

Figure 12: SPR Data Source Statistics

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.

Interval Statistics

The 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.

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 desired Policy Management device.
   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, select the **Logs** tab.

   Log information, including the log levels, is displayed. *Figure 13: Policy Server Logs Tab* shows an example. You can configure the following logs:

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

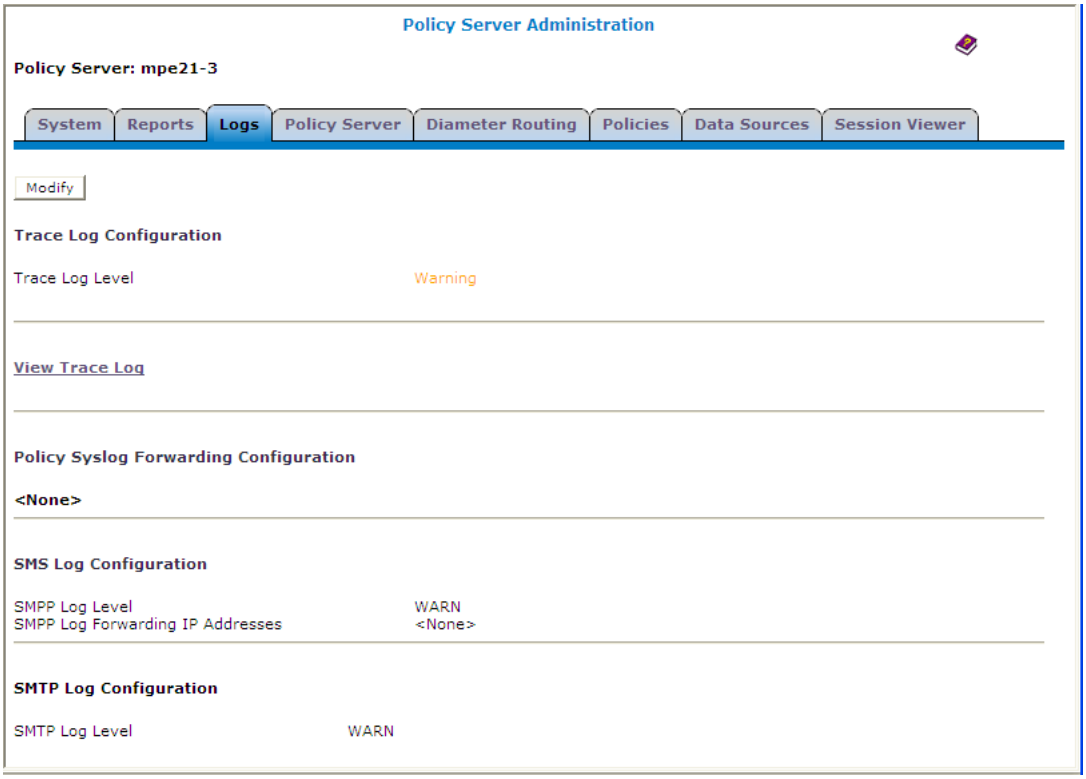


Figure 13: Policy Server Logs Tab

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. For more information, see *Configuring Log Settings*.

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 *Policy Management Troubleshooting Guide*.
   - **Severity** — Severity level of the event. Application-level trace log entries are not logged at a higher level than Error.
   - **Message** — The message associated with the event. If additional information is available, the event entry shows as a link. Click on the link to see additional detail in the frame below.

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

   - **Trace Log Viewer for Server** — Select the active, standby, or spare server
   - **Start Date/Time** — Click the calendar icon, select the desired starting date and time, then click **Enter**.
   - **End Date/Time** — Click the calendar icon, select the desired ending date and time, then click **Enter**.
   - **Trace 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 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.

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

Syslog Support

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

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, `/var/Camiant/log/SMPP.log`, 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. SMPP info appears on the MPE Logs tab of the MPE Configuration page, under the SMS Log Configuration heading. You can configure the severity of messages that are written to the SMPP log as well as set a forwarding address. For more information, see *Configuring Log Settings*.

The SMTP Log

The SMTP log, `/var/Camiant/log/SMTP.log`, contains all Simple Mail Transfer Protocol messages sent by the MPE device, as well as any ACK messages received from a mail transfer agent (MTA). SMTP Log info appears on the MPE Logs tab of the MPE Configuration page. You can configure the severity of messages that are written to the SMTP log. For more information, see *Configuring Log Settings*.

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 Modify Settings fields open in the work area.
2. In the **Modify Trace Log Settings** section of the page, configure the Trace Log Level.

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

   - **Emergency** — Provides the least amount of logging, recording only notification of events causing the system to be unusable.
   - **Alert** — Action must be taken immediately in order to prevent an unusable system.
   - **Critical** — Events causing service impact to operations.
   - **Error** — Designates error events which may or may not be fatal to the application.
   - **Warning** (the default) — Designates potentially harmful situations.

- **Notice** — Provides messages that may be of significant interest that occur during normal operation.
- **Info** — Designates informational messages highlighting overall progress of the application.
- **Debug** — Designates information events of lower importance.
- **All** — Used to turn on all logging.
- **Off** — Used to turn off logging.

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. On the other hand, 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 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 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** (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.
- **All** — Used to turn on all logging.
- **Off** — Used to turn off logging.

4. In the **Modify SMS Log Settings** section of the page, configure the following:
   a) **SMPP Log Level** — Indicates the severity of messages that are written to the file SMPP.log.

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

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

   Valid levels are:

   - **OFF** — Turns off logging.
   - **ERROR** — Designates error events which may or may not be fatal.

- **WARN** (the default) — Designates potentially harmful situations.
- **INFO** — Designates informational messages highlighting overall progress.
- **DEBUG** — Designates information events of lower importance.
- **TRACE** — Designates informational events of very low importance.
- **ALL** — Records all logging levels.

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

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

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

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

6. When you finish, click **OK** (or **Cancel** to discard your changes).
   The log configurations are changed.

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

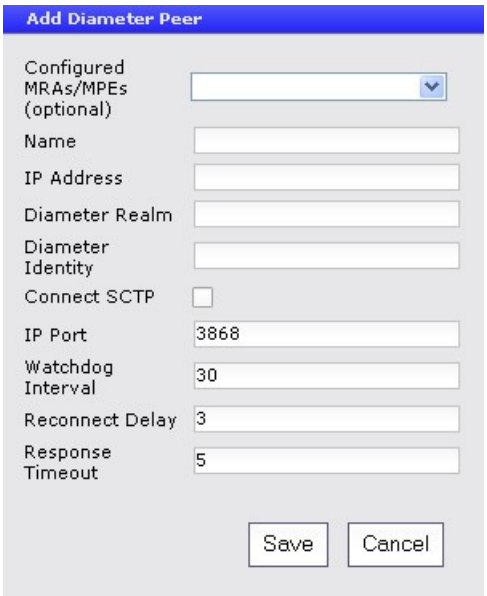
Configuring Diameter Peers

Policy Management devices support Diameter Rx, Gq, Ty, Gxx, Gx, and Gy 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 desired MPE device.
   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, select the **Diameter Routing** tab.
   The Diameter Routing configuration settings are displayed.
4. Click **Modify Peers**. The Modify the Diameter Peer Table page opens. The functions available from this table are as follows:

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



   Enter the following:

   - **Configured MRAs/MPEs (optional)** — If you are defining an existing Policy Management cluster as a Diameter peer, select it from this list; the other fields are populated.
   - **Name** — Name of the peer device (which must be unique within the CMP database).
   - **IP Address** — 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** — The peer's domain of responsibility (for example, `galactel.com`).

- **Diameter Identity** — Fully qualified domain name (FQDN) of the peer device (for example, `mpe33.galactel.com`).
- **Connect SCTP**— Connects the SCTP to the Diameter Peer. If selected, the field is set to *true*. If not selected, the field is set to *false*.
- **IP Port**— The port number of the primary server.
- **Watchdog Interval**— Used as a *keep alive* functionality. The default interval is 30 seconds.
- **Reconnect Delay**— Used as a delay between connection retries. The default interval is 3 seconds.
- **Response Timeout**— The maximum amount of time to wait for a response from the TDF before declaring that the message timed out.

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

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

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

You have defined a Diameter peer.

Configuring Diameter 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.

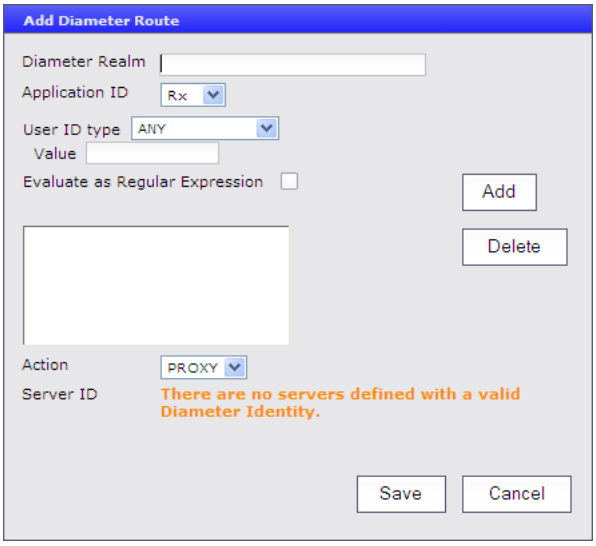
To configure the Diameter route table:

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

   The Modify the Diameter Route Table page opens.

   The functions available from this table are as follows:

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



The fields are as follows:

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

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

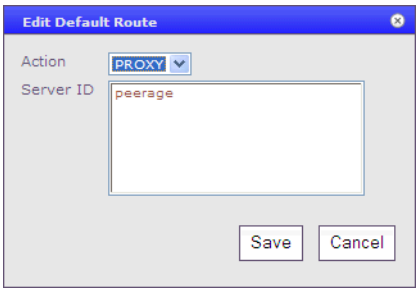
- **User ID type** — Select **ANY** (the default), **E.164(MSISDN)**, **IMSI**, **IP**, **NAI**, **PRIVATE**, **SIP_URI**, or **USERNAME**.
- **Value** — Enter the user ID to be routed (for example, an NAI or E.164 number). Separate user IDs using a comma (,); use an asterisk (*) as a wildcard character.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

  Note: If desired, you can define a server with a Diameter identity.

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

- **To change the order of a route in the table** — Select an existing route in the table and click **Up** or **Down**. The order of routes is changed.
- **To clone a route in the table** — Select an existing route in the table and click **Clone**; the Clone Diameter Route window opens with that route's information filled in. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To edit a route in the table** — Select an existing route in the table and click **Edit**; the Edit Diameter Route window opens with that route's information. Make changes as required. When you finish, click **Save** (or **Cancel** to discard your changes).
- **To delete a route from the table** — Select one or more existing routes and click **Delete**; you are prompted, "Are you sure you want to delete the selected Diameter Route(s)?" Click **Delete** (or **Cancel** to cancel your request). The route entry is removed.

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



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

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

The Diameter routes are configured.

Chapter 6

Managing Network Elements

Topics:

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

About Network Elements

A network element is a high-level device, server, or other entity within your network for which you would like to use an MPE device to manage Quality of Service (QoS). Examples include a packet-switched data network (PSDN), a gateway GPRS support node (GGSN), a router, a server, or a zone. Once you have defined a network element in the CMP, 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, configure its protocol options. The options available depend on the network element type.

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

Defining a Network Element

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

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

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

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

      Enter up to 255 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:

- **GGSN** — Gateway GPRS Support Node
- **HSGW** — HRPD Serving Gateway
- **PGW** — Packet Data Network Gateway
- **SGW** — Serving Gateway
- **DPI** — Deep Packet Inspection device

f) **Capability** — with the following options:

- **TDF-Solicit** — DPI accepts Sd session establishment requests from the MPE device.
- **Time-Tariff** — DPI supports Time-Tariff functionality.
- **Usage-Report** — DPI is compatible with usage_report event trigger value *26*.

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 moreMRA devices to associate with this network element.
7. To add a network element to a network element group, select the desired group (see *Adding a Network Element to a Network Element Group*).
8. When you finish, click **Save** (or **Cancel** to discard your changes).
   The network element is displayed in the Network Element Administration page.

You have created the definition for a network element.

Modifying a Network Element

To modify a network element:

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

The network element definition is modified.

Deleting Network Elements

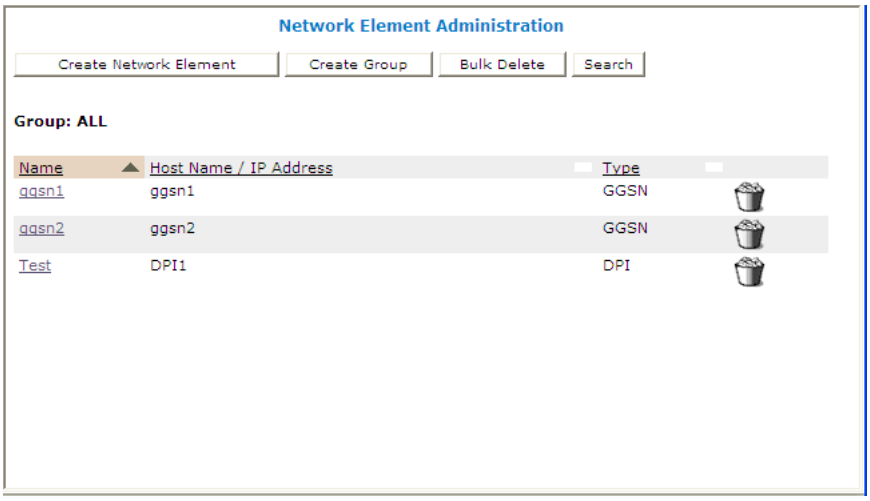
Deleting a network element definition removes it from the list of items that a Policy Management device can support. To delete a network element definition, delete it from the ALL group. Deleting a network element from the ALL group also deletes it from every group with which it is associated.

To delete a network element:

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

The Network Element Administration page opens in the work area, displaying all defined policy servers.

3. From the work area, click the **Delete** icon, located to the right of the network element you want to delete:



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

The network element is deleted.

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 `*-*`) and click **Filter**.
5. Click **Bulk Delete** (or **Cancel** to cancel the request).
   The selected network element(s) or group(s) are deleted from the CMP 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 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 desired search criteria:
   - **Name** — The name assigned to the network element.
   - **Host Name/IP Address** — The domain name or IP address in IPv4 or IPv6 format of the network element.
   - **Description** — The information pertaining to the network element that helps identify it within the network. Enter up to 250 characters.

     Note: Searches are not case sensitive. Criteria can be entered using the wildcard characters '*' and '?'.
5. After entering search criteria, click **Search** (or **Cancel** to cancel the request).

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

Configuring Options for Network Elements

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

Note: Configuration changes made in the CMP 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 rule time for the CMP. The discrepancy is resolved when the OSSI Distributor Task runs on the CMP. See *Managing Scheduled Tasks* for more information.

PDSN

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

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

- **Diameter Identity** — Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`). Click **Add** to add the identity to the list; select an identity from the list and click **Delete** to remove it.

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

The PDSN device is defined.

Home Agent

To configure options for a Home Agent network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the Home Agent tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the following:
   a) Diameter Features
   - **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   - **Diameter Identity** — Specifies the fully qualified domain name (FQDN) of the network element (for example, `ne.galactel.com`). Click **Add** to add the identity to the list; select an identity from the list and click **Delete** to remove it.

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

The Home Agent device is defined.

GGSN

To configure interface information for a GGSN network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the **GGSN** tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity** — Specifies the FQDN of the network element (for example, `ggsn1024.galactel.com`).
   Click **Add** to define multiple identities used by the network element. To delete one of the identities, select it from the list and click **Delete**.

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

The GGSN device is defined.

HSGW

To configure interface information for an HSGW network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the **HSGW** tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity** — Specifies the FQDN of the network element (for example, `hsgw1024.galactel.com`).

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

The HSGW device is defined.

PGW

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the **PGW** tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity** — Specifies the FQDN of the network element (for example, `pgw1024.galactel.com`).

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

The PGW device is defined.

SGW

To configure interface information for a signaling gateway (SGW) network element:

1. From the **Network** section of the navigation pane, select **Network Elements**.

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

2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the **SGW** tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity** — Specifies the FQDN of the network element (for example, `sgw1024.galactel.com`).

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

The SGW device is defined.

DPI

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, select the **DPI** tab and then click **Modify**.
   The Modify Network Element page opens.
4. Configure the following information:
   a) **Diameter Realm** — Specifies the network element's domain of responsibility (for example, `galactel.com`).
   b) **Diameter Identity** — Specifies the FQDN of this network element (for example, `dpi56.galactel.com`).

      Click **Add** to define multiple identities if used by this network element. To delete one of the identities, select it from the list and click **Delete**.
   c) **SCTP Enabled**— By selecting the check box, you can connect to the TDF using SCTP. TCP is the default connection.
   d) **Allow direct connection from MPE**— By selecting the check box, TDF connects directly to Sd with the PCRF (passing on MRA.)

      The following is shown only on debug mode if the option is checked:
   e) **TDF Port**— TDF listens for the Sd connection on this port.
   f) **Reconnect Delay**— Used as a delay between connection retries. The default interval is 3 seconds.
   g) **Watch Dog Interval**— Used as a *keep alive* functionality. The default interval is 30 seconds.
   h) **Response Timeout**— The maximum amount of time to wait for a response from the TDF before declaring that the message timed out.
   i) **Associated MRA Identity**— The MRA that the TDF is connected. Used by the PCRF to determine which MRA to send messages for the TDF.

j) **Backup TDF Identity**— The backup TDF associated with this TDF. If the primary TDF connection is down, the PCRF will send messages to the backup TDF.

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

The DPI device is defined.

NAS

To configure interface information for a NAS network element:

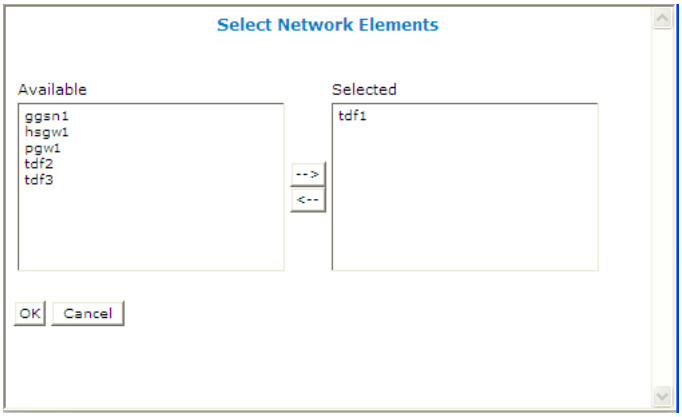
1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select a network element.
   The Network Element Administration page opens in the work area.
3. On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

The NAS device is defined.

Associating a Network Element with an MPE Device

To associate a network element with an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays a list of policy server groups; the initial group is **ALL**.
2. From the content tree, select the desired MPE device.
   The Policy Server Administration page opens in the work area.
3. On the Policy Server Administration page, select the **Policy Server** tab.
   In the Associations section of the page, the network elements associated with this MPE device are displayed.
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 desired network elements from the **Available** list and click **-->**.

   To disassociate a network element from the MPE device, select the network element from the **Selected** list and click **<--**. To select multiple entries, use the Ctrl and Shift keys.

7. When you finish, click **OK** (or **Cancel** to discard your changes).
   The selected network elements are added to the list of network elements managed by this MPE device.
8. To associate a network element group with the MPE device, select the group from the list of network element groups located under Associations.
9. When you finish, click **Save**, located at the bottom of the page (or **Cancel** to discard your changes).

The network element is associated with this MPE device.

Working with Network Element Groups

Creating a Network Element Group

Network element groups let you organize network elements.

To create a network element group:

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

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

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

You have created a network element group.

Adding a Network Element to a Network Element Group

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

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the desired 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.
   - If there are more than 25 network elements defined, the page does not display any of them. (*Figure 14: Add Network Element Page* shows an example.) Instead, use the Search Pattern field to filter the list. Enter an asterisk (*) to generate a global search, or a search pattern to locate only those network elements whose name matches the pattern (for example, `star*`, `*pGw`, or `*-*`). When you have defined a search string, click **Filter**; the page displays the filtered list.

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

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

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

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

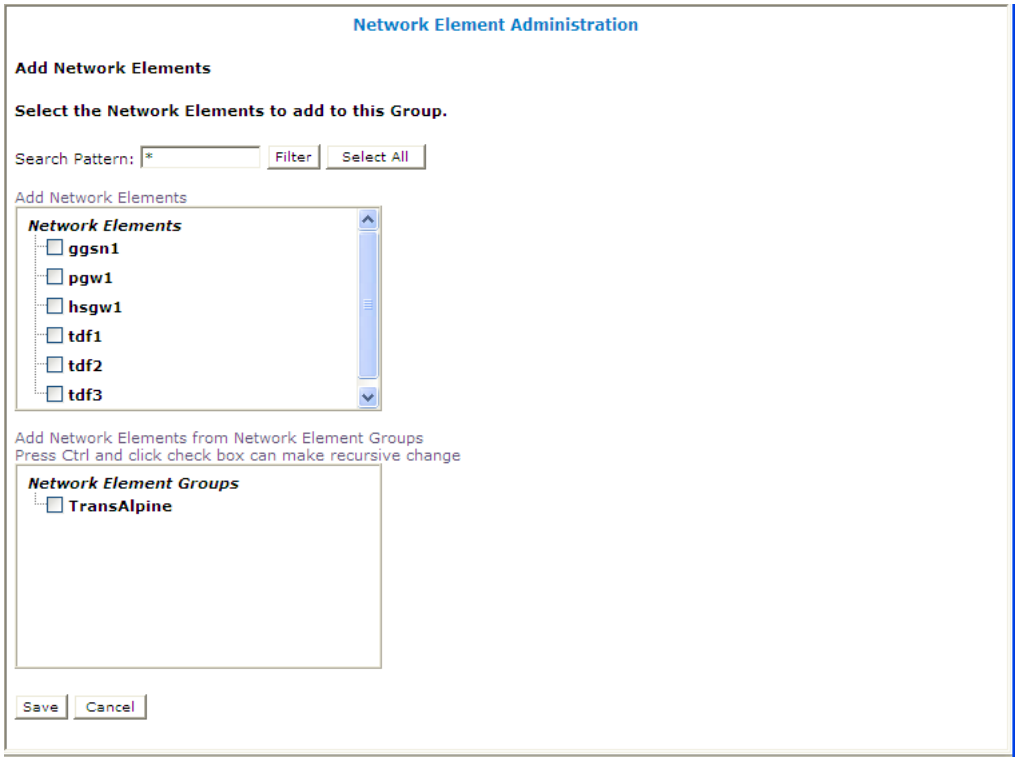


Figure 14: Add Network Element Page

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 desired network element group.
   The Network Element Administration page opens in the work area, displaying the contents of the selected network element group.
3. On the Network Element Administration page, click **Create Sub-Group**.
   The Create Group page opens.
4. Enter the name of the new sub-group.

   The name cannot contain quotation marks (") or commas (,).
5. Enter a text description of the sub-group.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The sub-group is added to the selected group, and now appears in the listing.

Deleting a Network Element from a Network Element Group

Removing a network element from a network element group or sub-group does not delete the network element from the ALL group, so it can be used again if needed. Removing a network element from the ALL group removes it from all other groups and sub-groups.

To remove a network element from a network element group or sub-group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the desired network element group or sub-group.

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

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

Modifying a Network Element Group

To modify a network element group or sub-group:

1. From the **Network** section of the navigation pane, select **Network Elements**.
   The content tree displays a list of network element groups; the initial group is **ALL**.
2. From the content tree, select the network element group or sub-group.
   The Network Element Administration page opens in the work area.
3. On the Network Element Administration page, click **Modify**.
   The Modify Group page opens.
4. Modify the name or description as desired.
5. When you finish, click **Save** (or **Cancel** to cancel the request).

The group is modified.

Deleting a Network Element Group or Sub-group

Deleting a network element group also deletes any associated sub-groups. However, any network elements associated with the deleted groups or sub-groups remain in the ALL group, from which they can be used again if needed. You cannot delete the ALL group.

To delete a network element group or sub-group:

1. From the 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. On the Network Element Administration page, click **Delete**.
   You are prompted, "Are you sure you want to delete this Group?"
4. Click **OK** to delete the group (or **Cancel** to cancel the request).

The network element group or sub-group is deleted.

Chapter 7

Managing Application Profiles

Topics:

Managing Application Profiles describes how to create and manage application profiles within the CMP.

About Application Profiles

An application is a service provided to users of your network for which you want to manage quality of service (QoS). Examples include voice over IP (VoIP) telephony, video on demand (VoD), and gaming. Once you have defined an application profile in the CMP database, you can associate it with the MPE devices that will manage that application.

When you offer application services in your network, there are usually one or more servers within your network that provide that service. These servers are referred to as Application Managers or Application Servers. When these servers are establishing a session that requires quality of service they issue a request to an MPE device.

When defining an application profile in the CMP database, you specify protocol information that is used by MPE devices to identify Application Managers and thus associate each request with its associated application. This lets the MPE device apply policy rules to the request that you have defined for the associated application.

Creating an Application Profile

To create an application profile:

1. From the **Policy Server** section of the navigation pane, select **Applications**.
   The content tree displays the **Applications** group.
2. Select the **Applications** group.
   The Application Administration page opens in the work area.
3. On the Application Administration page, click **Create Application**.
   The New Application page opens.
4. Enter the following application profile information:
   a) **General Configuration**:
      - **Name** — Name assigned to the application. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
      - **Description/Location** (optional) — Free-form text.
      - **Connection IP Address(s)** — Enter the IP address(es), in IPv4 or IPv6 format, that are used by Application Managers for this application. To include an address in the connection list, type it and click **Add**; to remove an address from the list, select it and click **Delete**.
      - **Latency Sensitive** — Select this option if the application is latency sensitive.

   b) **Diameter**:
      - **Diameter Identity** — Enter the Diameter identity (typically a fully qualified domain name) or identities used by application functions for this application. Click **Add** to define multiple values. To delete an existing value, select it from the list and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The application profile is created and stored in the **Applications** group.

The application profile is created.

Modifying an Application Profile

To modify an application profile:

1. From the **Policy Server** section of the navigation pane, select **Applications**.
   The content tree displays the **Applications** group.
2. Select the **Applications** group.
   The Application Administration page opens in the work area, listing the application profiles.
3. On the Application Administration page, select the application profile you want to modify.
   The profile is displayed.
4. Click **Modify**.
   The Modify Application page opens.
5. Modify the application profile information as necessary.
   See *Creating an Application Profile* for a description of the fields on this page.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The application profile is modified.

Deleting an Application Profile

To delete an application profile:

1. From the **Policy Server** section of the navigation pane, select **Applications**.
   The content tree displays the **Applications** group.
2. Select the **Applications** group.
   The Application Administration page opens in the work area.
3. Delete the application profile using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the profile you wish to delete.
   - From the content tree, select the application and click **Delete**. You are prompted: "Are you sure you want to delete this Application?"
4. Click **OK** (or **Cancel** to cancel the request).

The application profile is deleted from the CMP and all policy servers.

Chapter 8

Managing Match Lists

Topics:

Managing Match Lists defines how to create and manage match lists, which provide whitelist and blacklist functions in the CMP.

A match list is a set of defined values that can represent IDs or Internet addresses. Match list are used in policy rule requests. Match lists support wildcard matching.

Creating a Match List

To create a match list:

1. From the **Policy Server** section of the navigation pane, select **Match Lists**.
   The content tree displays the **Match Lists** group.
2. Select the **Match Lists** group.
   The Match List Administration page opens in the work area.
3. On the Match List Administration page, click **Create Match List**.
   The New Match List page opens.
4. Enter the following information:
   a) **Name** — The name assigned to the match list. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
   c) **Type** — Select from the following:
      - **string** (the default) — The list consists of strings.
      - **wildcard string** — The list consists of wildcard match patterns that use an asterisk (*) to match zero or more characters or a question mark (?) to match exactly one character.
      - **IPV4 address** — The list consists of IP addresses in IPv4 format.
      - **IPV6 address** — The list consists of IP addresses in IPv6 format.
   d) **Items** — Type an entry and click **Add**; to remove one or more entries from the list, select them and click **Delete**.
      The following match types are available:
      - APN
      - User Equipment Identity
      - USER IMSI
      - USER E.164
      - USER SIP URI
      - USER NAI
      - Serving MCC-MNC
      - Cell Identifier
      - Location Area Code
      - Serving Area Code
      - Routing Areas Code
      - Routing Area Identifier
      - Tracking Area Code
      - E-UTRAN Cell Identifier

      You can enter a match string combining multiple types (for example, a Location area Code and a Service Area Code) by separating the types with commas (,); for example, *lac1*,*sac1*. If you define multiple-type match lists, the types must be in the order shown.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The match list is created.

Modifying a Match List

To modify a match list:

1. From the navigation pane, select **Match Lists**.
   The content tree displays the **Match Lists** group.
2. From the content tree, select the **Match Lists** group.
   The Match List Administration page opens, displaying the list of defined match lists.
3. Select the match list you want to modify.
   Match list information is displayed.
4. Click **Modify**.
   The Modify Match List page opens.
5. Modify match list information as required.
   (You cannot change the type.)
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The match list is modified.

Note: You can also use the OSSI XML Interface to import and export match lists. This facilitates bulk changes or record keeping. For more information, see the *OSSI XML Interface Definition*.

Deleting a Match List

To delete a match list:

1. From the **Policy Server** section of the navigation pane, select **Match Lists**.
   The content tree displays the **Match Lists** group.
2. From the content tree, select the **Match Lists** group.
   The Match List Administration page opens, displaying the list of defined match lists.
3. Delete the match list using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the match list you want to delete.
   - From the content tree, select the match list and click **Delete**. You are prompted, "Are you sure you want to delete this Match List?"
4. Click **OK** (or **Cancel** to cancel the request).

The match list is deleted.

Chapter 9

Managing Quotas

Topics:

Managing Quotas describes how to create and manage Gx and Gy quotas in the CMP.

A quota sets a limit on a subscriber's usage, by any combination of volume (bytes of data), time (seconds of usage), or events (which are service specific). A quota can be applied by a policy rule trigger, or a quota can be applied by default if no policy rule is triggered.

Note: The actual options you see depend on whether your CMP system is configured in Gx mode, Gy mode, or both.

Creating a Quota Profile

In Gx mode, the MPE device can track and enforce a subscriber's total IP-CAN session time by day, week, or month, or track aggregate volume usage per IP-CAN session. In Gy mode, the MPE device can track usage for multiple services based on time, volume, or specific events.

Note: If the optional 3GPP-MS-TimeZone AVP is enabled, the MPE device can reset the quota based on the user local time. If so, and user equipment enters a different time zone near the end of a quota cycle, the subscriber may find that the quota reset earlier than expected, or the service provider may find that the quota reset later than expected.

To create a quota profile:

1. From the **Policy Server** section of the navigation pane, select **Quota Profile**.
   The content tree displays the **Quotas** group.
2. Select the **Quotas** group.
   The Quota Administration page opens in the work area.
3. On the Quota Administration page, click **Create Quota**.
   The New Quota page opens.
4. Enter the following information (*Figure 15: New Quota Page* shows an example):
   a) **Name** (required) — The name assigned to the quota. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
   c) **Quota Profile Type** — Select how the quota profile is assigned: **Subscriber** or **Pool**. The default value is **Subscriber**.

      Note: If you select the **Pool** option, the items in the quota profile can be added to support the quota account (Max Leakage Threshold, Dynamic Grant, etc). Once the quota profiles are created, they are applied to subscribers.

   d) **Max Leakage Threshold** — Maximum amount by which the usage can exceed. The range is 0 - 2147483647 (Max 32-bit integer.) The default is 0.
   e) **Enable Dynamic Grant** — (Optional) Specifies whether to track grant dynamically for the subscriber. This will cause the granted values to be updated by the MPE device to the SPR. If the box is checked, then the configuration is set to true. The default value is false.
   f) **Max Sessions Used For Dynamic Grant**— Number of simultaneous sessions used in the dynamic grant algorithm for granting quota. Enabled when the *Enable Dynamic Grant* box is checked. The range is 1 - 2147483647 (Max 32-bit integer.) The default is 20 sessions.

      Note: Do not enter a value if dynamic grant is not enabled.

   g) • If you select **Weekly**, a **Select Day** field appears. Weekly quotas are reset at midnight on the day you select from the list.
      • If you select **Daily**, an **Hour: Minute** field appears. Enter the hour and minute (in 24-hour format) at which quotas are reset.

   h) **Minimum Grant Size**— The minimum amount of remaining quota between the quota used and the maximum quota leakage value.
   i) **Reset Frequency** — Select how often subscriber quota usage counters are reset: **Monthly** (the default), **Weekly**, **Daily**, or **Never**.

j) **Reset Time Variable** — Optionally, specify a variable allowing the reset time for the quota bucket to be based on the value of the Custom1 custom field in the subscriber profile.
The MPE device uses the variable name and substitutes it to calculate the actual reset time for the quota bucket. The substitutable variable names are the same as the substitutable policy variables, that is, variables that are substituted in policy actions, such as {User.State.Property1}. Curly braces ({}) can be used but are not required.

- For a monthly quota bucket, specify a variable whose value is either a billing day (between 1 and 31) or a time of day (such as 11:02), in which case the billing day is retrieved using the current mechanism (that is, use the subscriber profile; if not set, use the global billing day); or an actual datetime, following the xsd:datetime (similar to custom fields and entity states), specifying the first reset time for the quota bucket. The MPE device manages setting the "nextResetTime" on the quota usage records by computing the closest datetime in the future that is a multiple of a month away from the configured datetime, conserving the time of day.
- For a weekly quota bucket, specify a variable containing either a time of day, in which case the day of week is taken from the configured "fixed" day of week, or a datetime representing the first reset time. The MPE device computes the next reset time similarly to the monthly bucket, but using multiple of one week instead.
- For a daily quota bucket, specify a variable containing either a time of day or a datetime. In both cases, the MPE device computes the next reset time based on the time of day.

k) **Report Offset Limit (minutes)** — This field defines the maximum amount of time after the Quota Reset usage report is sent. The field only becomes available when the value for Reset Frequency is set to any other value than *Never*. Enter a minute range from 0 to 180.

l) **Initial Total Volume Limit (bytes)** — Select **None** (the default) or select **Specify Limit** and enter a value.

m) **Initial Upstream Volume Limit (bytes)** — Gx or Gy mode. Select **None** (the default) or select **Specify Limit** and enter a value.

n) **Initial Downstream Volume Limit (bytes)** — Gx or Gy mode. Select **None** (the default) or select **Specify Limit** and enter a value.

o) **Volume Threshold Percentage** — Gy mode only. Enter a threshold percentage.
Below this percentage of volume quota, the charging traffic function must re-authorize.

p) **Initial Time Limit (seconds)** — Select **None** (the default) or select **Specify Limit** and enter a session time limit value.

q) **Time Threshold Percentage** — Gy mode only. Enter a threshold percentage.
Below this percentage of time quota, the charging traffic function must re-authorize.

r) **Initial number of Events (service-specific)** — Gy mode only. Select **None** (the default) or select **Specify Limit** and enter a value.

s) **Event Threshold Percentage** — Gy mode only. Enter a threshold percentage.
Below this percentage of event quota, the charging traffic function must re-authorize.

t) **Interim Reporting Interval (seconds)** — Gy mode only. How often the charging traffic function (such as a GGSN) must notify the MPE device. Select **None** (the default) or select **Specify Limit** and enter a time interval.

5. For Gy mode only, select a **Quota Exhaustion Action**, which specifies the action the charging traffic function (such as a GGSN) takes when a subscriber reaches the quota grant:

- **N/A** (the default) — Take no action.
- **TERMINATE** — Terminate the subscriber's session.
- **REDIRECT** — If you select this action, additional configuration fields appear:

- **Restriction Filters** — Enter a comma-separated list of Diameter IP Filter rules
- **Filter ID List** — Enter a comma-separated list of named filters on the charging traffic function
- **Redirect Server Type** — Select IPv4, IPv6, **URL**, or **SIP URI**
- **Redirect Server Address** — Enter the server address

- **RESTRICT ACCESS** — If you select this action, additional configuration fields appear:
  - **Restriction Filters** — Enter a comma-separated list of Diameter IP Filter rules
  - **Filter ID List** — Enter a comma-separated list of named filters on the charging traffic function

6. When you finish, click **Save** (or **Cancel** to discard your changes).
   The quota is created and stored in the **ALL** folder.

The quota is created.

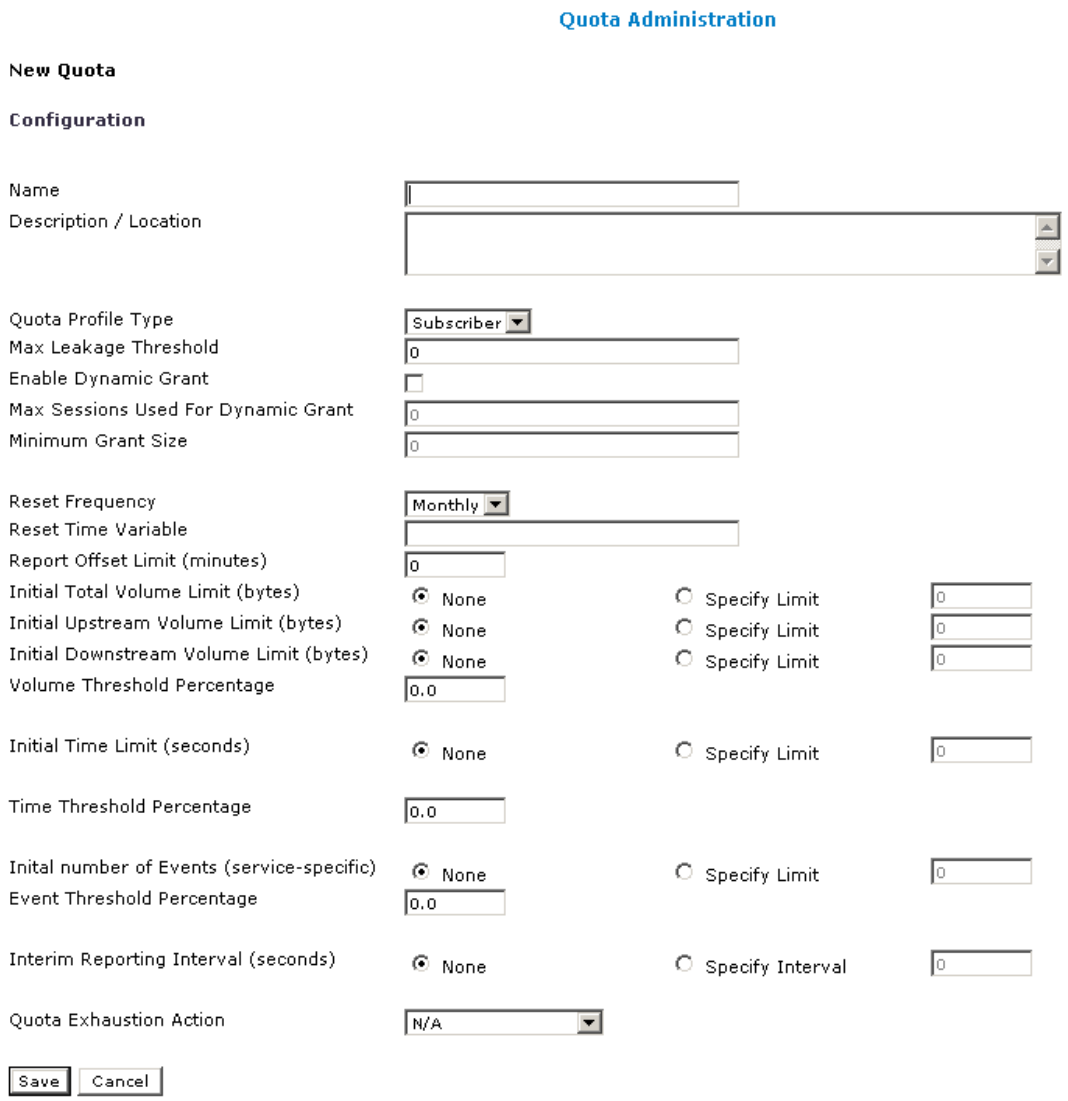


Figure 15: New Quota Page

Modifying a Quota

To modify a quota:

1. From the **Policy Server** section of the navigation pane, select **Quota Profile**.
   The content tree opens.
2. From the content tree, select the **Quotas** group.
   The Quota Administration page opens, displaying the list of defined quotas.
3. Select the quota you want to modify.
   The work area displays information about the quota.
4. Click **Modify**.
   The Modify Quota page opens.
5. Modify quota information as required.

   For a description of the fields contained on this page, see *Creating a Quota Profile*.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).

The quota is modified.

Deleting a Quota

You cannot delete a quota that is referenced in a policy. Otherwise, to delete a quota:

1. From the **Policy Server** section of the navigation pane, select **Quota Profile**.
   The content tree opens.
2. From the content tree, select the **Quotas** group.
   The Quota Administration page opens, displaying the list of defined quotas.
3. Delete the quota using one of the following methods:

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

   You are prompted, "Are you sure you want to delete this Quota?"
4. Click **OK** to delete the quota (or **Cancel** to cancel the request).

The quota is deleted.

Adding a Member to a Pooled Quota Group

You can add a member and associate a subscriber when creating 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. Enter the following information:
   a) **Data Source Primary Diameter Identity**— Select one of the configured V3 data sources.

      Key Fields: (one of the following is required)

   b) **Pool ID**— A string indicating if the subscriber is a member of a pool. It is a alphanumeric string, with no allowed spaces. You can have dashes and underscores. *0* is invalid.

      Note: The length cannot exceed 255 characters.

      Subscriber Information: (optional)

   c) **Account ID**— The account identification given to the specific quota.
   d) **Billing Day**— The billing day of the subscriber pool. This field is used only for monthly.
   e) **Tier**— If you click **Manage**, it will allow you to enter or select a tier.
   f) **Entitlements**— If you click **Manage**, it will allow you to add or move selected entitlements.
   g) **Custom 1, Custom 2, Custom 3, Custom 4, Custom 5** — A list of name value fields. These can be referred to from policies.
   h) **Custom N**— If you click **Add**, you can add additional custom fields.

      Add a member or associate a subscriber to the quota by selecting the **Key Type** and adding a **Key String**.

      Note: When associating a subscriber, the subscriber **key string** must be entered.

      Membership Information: (optional)

   i) **Key Type**— The type of Pool ID. You can select one of the following:
      - **E.164 (MSISDN)**
      - **IMSI**
      - **NAI**

   j) **Key String**— If you click **Add**, it will allow you to add a Pool ID search value.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

Querying by Pool ID

You can query a newly created 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** for the created quota.
   The Pool Group Quota Profile page opens with the search results. The following three related tabs are displayed:
   - **Pool Profile**
   - **Pool Quota**
   - **Pool State**
3. You can select the **Modify**, **Delete**, or **Back to Search Page** options, if so desired.

Creating a Pool Quota Profile

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

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. Click **Create**.
6. Enter the following:
   - **Name**— Select the name of the pool state.
   - **Time** (seconds) — The amount of time attributed to the quota in seconds.
   - **Total Volume** (bytes) — The amount of volume attributed to a length of time.
   - **Upstream Volume** (bytes) — Traffic from the handset (or other device) to the network.
   - **Downstream Volume** (bytes) — Traffic directed to the handset or other device.
   - **Service Specific Event** — Tracks text information.
   - **Next Reset Time** — The reset date and time of the subscriber or pool quota usage.

     Note: This is typically the billing day, although for a daily quota the usage is normally reset at midnight or shortly thereafter.
7. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Pool Quota Profile is created.

Modifying a Pool Quota Profile

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

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 Quota Profile**.
   The Pool Quota Profile view displays.
5. Select the **Name** of the profile that you want to modify.
6. Modify any of the following fields:

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

- **Time (seconds)**
- **Total Volume (bytes)**
- **Upstream Volume (bytes)**
- **Downstream Volume (bytes)**
- **Service Specific Event**
- **Next Reset Time**

7. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Pool Quota Profile content is modified.

Deleting a Pool Quota Profile

A pool quota profile can be deleted.

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

Modifying a Pool Profile

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

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 section displays.
5. Modify any of the field information.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The Pool Profile content is modified.

Deleting a Pool Profile

A pool profile can be deleted.

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The Pool Profile page opens with Pool Profile as the default.
4. Click **Delete**.
   You are prompted: "Are you sure you want to delete this pool profile?"
5. Click **OK**.
6. The Pool Profile is deleted.

Creating a Pool State

A pool state can be created when the ShProfile V3 data source is selected.

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Select a **Data Source Primary Diameter Identity**, and the **Key Type** of **Pool ID.**
   The Data Source Primary Diameter Identity and Key Type are selected.
3. Enter a **Key String**, and click **Search**.
   The Pool Profile page opens.
4. Click **Pool State**.
5. Click **Create**.
   The Create Property section is displayed.
6. Enter the following:
   - **Name**— The name of the pool state.
   - **Value**— The value can be any string. For example, Profile V1, V2, V3.
7. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Pool Entity State Properties section is displayed, with the Pool Quota Group Key Fields and the searched Pool ID.

Modifying a Pool State

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

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**.
8. When you finish, click **Save** (or **Cancel** to discard your changes).
   The Pool State content is modified.

Deleting a Pool State

A pool state can be deleted.

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**.
   Your chosen properties are deleted.

Chapter 10

Managing Services and Rating Groups

Topics:

Managing Services and Rating Groups describes how to create and manage Gy services and rating groups in the CMP.

A service is an identification of a class of traffic: for example, voice, peer-to-peer, or multimedia. You can apply a quota or a rating group (but not both) to a service.

For organizational purposes, you can associate services into rating groups. This is a convenient way of allowing multiple services to share the same quota.

Note: For information on defining quotas, see *Managing Quotas*.

Creating a Service

To create a service:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree displays the **Services & Rating Groups** group.
2. Select the **Services & Rating Groups** group.
   The Service Administration page opens in the work area.
3. On the Service Administration page, click **Create Service**.
   The New Service page opens.
4. Enter the following information:
   a) **Name** (required) — The name assigned to the service. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
   c) **Service Identifier** — A unique numeric identifier.
   d) **Rating Group** — Select **None** (the default) or one of the rating groups defined in the CMP.
   e) **Quota** — Select **None** (the default) or one of the quotas defined in the CMP.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The service is created and appears in the **Services** group

The service is created.

Modifying a Service

To modify a service:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree opens.
2. From the content tree, select the **Services** group.
   The Service Administration page opens, displaying the list of defined services.
3. Select the service you want to modify.
   The work area displays information about the service.
4. Click **Modify**.
   The Modify Service page opens.
5. Modify service information as required.
   For a description of the fields contained on this page, see *Creating a Service*.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).

The service is modified.

Deleting a Service

To delete a service:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree opens.
2. From the content tree, select the **Services** group.
   The Service Administration page opens, displaying the list of defined services.
3. Delete the service using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the service you want to delete.
   - From the content tree, select the service and click **Delete**.

   You are prompted, "Are you sure you want to delete this Service?"
4. Click **OK** to delete the service (or **Cancel** to cancel the request).

The service is deleted.

About Rating Groups

For organizational purposes, you can aggregate services into rating groups. The same quotas apply to all the services in a rating group. Once a rating group is created, you can populate it with services.

Creating a Rating Group

To create a rating group:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree displays the **Services & Rating Groups** group.
2. Select the **Services & Rating Groups** group.
   The Service Administration page opens in the work area.
3. On the Service Administration page, click **Create Rating Group**.
   The Create Rating Group page opens.
4. Enter the following information:
   a) **Name** (required) — The name assigned to the rating group. The name can be up to 255 characters long and must not contain quotation marks ("), colons (:), or commas (,).
   b) **Description/Location** — Free-form text.
   c) **Rating Group Identifier** — A unique numeric identifier.
   d) **Quota** — Select **None** (the default) or one of the quotas defined in the CMP.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The rating group is created and stored in the **Services & Rating Groups** folder.

The rating group is created.

Adding a Service to a Rating Group

To add a service to a rating group:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree displays the **Services & Rating Groups** group.
2. In the content tree, select the rating group to which you want to add a service.
   The Rating Group Administration page opens in the work area.
3. On the Rating Group Administration page, click **Add Service**.
   The Add Service page opens, displaying the services not already part of the group.
4. Click on the service you want to add; use the Ctrl or Shift keys to select multiple services.
5. When you finish, click **Save** (or **Cancel** to cancel the request).

The service is added to the selected rating group.

Modifying a Rating Group

You cannot rename a rating group that is referenced in a policy. Otherwise, to modify a rating group:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree displays the **Services & Rating Groups** group.
2. In the content tree, select the rating group you want to modify.
   The work area displays information about the rating group.
3. On the Rating Group Administration page, click **Modify**.
   The Modify Rating Group page opens.
4. Make changes as desired. For information on the fields on this page, see *Creating a Rating Group*.
5. When you finish, click **Save** (or **Cancel** to cancel the request).

The rating group is modified.

Removing a Service from a Rating Group

Removing a service from a rating group does not delete the service. To delete a service, see *Deleting a Service*.

To remove a service from a rating group:

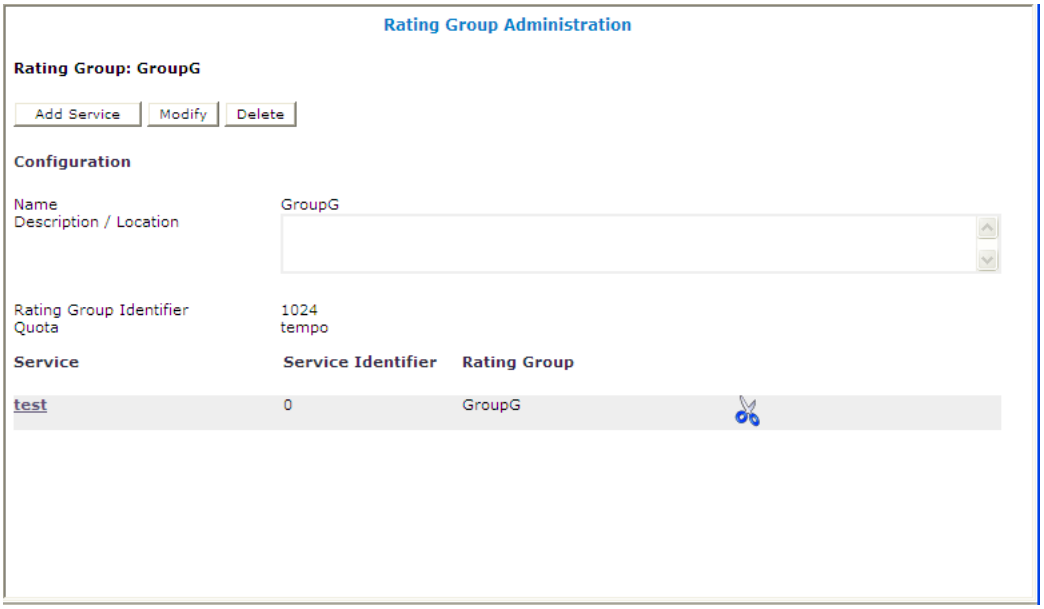
1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree displays the **Services & Rating Groups** group.
2. In the content tree, select the rating group from which you want to remove the service.
   The work area displays information about the rating group.
3. Remove the service using one of the following methods:
   - On the Rating Group Administration page, click the Remove icon, located to the right to the service you want to remove. The service is removed from the rating group immediately; there is no confirmation message.
   - From the content tree, select the service in the rating group; the Service Administration page opens, displaying information about the service. Click **Delete**. You are prompted: “Are you sure you want to delete this Service?” Click **OK** (or **Cancel** to abandon the request).

The service is removed from the rating group.

Deleting a Rating Group

Deleting a rating group does not delete any services associated with the deleted group; services remain in the Services & Rating Groups group. You cannot delete the Services & Rating Groups group. You cannot delete a rating group that is referenced in a policy. Otherwise, to delete a rating group:

1. From the **Policy Server** section of the navigation pane, select **Services & Rating Groups**.
   The content tree displays the **Services & Rating Groups** group.
2. From the content tree, select the rating group you want to delete.
   The Rating Group Administration page opens in the work area, displaying the contents of the selected rating group; for example:



3. On the Rating Group Administration page, click **Delete**.
   You are prompted, "Are you sure you want to delete this Group?"
4. Click **OK** (or **Cancel** to cancel the request).

The rating group is deleted.

Chapter 11

Managing Traffic Profiles

Topics:

Managing Traffic Profiles defines how to create and manage traffic profiles in the CMP.

About Traffic Profiles

A traffic profile is a set of values defined for parameters that are used in protocol messages within the MPE device. Typically, these traffic profile values are used to define the Quality of Service (QoS) for sessions that are managed by those protocol messages. You can use traffic profiles to implement policy and charging control (PCC) rules.

Traffic profiles are used in the MPE device under several situations; for example:

- They define default settings for protocol messages (see *Configuring Protocol Options on the Policy Server*)
- They modify protocol messages, thus modifying the QoS for sessions managed by those messages (see *Creating a New Policy*)

A traffic profile can be applied by a policy rule trigger, or by default if no policy rule is triggered.

Each traffic profile has a type associated with it. Since each protocol supports different parameters for controlling QoS settings, the available MPE parameters depend on the underlying protocol. Therefore, each profile type is associated with a single protocol, but a single protocol can support multiple profile types.

You can create multiple traffic profiles of the same type, as the values of the parameters for each profile determine the actual QoS that is associated with that profile. For example, one possible set of traffic profiles is as follows:

- **Default** — default predefined profile
- **P2P** — profile for peer-to-peer traffic
- **RATE_LIMIT_128K** — profile to limit download rate to 128 Kbps
- **RATE_LIMIT_64K** — profile to limit download rate to 64 Kbps

Creating a Traffic Profile

To create a traffic profile:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays the **Traffic Profiles** group. The default group is **ALL**.
2. Select the **Traffic Profiles** group.
   The Traffic Profile Administration page opens in the work area, listing available traffic profiles.
3. On the Traffic Profile Administration page, click **Create Traffic Profile**.
   The New Traffic Profile page opens.
4. Enter the following information:
   a) **Name** — The name assigned to the profile. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Traffic Profile Type** — Select from the following:
      - **Diameter QoS**
      - **PCC Profile**
      - **PCC Rule** — a policy and charging control rule.

- **Predefined PCC Rule** — a pre-defined PCC rule residing on the PCEF device.
- **Predefined PCC Rule Base** — a pre-defined group of PCC rules residing on the PCEF device.

c) Protocol Fields — The set of protocol fields displayed on the Traffic Profile page varies depending on the Traffic Profile Type selected. *Table 5: Traffic Profile Type Configuration Parameters* describes the protocol fields for each traffic profile type.

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

The traffic profile is defined.

Table 5: Traffic Profile Type Configuration Parameters

Traffic Profile Type	Configuration Parameter	Description
Diameter QoS	QoS Class Identifier	Identifies the QoS class. Select from the following: • **1 = Conversational speech** • **2 = Conversational** • **3 = Streaming speech** • **4 = Streaming** • **5 = Interactive with priority 1 signalling** • **6 = Interactive with priority 1** • **7 = Interactive with priority 2** • **8 = Interactive with priority 3** • **9 = Background**
	Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
	Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
	Uplink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for uplinks (user equipment to network). Only applicable if the QoS class identifier is between 1 and 4.
	Downlink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for downlinks (network to user equipment). Only applicable if the QoS class identifier is between 1 and 4.
	ARP Priority Level	Allocation and Retention Priority level of the service flows associated with this Diameter profile. Specify **1** (highest) to **15** (lowest).
	ARP Preemption Capability	Select from the following: • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**

Traffic Profile Type	Configuration Parameter	Description
	ARP Preemption Vulnerability	Select from the following: • **PREEMPTION_VULNERABILITY_ENABLED** • **PREEMPTION_VULNERABILITY_DISABLED**
PCC Profile	QoS Class Identifier	Identifies the QoS class. Select from the following: • **1 = Conversational speech** • **2 = Conversational** • **3 = Streaming speech** • **4 = Streaming** • **5 = Interactive with priority 1 signalling** • **6 = Interactive with priority 1** • **7 = Interactive with priority 2** • **8 = Interactive with priority 3** • **9 = Background**
	Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
	Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
	Uplink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for uplinks (user equipment to network). Only applicable if the QoS class identifier is between 1 and 4.
	Downlink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for downlinks (network to user equipment). Only applicable if the QoS class identifier is between 1 and 4.
	ARP Priority Level	Allocation and Retention Priority level of the service flows associated with this PCC profile. Specify **1** (highest) to **15** (lowest).
	ARP Preemption Capability	Select from the following: • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**
	ARP Preemption Vulnerability	Select from the following: • **PREEMPTION_VULNERABILITY_ENABLED** • **PREEMPTION_VULNERABILITY_DISABLED**
	Service Identifier	Credit-control service identifier associated with the traffic defined by this profile. Only applicable if online charging is enabled.

Traffic Profile Type	Configuration Parameter	Description
	Rating Group	Credit-control rating group associated with the traffic defined by this profile. Only applicable if online charging is enabled.
	Reporting Level	Select from the following: • **SERVICE_IDENTIFIER_LEVEL** • **RATING_GROUP_LEVEL**
	Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • **DISABLE_ONLINE** • **ENABLE_ONLINE**
	Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following: • **DISABLE_OFFLINE** • **ENABLE_OFFLINE**
	Metering Method	Specifies whether this profile meters by duration, volume, or both. Select from the following: • **DURATION** • **VOLUME** • **DURATION_VOLUME**
	Flow Status	Select from the following: • **ENABLED_UPLINK** • **ENABLED_DOWNLINK** • **ENABLED** • **DISABLED**
	Flow Description(s)	IP flows associated with this profile. A comma-separated list of Diameter IP Filter rules following the format specified in RFC 3588 section 4.3.
	Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.
PCC Rule	Rule Name	Name identifying the provisioned PCC (policy and charging control) rule. The name must not contain apostrophes (‘).
	QoS Class Identifier	Identifies the QoS class. Select from the following: • **1 = Conversational speech** • **2 = Conversational**

Traffic Profile Type	Configuration Parameter	Description
		• **3 = Streaming speech** • **4 = Streaming** • **5 = Interactive with priority 1 signalling** • **6 = Interactive with priority 1** • **7 = Interactive with priority 2** • **8 = Interactive with priority 3** • **9 = Background**
	Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
	Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
	Uplink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for uplinks (user equipment to network). Only applicable if the QoS class identifier is between 1 and 4.
	Downlink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for downlinks (network to user equipment). Only applicable if the QoS class identifier is between 1 and 4.
	ARP Priority Level	Allocation and Retention Priority level of the service flows associated with this PCC rule. Specify **1** (highest) to **15** (lowest).
	ARP Preemption Capability	Select from the following: • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**
	ARP Preemption Vulnerability	Select from the following: • **PREEMPTION_VULNERABILITY_ENABLED** • **PREEMPTION_VULNERABILITY_DISABLED**
	Service Identifier	Credit-control service identifier associated with the traffic defined by this rule. Only applicable if online charging is enabled.
	Rating Group	Credit-control rating group associated with the traffic defined by this rule. Only applicable if online charging is enabled.
	Monitoring Key	Value of the monitoring key.
	Reporting Level	Select from the following: • **SERVICE_IDENTIFIER_LEVEL**

Traffic Profile Type	Configuration Parameter	Description
		• **RATING_GROUP_LEVEL**
	Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • **DISABLE_ONLINE** • **ENABLE_ONLINE**
	Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following: • **DISABLE_OFFLINE** • **ENABLE_OFFLINE**
	Metering Method	Specifies whether this profile meters by duration, volume, or both. Select from the following: • **DURATION** • **VOLUME** • **DURATION_VOLUME**
	Flow Status	Select from the following: • **ENABLED_UPLINK** • **ENABLED_DOWNLINK** • **ENABLED** • **DISABLED**
	Flow Description(s)	IP flows associated with this profile. This is a comma-separated list of Diameter IP Filter rules following the format specified in RFC 3588 section 4.3.
	Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.
Predefined PCC Rule	Rule Name	Name of the predefined rule. The name must not contain apostrophes (‘).
	Description	Description of the rule.
	Type	Select from the following: • **SESSION_LEVEL** • **PCC_RULE_LEVEL** • **ADC_RULE_LEVEL**
	Key	Unique string that identifies the quota profile to be used by a PCC rule for usage tracking.

Traffic Profile Type	Configuration Parameter	Description
Predefined PCC Rule Base	Rule-Base Name	Name of the predefined rule-base name. The name must not contain apostrophes (‘).
	Description	Description of the rule base.

Modifying a Traffic Profile

To modify a traffic profile:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree opens.
2. From the content tree, select the **Traffic Profiles** group.
   The Traffic Profile Administration page opens, displaying the list of defined traffic profiles.
3. Select the profile you want to modify.
   Profile information is displayed.
4. Click **Modify**.
   The Modify Traffic Profile page opens.
5. Modify profile information as required.
   For a description of the fields contained on this page, see *Creating a Traffic Profile*.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).

The traffic profile is modified.

Deleting a Traffic Profile

To delete a traffic profile:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree opens.
2. From the content tree, select the **Traffic Profiles** group.
   The Traffic Profile Administration page opens, displaying the list of defined traffic profiles.
3. Delete the traffic profile using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the traffic profile you want to delete.
   - From the content tree, select the traffic profile and click **Delete**.

   You are prompted, “Are you sure you want to delete this Traffic Profile?”
4. Click **OK** to delete the traffic profile (or **Cancel** to cancel the request).

The traffic profile is deleted.

Traffic Profile Groups

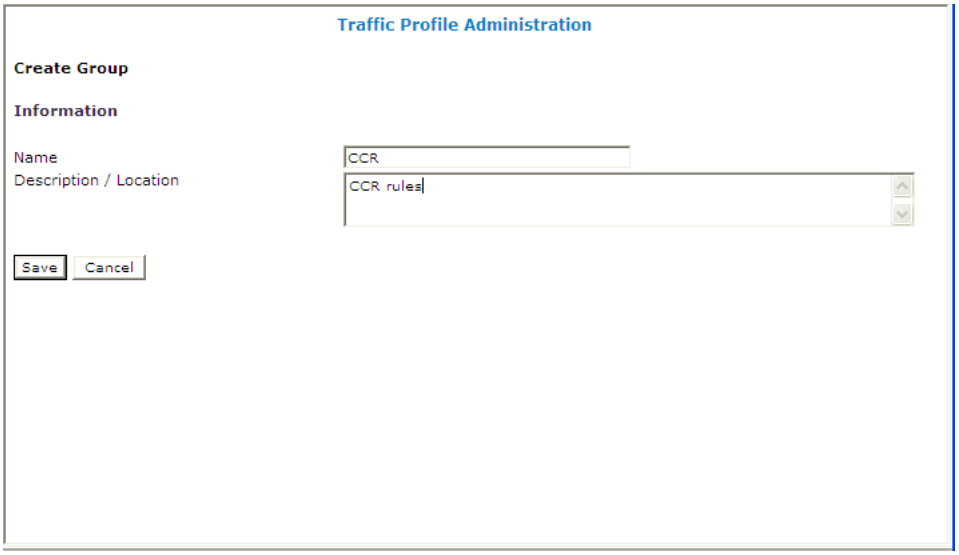
For organizational purposes, you can aggregate traffic profiles into groups. Once a traffic profile group is created, it can be populated with individual traffic profiles. The following subsections describe how to manage traffic profile groups.

Creating a Traffic Profile Group

To create a traffic profile group:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays a list of traffic profile groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The Traffic Profile Administration page opens in the work area, listing all defined traffic profiles.
3. On the Traffic Profile Administration page, click **Create Group**.
   The Create Group editor page opens.
4. Enter the name of the new traffic profile group.

   The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
5. Optionally, enter a description of the traffic profile group; for example:



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

The traffic profile group is created.

Adding a Traffic Profile to a Traffic Profile Group

To add a traffic profile to a traffic profile group:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays a list of traffic profile groups; the initial group is **ALL**.

2. From the content tree, select the desired traffic profile group.
   The Traffic Profile Administration page opens in the work area, displaying the contents of the selected traffic profile group.
3. On the Traffic Profile Administration page, click **Add Traffic Profile**.
   The Add Traffic Profile page opens, displaying the traffic profiles not already part of the group. *Figure 16: Add Traffic Profile Page* shows an example.
4. Click on the traffic profile you want to add; use the Ctrl or Shift keys to select multiple traffic profiles.
5. When you finish, click **Save** to add the traffic profile to the selected group (or **Cancel** to cancel the request).

The traffic profile is added to the traffic profile group.

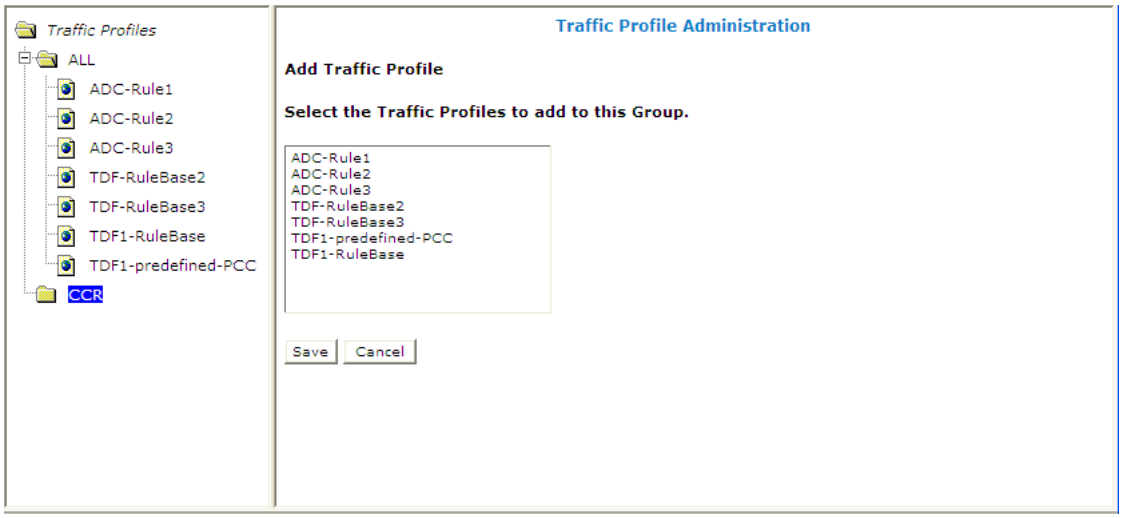


Figure 16: Add Traffic Profile Page

Modifying a Traffic Profile Group

To modify a traffic profile group:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays a list of traffic profile groups; the initial group is **ALL**.
2. From the content tree, select the traffic profile group you want to modify.
   The Traffic Profile Administration page opens in the work area.
3. On the Traffic Profile Administration page, click **Modify**.
   The Modify Group page opens.
4. Edit the information in the fields.
   The name cannot contain quotation marks (") or commas (,).
5. When you finish, click **Save** (or **Cancel** to cancel the request).

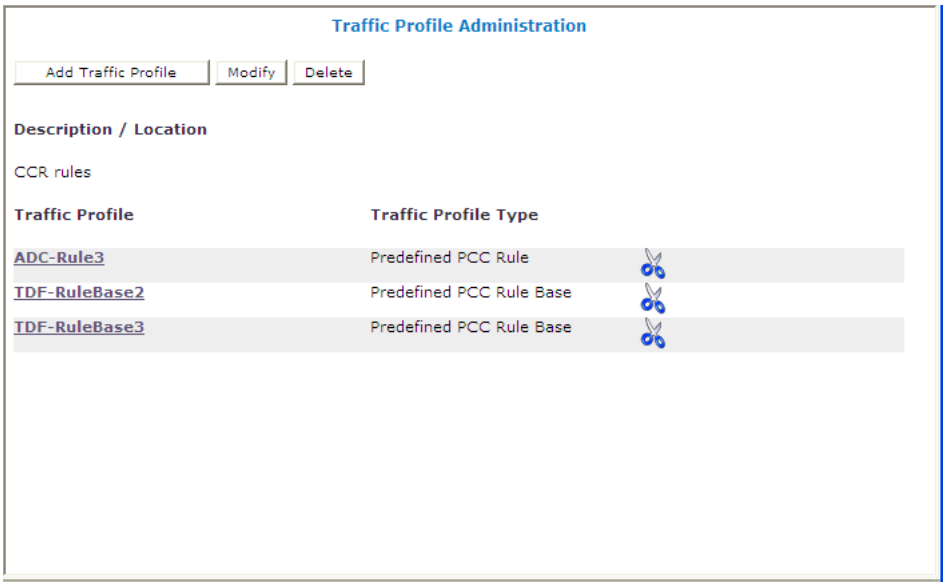
The group is modified.

Removing a Traffic Profile from a Traffic Profile Group

Removing a traffic profile from a traffic profile group does not delete the profile. To delete a traffic profile, see *Deleting a Traffic Profile*.

To remove a traffic profile from a traffic profile group:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays the list of traffic profile groups.
2. From the content tree, select the desired traffic profile group.
   The Traffic Profile Administration page opens in the work area, displaying the contents of the selected traffic profile group; for example:



3. Remove the traffic profile using one of the following methods:
   - Click the Delete icon, located to the right of the traffic profile you want to remove.
   - From the traffic profile group in the content tree, select the traffic profile and click **Remove**.

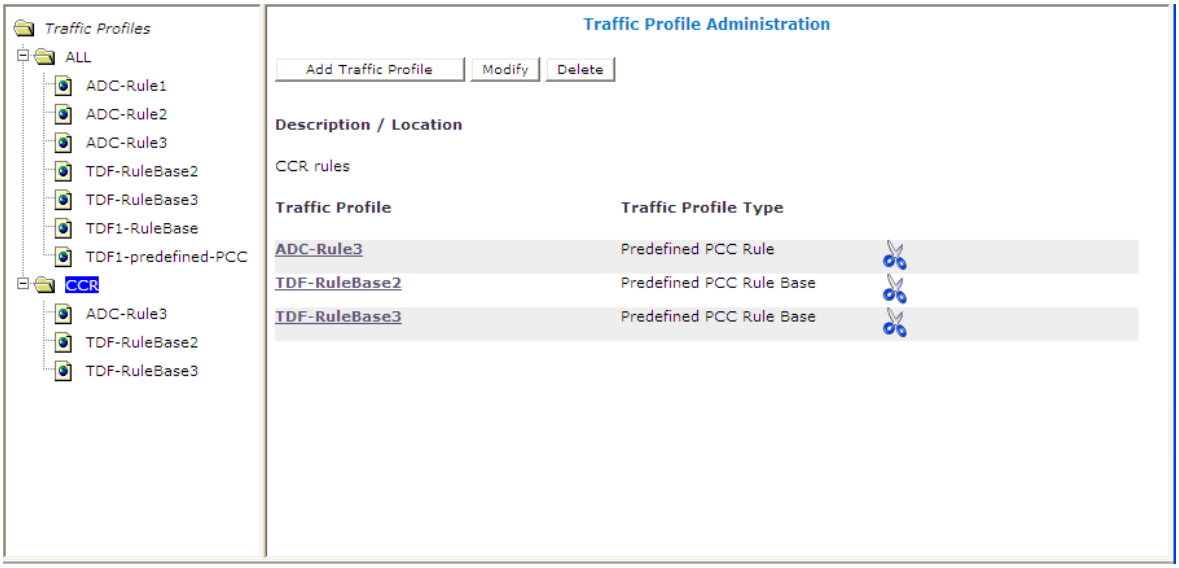
The traffic profile is removed from the group immediately; there is no confirmation message.

Deleting a Traffic Profile Group

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

To delete a traffic profile group:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays the list of traffic profile groups.
2. From the content tree, select the traffic profile group you want to delete.
   The Traffic Profile Administration page opens in the work area, displaying the contents of the selected traffic profile group; for example:



3. On the Traffic Profile Administration page, click **Delete**.
   You are prompted, "Are you sure you want to delete this Group?"
4. Click **OK** to delete the group (or **Cancel** to cancel the request).

The traffic profile group is deleted.

Chapter 12

Managing Retry Profiles

Topics:

Managing Retry Profiles describes how to create and manage retry profiles in the CMP.

About Retry Profiles

A retry profile specifies the circumstances under which installation of a policy and charging control (PCC) rule is retried if the rule is reported to have failed (for example, because the establishment of a network-initiated bearer failed), as indicated by a Charging-Rule-Report. The retry action consists of a configurable number of retry attempts, after initially waiting a configurable period of time and then using an exponential back-off algorithm.

A retry profile can be applied by a policy rule trigger, or by default if no policy rule is triggered.

You can define multiple retry profiles, each with different parameter values.

Note: See *Configuring Data Source Interfaces* for information on configuring the interval to wait for a failure before considering the rule installation successful.

Creating a Retry Profile

To create a retry profile:

1. From the **Policy Server** section of the navigation pane, select **Retry Profile.**
   The content tree displays the **Retry Profile** group.
2. Select the **Retry Profile** group.
   The Retry Profile Administration page opens in the work area, listing available retry profiles.
3. On the Retry Profile Administration page, click **Create Retry Profile.**
   The New Retry Profile page opens (*Figure 17: New Retry Profile Page*).
4. **Enter the following information:**
   a) **Name** — Unique name assigned to the profile. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text describing the profile.
   c) **Retry Profile Type** — The available choice is **PCC Retry Profile.**
   d) **Maximum Retry Attempt** — The maximum number of retry attempts after an initial failure, from 1 to 10.
   The default is five attempts.
   e) **Initial Retry Interval** — How long to wait, in seconds, after a reported failure before retrying. The default is 10 seconds. Type a value from 0 to 30 seconds. To specify a retry immediately after a reported failure, type 0.
   f) **Maximum Retry Interval** — The maximum wait, in seconds, after a reported failure before retrying.
   The default is 60 seconds. Type a value from from 1 to 180 seconds.
   g) **Rule Failure Code** — The upper box lists available rule failure codes; the lower box lists rule failure codes installed in the profile.
   The failure codes RESOURCES_LIMITATION and RESOURCE_ALLOCATION_FAILURE are installed by default. To add a rule failure code to the profile, select it in the upper box and click **Add**. To remove a rule failure code from the profile, select it in the lower box and click **Delete**.

   Note: If the profile does not contain any rule failure codes, the MPE device will retry the rule installation regardless of the failure code reported.

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

The retry profile is created.

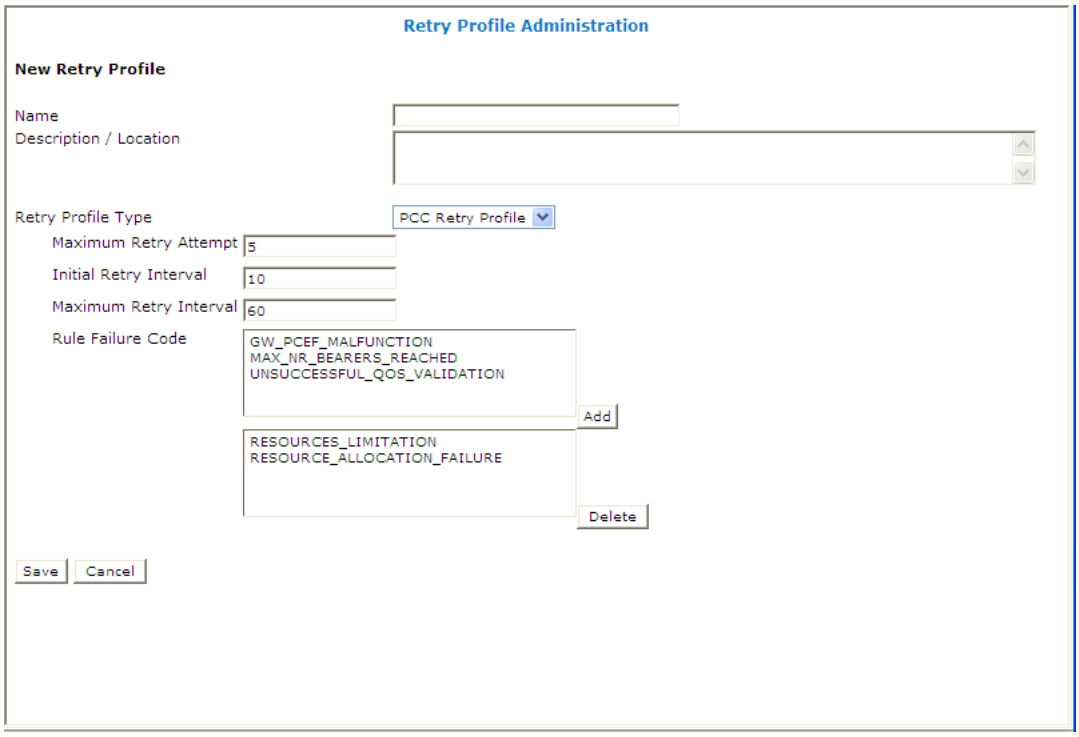


Figure 17: New Retry Profile Page

Modifying a Retry Profile

To modify a retry profile:

1. From the **Policy Server** section of the navigation pane, select **Retry Profile**.
   The content tree opens.
2. From the content tree, select the **Retry Profile** group.
   The Retry Profile Administration page opens, displaying the list of defined retry profiles.
3. Select the profile you want to modify.
   Profile information is displayed.
4. Click **Modify**.
   The Modify Retry Profile page opens.
5. Modify profile information as required.
   For a description of the fields contained on this page, see *Creating a Retry Profile*.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).

The retry profile is modified.

Deleting a Retry Profile

To delete a retry profile:

1. From the **Policy Server** section of the navigation pane, select **Retry Profile**.
   The content tree opens.
2. From the content tree, select the **Retry Profile** group.
   The Retry Profile Administration page opens, displaying the list of defined retry profiles.
3. Delete the retry profile using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the retry profile you want to delete.
   - From the content tree, select the retry profile and click **Delete**. You are prompted, "Are you sure you want to delete this Retry Profile?"
4. Click **OK** to delete the retry profile (or **Cancel** to cancel the request).

The retry profile is deleted.

Chapter 13

Managing Charging Servers

Topics:

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

About Charging Servers

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

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

Defining a Charging Server

To define a charging server:

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

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

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

      Enter up to 250 characters.

   c) **Host Name** (required) — Fully qualified domain name assigned to the charging server.
   d) **Port** — The port number on which the charging server is listening for messages.
      If left blank, port 3868 is used.
   e) **Transport** — The transport protocol used to communicate with the charging server.
      Select **tcp**, **udp**, or **sctp** from the list.
   f) **Protocol** — Specifies the AAA protocol used to communicate with the charging server.
      Select **diameter**, **radius**, or **tacacs+** from the list.

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

   g) **Security** — Select if transport security is used to communicate with the charging server.
5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The charging server is displayed in the Charging Server Administration page.

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

Modifying a Charging Server

To modify the definition of a charging server:

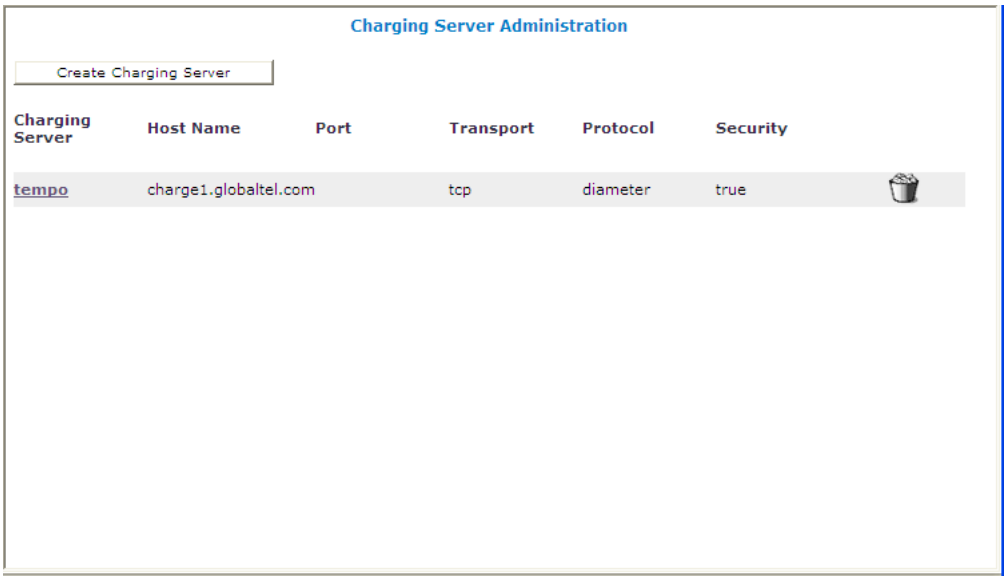
1. From the **Policy Server** section of the navigation pane, select **Charging Servers**.
   The Charging Server Administration page opens in the work area, listing the defined charging servers.
2. On the Charging Server Administration page, select the charging server you want to modify.
   The Charging Server Administration page displays information about the charging server.
3. Click **Modify**.
   The Modify Charging Server page opens.
4. Modify charging server information as required.
   For a description of the fields contained on this page, see *Defining a Charging Server*.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The charging server definition is modified.

Deleting a Charging Server

To delete a charging server:

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



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

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

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

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

The charging server definition is removed from the list.

Associating a Charging Server with an MPE Device

To associate a charging server with an MPE device:

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

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

Chapter 14

Managing Policy Time Periods

Topics:

Managing Policy Time Periods describes how to create and manage time periods in the CMP.

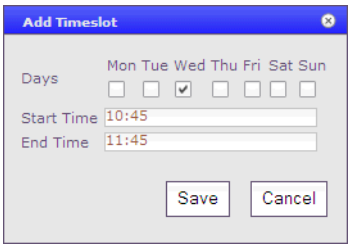
About Policy Time Periods

You can define a library of time periods to specify in policy time-of-day conditions. For example, you can define “peak” and “off-peak” periods, and then associate different policies with different periods. Time periods can include different times of day as well as different days of the week.

Creating a Time Period

To create a time period:

1. From the **Policy Server** section of the navigation pane, select **Time Periods**.
   The content tree displays the **Time Period Administration** group.
2. From the content tree, select the **Time Period Administration** group.
   The Time Period Administration page opens in the work area.
3. Click **Create Time Period**.
   The New Time Period page opens.
4. To configure the time period, enter the following:
   a) **Name** (required) — Name of the time period.
      The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description / Location** — A descriptive phrase.
   c) **Precedence** (required) — A positive integer.
      The lower the number, the higher the precedence. If time periods overlap, the time period with the highest precedence (lowest number) applies.
   d) **Time Slot** (required) — Click in the time slot area.
      The Add Timeslot window opens; for example:



   - To create a time slot, select one or more days, and start and end times for the selected day(s), in 15-minute intervals, in the format *hh*:*mm*. A time period must be at least one hour. When you finish, click **Save**.
   - To edit an existing time slot, select it; the Edit Timeslot window opens. Edit the timeslot and click **Save**.
   - To delete an existing time slot, select it; the Edit Timeslot window opens. Click **Delete**; the timeslot is deleted.

5. When you finish defining the time period, click **Save** (or **Cancel** to cancel your request).

The time period is added to the library, and you can now include it in a policy time condition.

Deleting a Time Period

To delete a time period:

1. From the **Policy Server** section of the navigation pane, select **Time Periods**.
   The content tree displays the **Time Period Administration** group.
2. From the content tree, select the **Time Period Administration** group.
   The Time Period Administration page opens in the work area.
3. Select the time period using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the time period you want to delete.
   - From the content tree, select the time period and click **Delete**. You are prompted, "Are you sure you want to delete this Time Period?"
4. Click **OK** (or **Cancel** to cancel the request).

The time period is deleted.

Time-of-Day Triggers

Time-of-day triggers are supported for Diameter Gx sessions. If time-of-day triggers are configured, the MPE device periodically examines policies and provisions the appropriate policies to enforcement points, even for connected subscribers.

For example, if a subscriber connects to a network during an off-peak period and continues to use the network into a peak period, the MPE device removes the off-peak policy rule at the enforcement point at the appropriate time and installs the peak policy rule.

The MPE device evaluates policies every 15 minutes: on the hour, 15 minutes past the hour, 30 minutes past the hour, and 45 minutes past the hour. If a time period is changed, it can take up to 15 minutes for the change to take effect.

Note: If a time period transition occurs and an MPE device is still updating sessions for the previous period, the MPE device aborts the updates in progress and processes the new transition by updating the sessions based on the time periods to which it transitioned.

Time-of-day triggering must be enabled as part of MPE configuration. For more information, see *Configuring Protocol Options on the Policy Server*.

Chapter 15

Managing Serving Gateways to MCCs/MNCs

Topics:

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

About Mapping Serving Gateways to MCCs/MNCs

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

Creating a Mapping

To create a mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
   The content tree displays the **Serving Gateway/MCC-MNC Mappings** group.
2. Select the **Serving Gateway/MCC-MNC Mappings** group.
   The Serving Gateway/MCC-MNC Mappings Administration page opens in the work area, listing available mappings.
3. On the Serving Gateway/MCC-MNC Mappings Administration page, click **Create Serving Gateway/MCC-MNC Mapping**.
   The New Serving Gateway/MCC-MNC Mapping page opens.
4. Enter the following information:
   a) **Name** (required) — The name assigned to the mapping.
      The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description** — A descriptive phrase.
   c) **MCC-MNC** (required) — The MCC-MNC pair, in the format *mccmnc*; for example, 310012 for Verizon Wireless in the United States.
   d) **Serving Gateway IP Address/Subnet** (required) — The IP address or subnet, in IPv4 or IPv6 format, of a serving gateway.
      To add an address to the mapping list, type it and click **Add**. To remove one or more mappings from the list, select them and click **Delete**.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The mapping is created and stored in the Serving Gateway/MCC-MNC Mappings group.

Modifying a Mapping

To modify a Serving Gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
   The content tree opens.
2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.
   The Serving Gateway/MCC-MNC Mappings Administration page opens, displaying the list of defined mappings.
3. Select the mapping you want to modify.
   Mapping information is displayed.
4. Click **Modify**.
   The Modify Serving Gateway/MCC-MNC Mapping page opens.
5. Modify mapping information as required.
   For a description of the fields contained on this page, see *Creating a Mapping*.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).

The mapping is modified.

Deleting a Mapping

To delete a serving gateway/MCC-MNC mapping:

1. From the **Policy Server** section of the navigation pane, select **Serving Gateway/MCC-MNC Mapping**.
   The content tree opens.
2. From the content tree, select the **Serving Gateway/MCC-MNC Mappings** group.
   The Serving Gateway/MCC-MNC Mappings Administration page opens, displaying the list of defined mappings.
3. Delete the mapping using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the mapping you want to delete.
   - From the content tree, select the mapping and click **Delete**. You are prompted, "Are you sure you want to delete this Serving Gateway/MCC-MNC mapping?"
4. Click **OK** to delete the Serving Gateway/MCC-MNC mapping (or **Cancel** to cancel the request).

The mapping is deleted.

Chapter 16

Managing Monitoring Keys

Topics:

Managing Monitoring Keys describes how to create and manage monitoring keys in the CMP.

About Monitoring Keys

A monitoring key is a unique string that identifies the quota profile to be used by a policy and charging control (PCC) rule and application detection control (ADC) rule for usage tracking. The monitoring key is associated with the quota profile by selecting a policy action that grants usage to a selected number of quota profiles. You configure monitoring keys through the CMP.

The PCC Rule Profile is used to populate the Charging Rule Definition AVP and the ADC Rule definition AVP values in a Diameter message when a new rule is installed. Therefore, the monitoring key to be defined in the PCC Rule Profile is specified in the Monitoring Key AVP, which is contained in the Charging Rule Definition or ADC Rule Definition AVP for that particular rule. The monitoring key is supported for Sd and Release 9 is not needed. When reporting usage to the MPE device, the monitoring key associated with the PCC/ADC Rule is included in a Usage Monitoring AVP, along with the usage accumulated. The usage accumulated is reported for the total volume, uplink volume, or downlink volume.

At the session level, the monitoring key is optional, but is set by the selection of the appropriate policy action. These policy actions include the ability to:

- Disable or re-enable usage tracking for specified monitoring keys
- Request a usage report from the PCEF for specified monitoring keys
- Monitor multiple PCC/ADC rules against the same quota
- Monitor usage for a PCC/ADC rule or session level against multiple quotas such as monthly and daily quotas

  Note: The granted usage sent to the PCEF/TDF will always be the smallest remaining amount of the quotas, and the re-validation time will always be calculated based on the shortest or closest time in the future for the quotas.

- Change a monitoring key for a rule or session level during the middle of a session upon receiving a Credit Control Request (CCR) update message

Creating a Monitoring Key

1. From the **Policy Server** section of the navigation pane, select **Monitoring Key**.
   The content tree displays the Monitoring Key group.
2. Select the **Monitoring Key** group.
   The Monitoring Key Administration page opens in the work area.
3. On the Monitoring Key Administration page, click **Create Monitoring Key**.
   The New Monitoring Key page opens.
4. Enter information as appropriate for the monitoring key:
   a) **Name** (required) — The name you assign to the monitoring key.
      The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description** — Free-form text that identifies the monitoring key.
      Enter up to 250 characters.

c) **Type** (required) — The level assigned to the monitoring key.

Select **PCC_RULE_LEVEL** value (1), **ADC_RULE_LEVEL** value (2), or **SESSION_LEVEL** from the list.

d) **Key** — Specifies unique string from all other monitoring keys.

The key can be up to 255 characters long and must not contain backslashes (\), quotation marks ("), semcolons (;), commas (,), or apostrophes (').

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

   The monitoring key is displayed in the Monitoring Key Administration page.

Once you define monitoring keys, you can select them from the PCC Rule Profile when configuring quota profiles or use them in policy actions in the policy wizard (see *User State Conditions*).

Modifying a Monitoring Key

1. From the **Policy Server** section of the navigation pane, select **Monitoring Key**.
   The Monitoring Key Administration page opens in the work area, listing the defined monitoring keys.
2. On the Monitoring Key Administration page, select the monitoring key you want to modify.
   The Monitoring Key Administration page displays information about the monitoring key.
3. Click **Modify.**
   The Modify Monitoring Key page opens.
4. Modify monitoring key information as required.

   For a description of the fields contained on this page, see *Creating a Monitoring Key*.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The monitoring key definition is modified.

Deleting a Monitoring Key

1. From the **Policy Server** section of the navigation pane, select **Monitoring Key**.
   The Monitoring Key Administration page opens in the work area, listing the defined monitoring keys.
2. Delete the monitoring key using one of the following methods:

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

   You are prompted: "Are you sure you want to delete this Monitoring Key?"
3. Click **OK** (or **Cancel** to cancel the request).

The monitoring key is deleted.

Chapter 17

Managing Third-Party AVPs

Topics:

Managing Third- Party AVPs describes how to create, modify, and delete third-party AVPs in the CMP.

About AVPs

An AVP is used to encapsulate protocol-specific information with usage monitoring supported by the MPE. Diameter messages for example, RAA, CCA, CCR, and RAR, are supported by third-party AVP policy conditions. The supported outgoing messages set or remove third-party AVPs in Diameter.

Note: The Diameter messages listed above are only an example. There are many messages associated with Diameter.

Policy conditions are defined which evaluate the presence of third-party AVPs in Diameter messages or group AVPs during policy execution. The policy condition is checked to ensure the presence of third-partyAVP for incoming Diameter messages and to evaluate predefined values. Custom AVPs are located at the end of a Diameter message or group AVP when defined. For example, the custom defined AVP appears at the end of the message:

```
 Charging-Rule-Install: : <AVP Header: 1001>
*[Charging-Rule-Definition]
*[Charging-Rule-Name]
*[Charging-Rule-Base-Name]
[Bearer-Identifier]
[Rule-Activation-Time]
[Rule-Deactivation-Time]
[Resource-Allocation-Notification]
[Charging-Correlation-Indicator]
*[AVP]
```

A Set or Get SPR user attribute value can be set to the defined third-party AVP in Diameter messages. You can also set or remove defined third-party AVPs during the execution point.

The existence of third-partyAVP can be defined by a unique identifier in the following format:

<NAME>:<VendorId>

For example:

Condition	**where the request AVP NEW_TEST_AVP3:555 value is numerically equal to 2012**
Parameters	The AVP name and vendor ID. In the example above. the vendor ID is 555.
Description	A well defined AVP custom name is referred to if the vendor ID is not specified.
Mode	Wireless

When entering and sending a new third-partyAVP definition to a registered MPE or MRA, the definition must include the AVP name, code, vendor ID, data type, and an optional AVP flag.

The validation of the AVP code, Name, and vendor ID, prohibits a user from overwriting the existing base AVPs.

These AVP actions include the ability to perform the following:

- Routing
- Authentication
- Authorization
- Accounting

Creating an AVP

1. From the **Policy Server** section of the navigation pane, select **Custom AVP Definitions**.
   The content tree displays the Custom AVP Definitions group.
2. Select the **Custom AVP Definitions** group.
   The AVP Definition Administration page opens in the work area.
3. On the AVP Definition Administration page click **Create AVP Definition**.
   The New AVP Definition page opens.
4. Enter information as appropriate for the AVP Definition:
   a) **AVP Name** (required) — The name you assign to the AVP Definition.

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

   b) **Description** — Free-form text that identifies the AVP Definition.

      Enter up to 250 characters.

   c) **AVP Code** (required) — A unique numeric value assigned to the new AVP Definition.
   d) **Vendor Id**— Enter the vendor ID. The default is *0*.
   e) **Protect Flag**— A non-mandatory field which when checked, specifies the protected AVP values.
   f) **May Encrypt Flag**— The AVP is encrypted if the checkbox is specified.
   g) **Vendor Specific Flag**— The AVP is vendor specific if the checkbox is specified.

      Note: This box is checked automatically if the value of the vendor Id is not *0*.

   h) **AVP Type**— The pulldown list is used to select the available data type. You will have the following options:

      - address
      - enumerated
      - float32
      - float64
      - grouped
      - id
      - int32
      - int64
      - ipFilterRule
      - octetString
      - time
      - unit32
      - unit64
      - uri
      - utf8String

   i) **Parent AVP**— If the AVP is a member of a grouped AVP, then the parent AVP must be specified. You will have the following options:

   - ADC-Rule-Definition:10415
   - ADC-Rule-Install:10415

- ADC-Rule-Remove:10415
- ADC-Rule-Report:10415
- AF-Correlation-Information:10415
- Acceptable-Service-Info:10415
- Access-Network-Charging-Identifier-Gx:10415
- Access-Network-Charging-Identifier:10415
- Access-Network-Physical-Access-ID:10415
- Allocation-Retention-Priority:10415
- Application-Detection-Information:10415
- CC-Money
- Charging-Information:10415
- Charging-Rule-Definition-3GPP2:5535
- Charging-Rule-Definition:10415
- Charging-Rule-Event-Cisco:9
- Charging-Rule-Event-Trigger-Cisco:9
- Charging-Rule-Install-3GPP2:5535
- Charging-Rule-Install:10415
- Charging-Rule-Remove:10415
- Charging-Rule-Report-3GPP2:5535
- Charging-Rule-Report:10415
- Codec-Data-Tmp:10415
- Codec-Data:10415
- Cost-Information
- Default-EPS-Bearer-Qos:10415
- E2E-Sequence
- Envelope:10415
- Event-Report-Indication:10415
- Explicit-Route-Record:21274
- Explicit-Route:21274
- Failed-AVP
- Final-Unit-Indication
- Flow-Description-Info:5535
- Flow-Description:10415
- Flow-Grouping:10415
- Flow-Info:5535
- Flow-Information:10415
- Flow:10415
- G-S-U-Pool-Reference
- Granted-Qos:5535
- Granted-Service-Unit
- Juniper-Discovery-Descriptor:2636
- Juniper-Provisioning-Descriptor:2636
- LI-Indicator-Gx:12951
- LI-TargetMFAddr:12951
- Media-Component-Description:10415
- Media-Sub-Component:10415

- Multiple-Services-Credit-Control
- Offline-Charging:10415
- PCEF-Forwarding-Info:971
- PCEF-Info:971
- PS-Furnish-Charging-Information:10415
- PS-information:10415
- Qos-Information-3GPP2:5535
- Qos-Information:10415
- Qos-Rule-Install:10415
- Qos-Rule-Definition:10415
- Qos-Rule-Remove:10415
- Qos-Rule-Report:10415
- Reachable-Peer:21274
- Redirect-Information:10415
- Redirect-Server
- Requested-Qos:5535
- Requested-Service-Unit
- Service-Information:10415
- Service-Parameter-Info
- Siemens-DL-SDP-Data:4329
- Siemens-UL-SDP-Data:4329
- Subscription Id
- Subscription-Id-3GPP:10415
- Supported-Features:10415
- TDF-Information:10415
- TFT-Packet-Filter-Information:10415
- TMO-Redirect-Server-29168
- Time-Quota-Mechanism:10415
- Trigger:10415
- Tunnel-Header-Filter:10415
- Unit-Value
- Usage-Monitoring-Control:21274
- Usage-Monitoring-Information:10415
- Used-Service-Unit
- User-Equipment-Info
- User-Location-Info-3GPP:10415
- VZW-Access-Network-Physical-Access-ID:12951
- Vendor-Specific-Application-Id

5. When you finish, click **Save** (or **Cancel** to discard your changes).
   The custom AVP definition is displayed in the AVP Definition Administration page.

Modifying an AVP

1. From the **Policy Server** section of the navigation pane, select **Custom AVP Definitions**.
   The AVP Definition Administration page opens in the work area, listing the defined AVPs.
2. On the AVP Definition Administration page, select the AVP you want to modify.
   The AVP Definition Administration page displays information about the AVP.
3. Click **Modify.**
   The Modify AVP Definition page opens.
4. Modify AVP information as required.

   For a description of the fields contained on this page, see *Creating an AVP*.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The AVP definition is modified.

Deleting an AVP

1. From the **Policy Server** section of the navigation pane, select **Custom AVP Definitions**.
   The AVP Definition Administration page opens in the work area, listing the defined monitoring keys.
2. Delete the AVP using one of the following methods:
   - From the work area, click the **Delete** icon, located to the right of the AVP Name you wish to delete.
   - From the content tree, select the **AVP** and click **Delete**.

   You are prompted: "Are you sure you want to delete this AVP?"
3. Click **OK** (or **Cancel** to cancel the request).

The AVP is deleted.

Chapter 18

Managing Multi-Protocol Routing Agents

Topics:

Managing Multi-Protocol Routing Agents describes how to define and manage Multi-Protocol Routing Agents (MRAs) in the CMP.

Note: For information on operating MRA devices, refer to the *Multi-Protocol Routing Agent User's Guide*.

Configuring the CMP to Manage an MRA Cluster

The Multi-Protocol Routing Agent (MRA) is a standalone entity that supports Multimedia Policy Engine (MPE) devices. The CMP 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 Tekelec Technical Support. Setting modes inappropriately could 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 Tekelec Technical Support for information on this button.

   The Mode Settings page opens.
3. At the bottom of the page, select **Manage MRAs**.
4. Click **OK**.
   The browser page closes and you are automatically logged out.
5. Refresh the browser page.
   The Welcome admin page is displayed.

You are now ready to define an MRA cluster profile, specify network settings for the MRA cluster, and associate MPE devices with the MRA cluster.

Defining an MRA Cluster Profile

You must define a profile for each MRA cluster you are managing. To define an MRA cluster profile:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the ALL group.
   The MRA Administration page opens in the work area.
3. On the MRA Administration page, click **Create Multi-protocol Routing Agent**.
   The New MRA page opens.
4. Enter information as appropriate for the MRA cluster:
   a) **Associated Cluster** (required) — Select the MRA cluster from the pulldown list.
   b) **Name** (required) — Enter a name for the MRA cluster.

      Enter up to 255 characters. The name can contain any alphanumeric characters except quotation marks (") and commas (,).
   c) **Description/Location** (optional) — Free-form text.

      Enter up to 255 characters.

d) **Secure Connection** — Select to enable a secure HTTP (HTTPs) connection 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** (or **Cancel** to discard your changes).
   The MRA cluster profile is displayed in the MRA Administration page.

The MRA cluster profile is defined.

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

The MRA cluster profile settings are modified.

Working with MRA Groups

MRA groups let you organize MRA cluster profiles into groups. You can create, rename, and delete MRA groups, and add and remove MRA cluster profiles from groups.

Creating an MRA Group

To create an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The MRA Administration page opens in the work area.
3. On the MRA Administration page, click **Create Group**.
   The Create Group page opens.
4. Enter the name of the new MRA group.
5. When you finish, click **Save** (or **Cancel** to abandon your request).

The new group appears in the content tree.

The MRA group is created.

Adding an MRA Cluster Profile to an MRA Group

Once an MRA group is created, you can add MRA cluster profiles to it. To add an MRA cluster profile to an MRA group:

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the desired MRA group.
   The MRA Administration page opens in the work area, displaying the contents of the selected MRA group.
3. On the MRA Administration page, click **Add Multi-protocol Routing Agent**.
   The Add Multi-protocol Routing Agent page opens.
4. Select the MRA cluster profile you want to add; use the Ctrl or Shift keys to select multiple MRA cluster profiles.
5. When you finish, click **Save** (or **Cancel** to abandon the request).

The MRA cluster profile is added to the MRA group.

Deleting an MRA Cluster Profile from an MRA Group

Removing an MRA cluster profile from an MRA group does not delete the MRA cluster profile from the ALL group, so it can be used again if needed. Removing an MRA cluster profile from the ALL group removes it from all other groups.

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

1. From the **MRA** section of the navigation pane, select **Configuration**.
   The content tree displays a list of MRA groups; the initial group is **ALL**.
2. From the content tree, select the desired MRA group.
   The MRA Administration page opens in the work area, displaying the contents of the selected MRA group.
3. Remove the desired 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 desired MRA group or subgroup from the content tree.
   The contents of the selected MRA group are displayed.
3. Click **Delete**.
   You are prompted: "Are you sure you want to delete this Group?"
4. Click **OK** to delete the selected group (or **Cancel** to abandon the request).

The MRA group is deleted.

Enabling Stateless Routing

To enable stateless routing, from within the MRA creation page or within the System Tab page for the MRA, select **Stateless Routing** (*Figure 18: Enabling Stateless Routing* shows an example).

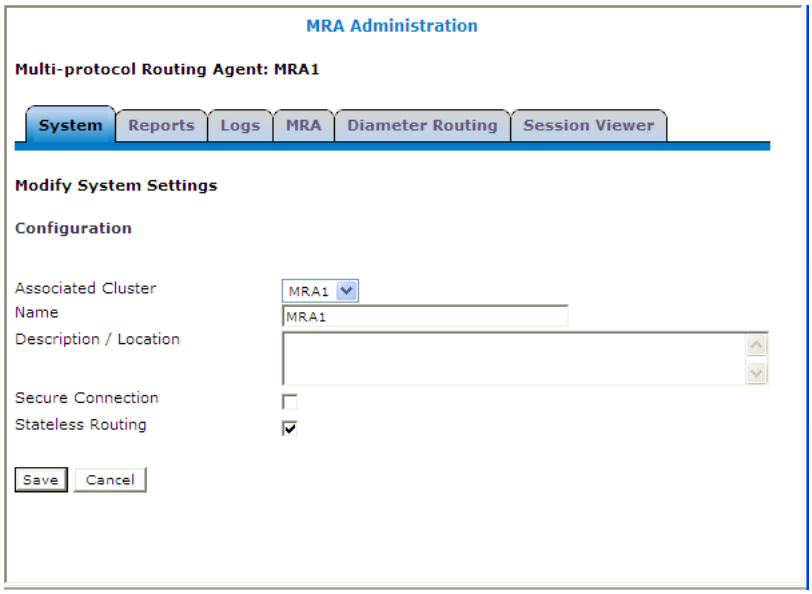


Figure 18: Enabling Stateless Routing

Chapter 19

Managing Subscriber Profile Repositories

Topics:

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

Note: For information on operating MRA devices, refer to the *Multi-Protocol Routing Agent User's Guide*.

About Subscriber Profile Repositories

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

An SPR can be deployed in environments where the Multimedia Policy Engine (MPE) 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 Tekelec SPR 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 either a Tekelec proprietary RESTful API interface or a Diameter Sh interface.

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

For detailed information on the SPR, see the Tekelec Subscriber Data Management (SDM) documentation.

Configuring the CMP 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.

Note: The procedures that follow assume that you have installed the SPR software on a device. If you have not, do so now.

To reconfigure the CMP operating mode, complete the following:

CAUTION

CAUTION: CMP operating modes should only be set in consultation with Tekelec Technical Support. Setting modes inappropriately could result in the loss of network element connectivity, policy function, OM statistical data, and cluster redundancy.

1. From the **Help** section of the navigation pane, select **About**.
   The About page opens, displaying the CMP software version number.
2. Click the **Mode** button.
   Consult with Tekelec Technical Support for information on this button.
   The Mode Settings page opens.

3. In the Mode section, select the mode **Diameter 3GPP**, **Diameter 3GPP2**, or **PCC Extensions**, as appropriate.
4. At the bottom of the page, select **Manage SPR Subscriber Data**.
5. Click **OK**.
   The browser page closes and you are automatically logged out.
6. Refresh the browser page.
   The Welcome admin page is displayed.

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

Configuring the SPR Connection

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

To configure the SPR connection:

1. From the **SPR** section of the navigation pane, select **Configuration**.
   The SPR Connection Configuration page opens in the work area, displaying connection information.
2. On the SPR Connection Configuration page, click **Modify**.
   The Configuration page opens.
3. Enter information as appropriate for the SPR system:
   a) **SPR Operation Mode** (required) — Select from the pulldown list:
      - **Diameter Sh Protocol**
      - **SDM RESTful API** (the default)

      This choice of operation mode applies to all subscriber profile management on this CMP system. However, you can switch back and forth between these two settings if necessary. Depending on the mode selected, additional required fields appear.
   b) **Diameter Identity** (Diameter Sh Protocol mode) — Enter the fully qualified domain name of the CMP system (for example, `cmp10-24.galactel.com`) as it will be seen by the SPR system.
   c) **Diameter Realm** (Diameter Sh Protocol mode) — Enter the realm in which the SPR system is located (for example, `galactel.com`).
   d) **Remote Port** (SDM RESTful API mode) — Enter the port (a number from 1 to 65535) to listen on for SPR traffic.

      The default is 8787.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

The SPR connection is configured.

Modifying the SPR Connection

To modify the SPR connection:

1. From the **SPR** section of the navigation pane, select **Configuration**.
   The SPR Connection Configuration page opens in the work area, displaying connection information.
2. On the SPR Connection Configuration page, click **Modify**.
   The Configuration page opens.
3. Modify the configuration information as necessary. See *Configuring the SPR Connection* for information on the fields on this page.
4. When you finish, click **Save** (or **Cancel** to discard your changes).

The SPR connection configuration is modified.

Finding a Subscriber Profile

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

To find a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Select the **Data Source Primary Diameter Identity**.
   This is the list of defined SPR devices. You can select any SPR device configured for the Policy Management network. Devices are identified by both their primary identity and MPE device name.
3. Select the **Key Type**:
   - **E.164 (MSISDN)** (the default) — search by Mobile Station International Subscriber Directory Number. This is a number of up to 15 digits.
   - **IMSI** — search by International Mobile Subscriber Identity. This is a number of up to 15 digits.
   - **NAI** — search by Network Access Identifier.
   - **Pool ID** — search by quota pool identifier.
4. **Key String** — enter a search string in the format appropriate for the selected key type.
   The string must match exactly; partial or wildcard searching is not supported.
5. Click **Search**.
   The Subscriber Profile page opens, displaying information about the subscriber.

   Note: If no matching subscriber profile is found, the page displays the message "No matching user is found."
6. When you finish, click **Back to Search Page**.
   The Subscriber Profile Administration page opens.

Creating a Subscriber Profile

If an SPR 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.

   Note: If the SPR is configured as an Sh data source, this button is grayed out, and you cannot create a subscriber profile.

3. Enter the following information:
   a) Select the **Data Source Primary Diameter Identity**.
      You can select any SPR device configured for the Policy Management network.
   b) In the **Key Fields** section, enter one format:

      - **NAI** — Network Access Identifier. You must enter a valid user name, optionally followed by a valid realm name. A valid user name consists of the characters &*+0-9?a-z_A-Z{}!#$%'^/=`|~-, optionally separated by a period (.). A valid realm name consists of the characters 0-9a-zA-Z- separated by one or more period (.), but the minus sign (-) cannot be first, last, or adjacent to a period.
      - **E.164 (MSISDN)** — Mobile Station International Subscriber Directory Number. Enter up to 15 Unicode digits, optionally preceded by a plus sign (+).
      - **IMSI** — International Mobile Subscriber Identity. Enter up to 15 Unicode digits.

   c) Optionally, in the **Subscriber Information** section, enter the following:

      - **Account ID** — Free-form string that can identify the account for the subscriber. You can enter up to 255 characters.
      - **Billing Day** — The day of the month on which the subscriber's associated quota is reset. Enter a number between 0 and 31. If you enter 0 or leave this field blank, then the default global value configured for this MPE device is used instead.
      - **Tier** — The subscriber's tier. Enter a tier name defined in the CMP system; or, if you click **Manage**, a window opens from which you can select a tier name. In order to add a tier, you must enter the tier name prior to clicking **Manage**. See *Managing Subscribers* for information on tiers.
      - **Entitlements** — The subscriber's entitlement(s). Enter the entitlement name(s); or, if you click **Manage**, a window opens from which you can enter or select entitlement names defined in the CMP system.

        Note: Entitlements are defined external to the CMP system.

      - **Custom** — Free-form strings representing custom subscriber fields. You can enter up to 255 characters per field. By default, five fields are available, but if the subscriber profile has more than five custom fields defined, the page displays them. Click **Add** to create additional fields as needed.

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

The subscriber profile is defined.

Modifying a Subscriber Profile

To modify a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click **Modify**.
   The Subscriber Profile Administration page opens.
4. Modify subscriber profile information as required.
   For a description of the fields contained on this page, see *Creating a Subscriber Profile*.
5. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The page displays the message "Subscriber profile updated successfully."

The subscriber profile is modified.

Deleting a Subscriber Profile

Using the RESTful API operation mode, you can delete a subscriber profile. See *Configuring the SPR Connection* for information on setting the operation mode.

To delete a subscriber profile:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to delete.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click **Delete**.
   You are prompted, “Are you sure you want to delete this subscriber profile?”
4. Click **OK** to delete the subscriber profile (or **Cancel** to cancel the request).
   The page displays the message "Subscriber profile successfully deleted."

The subscriber profile is deleted.

Viewing Subscriber Entity States

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

To view the entity states associated with a subscriber:

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

2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Click the State tab.
   Entity state information is displayed.
4. When you finish, click **Back to Search Page**.

You have viewed the subscriber entity states.

Creating a Subscriber Entity State Property

To create a subscriber entity state property:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the State tab.
   Entity state information is displayed.
4. Click **Create**.
   The Create Property page opens.
5. Enter the following information:
   a) **Name** — The name assigned to the property.
      The name cannot be blank and must be unique within this list of properties.
   b) **Value** — The property value.
      The value cannot be blank.
6. Click **Save** (or **Cancel** to discard your changes).
   The profile information page opens, and displays the message "Properties created successfully."
7. To create additional properties, repeat steps 4 through 6.
   If you exceed 100 states, you are prompted whether you wish to add more; click **Yes** to continue, or **No** to stop.
8. When you finish, click **Back to Search Page**.
   The page displays the message "Properties created successfully."

The subscriber entity state property is defined.

Modifying a Subscriber Entity State Property

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

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

2. Find the subscriber profile you want to modify.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the State tab.
   Entity state information is displayed.
4. In the list of entity state properties, click on the property you want to modify.
   The Modify Property page opens.
5. Modify the property value as required.
   The value cannot be blank.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The page displays the message "Properties updated successfully."

The subscriber entity state property value is modified.

Deleting a Subscriber Entity State Property

To delete a subscriber entity state property:

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

The subscriber entity state properties are deleted.

Viewing Subscriber Quota Information

To view the quotas associated with a subscriber:

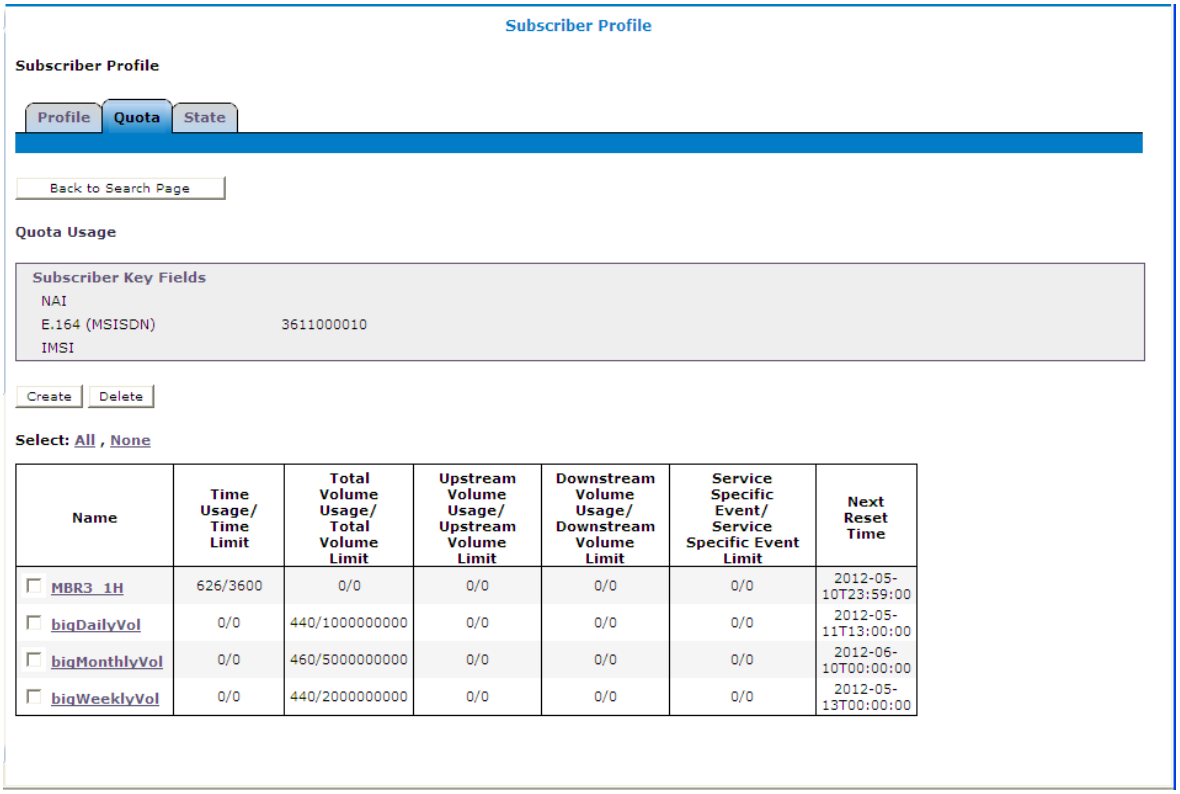
1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)

3. Select the Quota tab.
   The Subscriber Profile Quota Usage page is displayed. (*Figure 19: Subscriber Profile Quota Usage Page* shows an example.) 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.

4. When you finish, click **Back to Search Page**.

You have viewed the subscriber quota information.



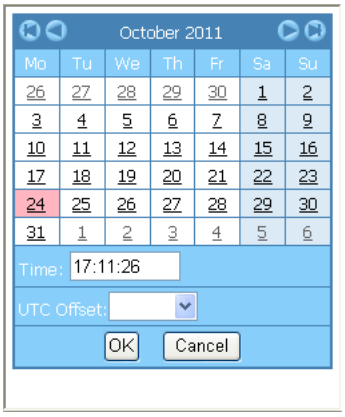
Name	Time Usage/ Time Limit	Total Volume Usage/ Total Volume Limit	Upstream Volume Usage/ Upstream Volume Limit	Downstream Volume Usage/ Downstream Volume Limit	Service Specific Event/ Service Specific Event Limit	Next Reset Time
MBR3_1H	626/3600	0/0	0/0	0/0	0/0	2012-05-10T23:59:00
bigDailyVol	0/0	440/1000000000	0/0	0/0	0/0	2012-05-11T13:00:00
bigMonthlyVol	0/0	460/5000000000	0/0	0/0	0/0	2012-06-10T00:00:00
bigWeeklyVol	0/0	440/2000000000	0/0	0/0	0/0	2012-05-13T00:00:00

Figure 19: Subscriber Profile Quota Usage Page

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 Subscriber Profile Quota Usage page is displayed.
4. Click **Create**.
   The Quota Usage page opens. If you exceed 10 quotas, you are prompted whether you wish to add more; click **Yes** to continue, or **No** to stop.
5. Enter the following information:
   a) **Name** (required) — Select the name of a quota defined in the CMP system from the pulldown list. You cannot add the same quota twice for a subscriber. See *Managing Quotas* for information on creating quotas.
   b) **Time (seconds)** — Enter a value, in seconds, to track time consumption.
   The valid range is -2^{63} to $2^{63} - 1$ (that is, a 64-bit value).
   c) **Total Volume (bytes)** — Enter a value, in bytes, to track bandwidth volume consumption.
   The valid range is -2^{63} to $2^{63} - 1$ (that is, a 64-bit value).
   d) **Upstream Volume (bytes)** — Enter a value, in bytes, to track upstream bandwidth volume consumption.
   The valid range is -2^{63} to $2^{63} - 1$ (that is, a 64-bit value).
   e) **Downstream Volume (bytes)** — Enter a value, in bytes, to track downstream bandwidth volume consumption.
   The valid range is -2^{63} to $2^{63} - 1$ (that is, a 64-bit value).
   f) **Service Specific Event** — Enter a value representing service-specific resource consumption.
   The valid range is -2^{63} to $2^{63} - 1$ (that is, a 64-bit value).
   g) **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 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** (or **Cancel** to discard the date/time).



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

The subscriber quota is defined.

Modifying a Subscriber Quota Category

To modify a subscriber quota category:

1. From the **SPR** section of the navigation pane, select **Profile Data**.
   The Subscriber Profile Administration page opens.
2. Find the subscriber profile you want to view.
   Profile information is displayed. (See *Finding a Subscriber Profile* for information on finding a subscriber profile.)
3. Select the Quota tab.
   The Subscriber Profile Quota Usage page is displayed.
4. Click the name of the quota you want to modify.
   The Quota Usage page opens, displaying information about the quota.
5. Modify subscriber quota information as required.
   For a description of the fields contained on this page, see *Adding a Subscriber Quota Category*.
6. When you finish, click **Save** (or **Cancel** to abandon your changes).
   The page displays the message "Quota updated successfully."

The subscriber quota category is modified.

Deleting a Subscriber Quota Category

To delete a subscriber quota category:

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

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

3. Select the Quota tab.
   Entity quota information is displayed.
4. In the list of quotas, use the check boxes to select the quota or quotas you want to delete.
   To select all quotas, click **All**. To deselect all quotas, click **None**.
5. Click **Delete**.
   You are prompted, "Delete selected properties?"
6. Click **OK** (or **Cancel** to abandon your request).
   The quota or quotas are removed from the list, and the page displays the message "Quota deleted successfully."

The subscriber quota categories are deleted.

Chapter 20

Understanding and Creating Policy Rules

Topics:

Policy rules dynamically control how the Multimedia Policy Engine (MPE) processes protocol messages as they pass through the MPE device. Using these rules, you can define how and when network resources are utilized by subscribers. For example, when the MPE device receives a request to establish a session with a certain Quality of Service (QoS) level, you can use a policy rule to approve the request as is, to reject the request, or to make changes in the request before it is forwarded to the intended destination network element.

Structure and Evaluation of Policy Rules

The following topics provide an overview of how policy rules are structured and evaluated.

Note: The conditions, actions, and parameters available for your use in creating policy rules depend on the mode in which the CMP is operating.

Structure of Policy Rules

Understanding how a policy rule is structured is helpful in understanding other policy management concepts. A policy rule is defined as a simple If-Then construct, consisting of a set of conditions that the MPE device compares to protocol messages, and a set of actions that are executed (or not executed) when the conditions match. Many conditions can be tested for existence or non-existence (by selecting the logical operator **NOT** or the policy condition operator **is** or **is not**).

Policy Parameters

When you define a policy rule, you select from a list of available conditions and actions. Most of the conditions and actions are parameterized (that is, they contain placeholders that may be replaced with specific values to allow you to customize them as needed).

For example, consider the following policy rule, which has one condition and two actions:

```
where the device will be handling greater than 100 upstream reserved flows

apply profile Default Downstream Profile to request
continue processing message
```

The condition, **where the device will be handling**..., allows the following parameters to be specified:

- An operator (**greater than**)
- A value (**100**)
- The flow direction (**upstream**)
- The bandwidth reservation type (**reserved**)

The first action, **apply profile**..., specifies a single parameter that is the name of a traffic profile to be applied to the request. The second action, **continue processing message**, instructs the MPE device to evaluate the remaining rules within the policy rules list (as opposed to immediately accepting or rejecting the request). The conditions and actions that are available for writing policies are discussed later in this section.

Policy Logical Operators

The policy wizard supports creation of rules using an explicit **AND** logical operator that contains a set of conditions. An AND operator must include at least two conditions. The actions are taken if all conditions are evaluated as true. For example, you can use an AND operator two define two conditions as follows:

```
And
     where the request is re-authorizing an existing session
     where the enforcement session is a DPI enforcement session
.
```

```
.
.
```

The policy wizard supports creation of rules using an **OR** logical operator that contains a set of conditions. An OR operator must include at least two conditions. The actions are taken if any condition is evaluated as true. For example, you can define the following set of conditions using an OR operator:

```
Or
     where the request is creating a new session
     where the session is an enforcement session
     where the APN matches one of imode.g1t2
     where the subscriber profile data is not available
.
.
.
```

The policy wizard supports creation of rules using a **NOT** logical operator that contains a single condition. The actions are taken if the condition is evaluated as false. For example, you can define the following using a NOT operator:

```
Not
     where today is a weekend day using CONFIGURED LOCAL TIME
.
.
.
```

Note: Many conditions also include optional **is** and **is not** parameters. These parameters are functionally equivalent to (that is, synonymous with) using the **NOT** operator, and you are free to use or mix **NOT** with **is** and **is not** as you prefer.

Finally, the policy wizard supports creation of rules using combinations of logical operators. You can nest operators. For example, you can define the following rule:

```
Or
     And
          Not
               where the service info status is one of FINAL_SERVICE_INFORMATION
          where the session is an enforcement session
     where the session is an application session
     Not
          where the session is an application session

evaluate policy 5555
reject message
```

The policy wizard validates condition trees.

Parent and Reference Policies

As a result of evaluating conditions, a policy can execute another policy. A policy that calls another policy is called a parent policy, and a policy executed by another policy is called a reference policy. A policy can be both a parent policy and a reference policy. Additionally, you can group policies, and a parent policy can execute all the policies in the group.

Note: Do not nest policies more than five levels deep.

Evaluating Policy Rules

To write policy rules, it is important to understand how they are evaluated by the Policy Rules Engine contained within the MPE device, and how the engine fits into the protocol message processing within the MPE device.

If you look at the policy conditions that are available, you will see that many are not protocol specific. Although you can write protocol-specific policy rules, the Policy Rules Engine itself does not have any protocol knowledge. Instead, it deals with a set of abstractions that are mapped to the underlying protocol messages that are being processed. This allows the same policy rules to be used across multiple protocols.

When the MPE device receives a protocol message, it performs the initial processing of that message and then determines whether or not the message should be processed by the Policy Rules Engine. Generally, protocol messages that are either requesting bandwidth or modifying previous requests for bandwidth are processed by the Policy Rules Engine. Most other protocol messages are not. For example, a protocol message that releases bandwidth is typically not processed by the Policy Rules Engine because there is no reason to prevent or modify that action.

Once a message is identified as a candidate for the policy rules, the MPE device attempts to associate as much information with the request as possible. For example:

- Which network elements will be impacted if the request is allowed to proceed?
- Which subscriber is associated with the request? What services is that subscriber entitled to?
- Which application is associated with the message?
- What time zone is the user equipment located in?

The reason for collecting this information is to make it available to the policy rules. The information that can be associated varies and depends on a number of factors, including:

- The protocol in question and how much information is provided in the protocol message
- The amount of network topology information that has been provisioned into the MPE device
- Whether there are other protocol sessions that can be associated with this message
- Whether there are external data sources configured that the MPE device can use to associate information with the message

When the process of associating information with the request is complete, the MPE device analyzes the information and maps it into several important abstractions that are central to the functioning of the Policy Rules Engine:

1. A list of network devices that the request affects. A network device is any network element, any logical or physical sub-component of a network element, or any other network equipment.
2. A list of flows associated with the request. A flow is a logical representation of a QoS enforcement point that is used for a specific purpose (typically in a single direction, either upstream or downstream). A flow is usually characterized by a collection of bandwidth parameters. Different protocols can have a different number of flows associated with a message. For example, DQoS messages have one or two flows per request (for each direction).
3. A list of policies associated with the request. This includes policy groups and reference policies called by the parent policy.

After constructing these lists, the Policy Rules Engine applies the policy rules according to the following algorithm:

```
For each network device:
```

```
   For each flow that is being created or modified:
      For each policy that is being evaluated:
         Evaluate all policy rules
      End
   End
End
```

A "device" is any device that creates a Gx session, such as a PGW or GGSN; the enforcement device associated with with the corresponding Gx IP-CAN session; or any device that creates a Gxx session, such as an HSGW.

It should be clear from this algorithm that a single message can result in multiple policies being evaluated, and a policy rule being evaluated multiple times. This is important to understand to ensure that the policy rules you write operate in the way you intended.

By using parent policies, reference policies, and policy groups, you can control the order of policy execution. For example, assume there are four policies: two parent policies, $policy_1$ and $policy_4$, and two reference policies, $policy_2$ and $policy_3$ that are in a policy group, $group_1$. The hierarchy is as follows:

```
policy1
   policy2
   policy3
policy4
```

The order of execution can vary, depending on how each policy evaluates and what actions each contains:

- The normal order of execution would be $policy_1 > policy_2 > policy_3 > policy_4$.
- If the conditions in $policy_1$ evaluate to false, the order of execution would be $policy_1 > policy_4$.
- if $policy_2$ includes the mandatory action "break from policy level," the order of execution would be $policy_1 > policy_2 > policy_4$.

If the optional 3GPP-MS-TimeZone AVP is available over the Gx protocol from a PCEF, the MPE device can compute the local time for user equipment, even if the user enters a different time zone or the time offset changes because of Daylight Savings Time.

Note: Policies created using a more recent version of the CMP software may not evaluate and execute as intended on an MPE device running an older version of the MPE software. To ensure that policies are evaluated and executed as intended, update all systems to the same version of the software.

Activating and Deactivating Policy Rules

Rules can be activated and deactivated at specific times by selecting actions that are time-based. The methods by which activation/deactivation times can be defined are:

- **Time Period** — Uses pre-defined time period. At least one time period must be defined to use this option.
- **Policy Table field** — Uses time-related field from a policy table. At least one policy table must be defined, at least one time-related field must be specified in that table, and that table must be selected during the rule definition process to use this option.
- **Absolute time** — Uses exact time, or a combination of the time and date, to define rule activation/deactivation. If only a time is specified, the begin/end dates are calculated as the minimum future dates for those times.
- **Relative time** — Uses the number of hours, minutes, or seconds from the current time to start/end. For example, the value "5" with units of hours would state that a rule should activate (or deactivate)

5 hours after this policy condition is processed by the MPE device. Expressions may include policy variables.

Note: If an activation time is not specified, a rule becomes active immediately. If a deactivation time is not specified (or it is in the past), a rule never deactivates.

CAUTION

CAUTION: If all rules defined in a system have a deactivation time specified, all rules for the session on a PCEF system can become deactivated. To prevent this from occurring, the session on the PCEF is set to revalidated 1 to 30 minutes before the last active rule deactivates.

Using Reference Policies

Multiple policies that share the same conditions can be simplified by including the common conditions in a parent policy and any unique conditions in reference policies. During execution, the common conditions are only evaluated once.

For example, consider the following policies, which apply tiers to session requests. Each policy uses the same conditions, and the Policy Rules Engine evaluates the same conditions up to three times:

```
Bronze Policy
where the request is creating a new session
   and where the flow is an application flow
   and where the AF-Application-ID matches one of voip
   and where the tier is one of Bronze
apply bronze to request
accept message
```

```
Silver Policy
where the request is creating a new session
   and where the flow is an application flow
   and where the AF-Application-ID matches one of voip
   and where the tier is one of Silver
apply silver to request
accept message
```

```
Gold Policy
where the request is creating a new session
   and where the flow is an application flow
   and where the AF-Application-ID matches one of voip
   and where the tier is one of Gold
apply gold to request
accept message
```

Using reference policies in a policy group, the same results can be obtained with the following policies:

```
where the request is creating a new session
   and where the flow is an application flow
   and where the AF-Application-ID matches one of voip
evaluate policy group Tier Policies
```

```
   Bronze Policy
   where the tier is one of Bronze
   apply bronze to request
   accept message
```

```
   Silver Policy
   where the tier is one of Silver
   apply silver to request
   accept message
```

```
   Gold Policy
   where the tier is one of Gold
```

```
   apply gold to request
   accept message
```

Creating a New Policy

Policy rules are created and modified using the policy wizard in the CMP. Once created or modified, the rule is stored in the policy library. The policy wizard guides you step by step to creating a new policy rule. The wizard displays only the options available at each step.

The following procedure describes how to create a new policy rule, using this policy as an example:

```
And
     where the request is creating a new session
     where the session is an enforcement session
     where the APN matches one of imode.g1t2
     where the subscriber profile data is not available
set gg to `op`
reject message
```

To create a new policy rule:

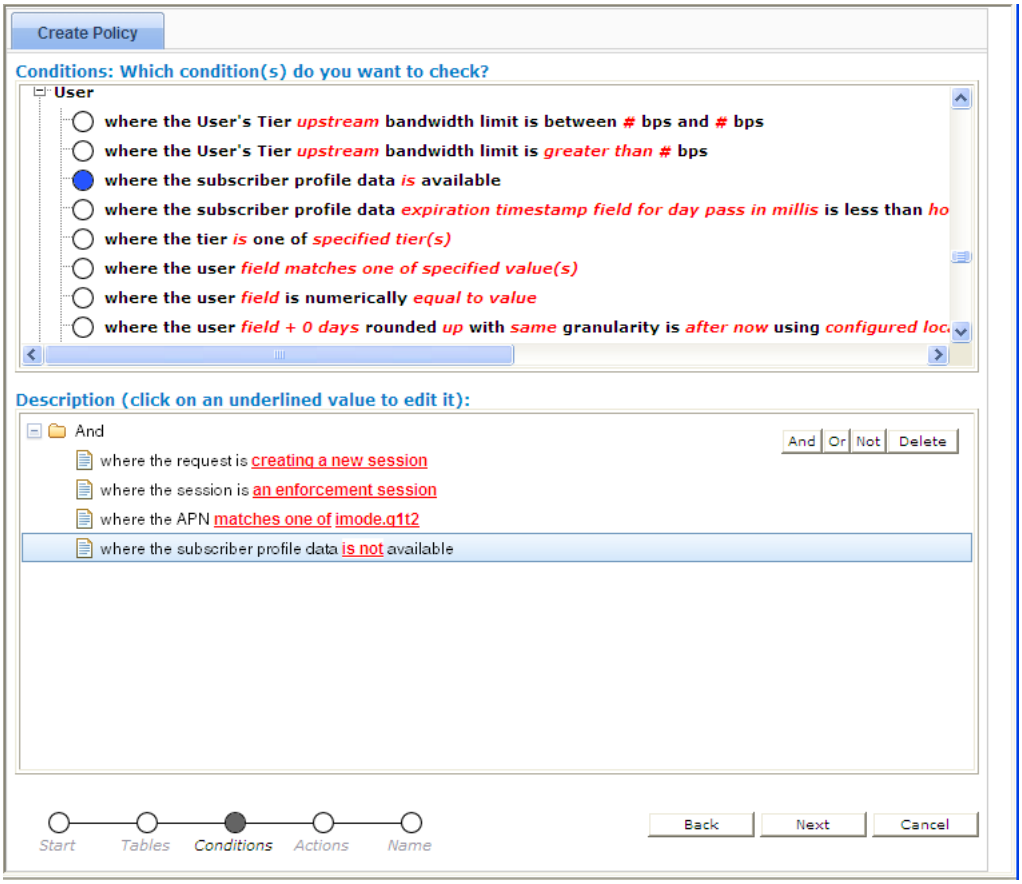
1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
   The content tree displays a list of policy library groups; the default is **ALL**.
2. From the content tree, select the **ALL** group.
   The Policy Administration page opens in the work area.
3. On the Policy Administration page, click **Create Policy**.
   The Create Policy page opens.
4. Select a starting point for the new policy:
   - **Blank** — The policy rule is created from the beginning, without any attributes being pre-defined.
   - **Use Template** — The policy rule is created based on a user-defined template that may have policy parameters pre-defined. This template can be modified as needed.
   - **Copy Existing Policy** — The policy rule is created based on an existing policy rule, which you modify as needed.
5. Click **Next** (or **Cancel** to close the wizard without saving the policy).
   The Tables page opens.
6. Specify the table(s) you want to use in the policy.
   If no tables are associated with the policy, click **Next**.
   - To specify multiple tables, click the selection icon ( ) multiple times
   - To move a table so that it is evaluated earlier in the rule, click the up icon ( )
   - To move a table so that it is evaluated later in the rule, click the down icon ( )
   - To delete a table, click the delete icon ( )
7. When you finish defining tables, click **Next** (or **Cancel** to close the wizard without saving the policy).
   The Conditions page opens.
8. Select the desired policy conditions.
   As a condition is selected, it appears in the Description area at the bottom of the page.

You can select multiple conditions, enter multiple instances of each condition, change the order of conditions, group conditions logically, or remove conditions:

- To enter multiple instances of a condition, click the selection icon ( ) in the Condition window multiple times.
- To combine a logical group of conditions, click **And** or **Or**, located in the upper right corner of the Description window, and drag the conditions into the container that appears (represented by a folder icon). You can toggle a container between **And** and **Or** by double-clicking on the folder.
- To change a condition's order of evaluation or include it within a logical container, drag and drop the condition within the Description window. You cannot drop a container onto itself or one of its sub-containers.
- To negate a condition, change the **is** parameter if present, or click **Not**, located in the upper right corner of the Description window, and drag the condition into the container that appears (represented by a folder icon).
- To delete a condition or container from the rule, select it and click **Delete**. You are prompted, "The focused item and all its children will be deleted. Continue?" Click **OK** (or **Cancel** to keep the condition or container).

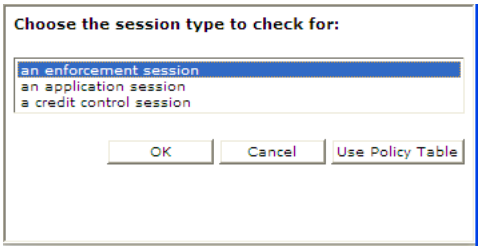
Tip: To add conditions directly to an existing container, select the container first.

For example:

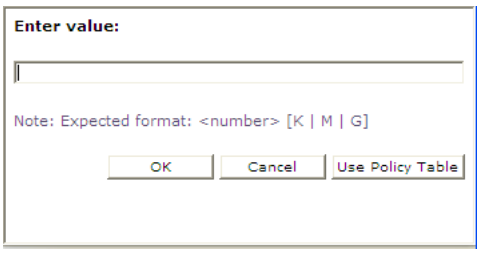


9. If a policy condition includes a parameter that requires further input, it displays red underlined text in the Description area. To provide the input, click the red underlined text; a popup window opens, from which you can do one of the following:

   - Select one or more options; for example:



   - Enter a value (such as a traffic bit rate or percentage); for example:

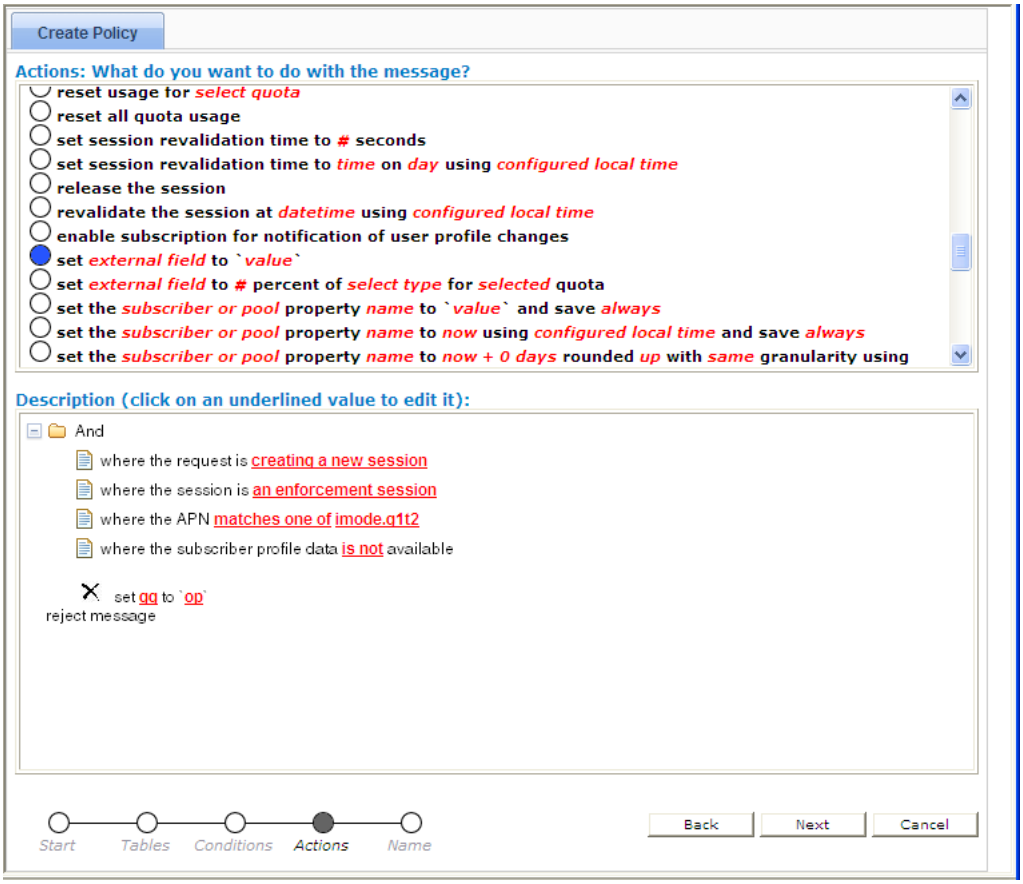


   When you finish, click **OK** (or **Cancel** to discard your changes). The popup window closes and the input is added to the policy condition.

10. When you finish defining policy conditions, click **Next** (or **Cancel** to close the wizard without saving the policy).
    The Actions page opens.

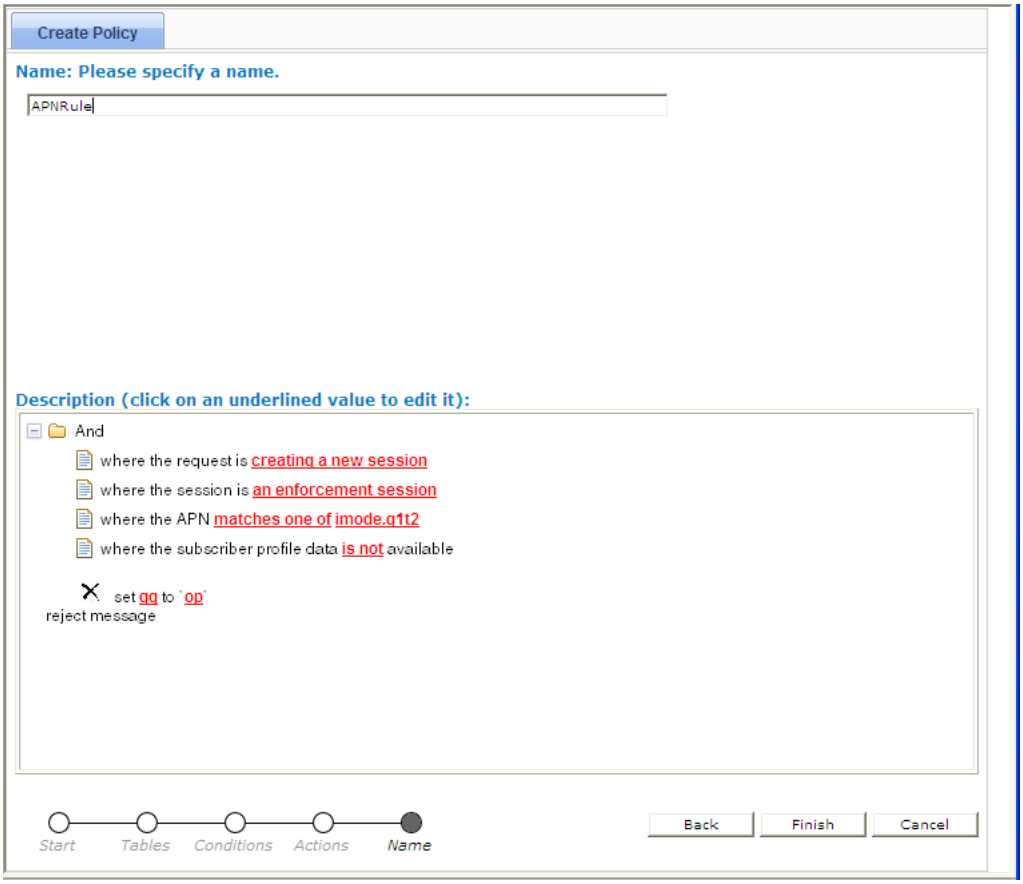
11. Select the required action and any optional actions that the MPE device should execute if the policy request matches the defined conditions of the policy rule.

    For example:



- To enter multiple instances of an action, click the selection icon ( ) multiple times
- To move an action so that it is evaluated earlier in the rule, click the up icon ( )
- To move an action so that it is evaluated later in the rule, click the down icon ( )
- To delete an action from the rule, click the delete icon ( )

12. When you finish, click **Next** (or **Cancel** to close the wizard without saving the policy). The Name page opens.
13. Assign a unique name (where uniqueness is not case sensitive) to the new policy rule; for example:



Note: The name cannot contain the following characters: `< > \ ; & ' " =`

14. Click **Finish** (or **Cancel** to close the wizard without saving the policy).
    The Create Policy page closes.

The policy rule is saved to the policy library in the CMP system.

Once a policy rule is created, you must deploy it to MPE devices so it can take effect. Reference policy rules (rules called by parent policy rules) do not need to be deployed; they are deployed automatically when called by a parent rule. See *Managing Policy Rules*.

Modes Within the Policy Wizard

The behavior of the policy wizard varies depending on the mode in which your CMP is running. The mode can affect many policy wizard behaviors, including the following:

- Entire categories of conditions are enabled or disabled.
- Specific conditions and/or actions are enabled or disabled.
- Some conditions will have a slightly different appearance.
- The set of valid values for some parameters will vary.

If your policy wizard does not include a category, condition, or action documented here, it means that those categories, conditions, or actions are not relevant in your present CMP mode.

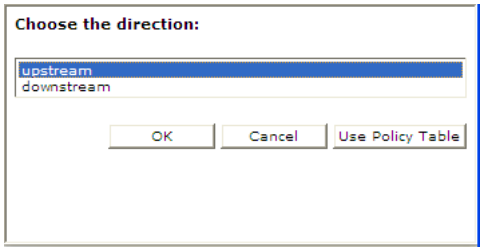
Parameters Within Policy Rules

When you are defining policy rules, both the conditions and actions may contain parameters. Parameters let you customize the specific situation in which a policy rule will be applied. Some conditions and actions may contain multiple parameters. For example, one possible condition is as follows:

```
where the device will be handling greater than 100 upstream reserved flows
```

This condition contains four different parameters. The policy wizard displays the parameters using a red font, with each parameter having a single continuous underline. In this example, greater than is a single parameter, as is 100, upstream, and reserved.

You can click on any parameter to open a pop-up window that lets you specify the value of that parameter. Each parameter has a data type associated with it that determines the values that can be specified: some may be numbers, some may be free-form text, and some may be limited to specific sets of values. For example, the following parameter is limited to a set of text values:



If you have many policies with similar structures, you can consolidate them using policy tables to capture the differences. To specify a parameter in a rule that uses a policy table, instead of selecting a value click **Use Policy Table**. For more information on table-driven policies see *Managing Policy Tables*.

Table 6: Common Parameters defines some common parameter types that are used in many of the policy rules. In this table, the column labeled "Default Text" shows the text value that is displayed in the condition or action text when they are initially displayed. (This may be different in some instances, but this value is the default.)

There are also many parameter types that are used in only one condition or action. These parameter types are defined in the sections where those conditions or actions are defined.

Table 6: Common Parameters

Parameter Type	Default Text	Description of Values
app-name	specified name	Names of applications that have been defined in the CMP.
bandwidth	#	A numeric value that specifies bandwidth in bits per second (bps). You can also type “k”, “K”, “m”,”M”, “g”, or “G” in the value to specify the value in units of kilobits, megabits, or gigabits per second instead.

Parameter Type	Default Text	Description of Values
class-of-service	specified class of	One (or more) of the following: • **Background** • **Conversational** • **Streaming** • **Interactive**
flow-direction	upstream	One of the following: • **upstream** • **downstream** • **upstream or downstream**
ip-address	specified address	An IPv4 or IPv6 address.
log-message	text	Any string. This text may contain policy parameters (as described later in this section) that perform parameter substitution within the message text.
matches-op	matches one of	One of the following: • **matches one of** • **does not match any of**
match-list		A comma-separated list of values, where each value is a wildcard match pattern that uses the "*" character to match zero or more characters and the "?" character matches exactly one character.
number	#	A numeric value. In some circumstances, the numeric value may be required to fall within a certain range of valid values.
operator	greater than	One of the following: • **greater than or equal to** • **greater than** • **less than or equal to** • **less than** • **equal to** • **not equal to**
operator-binary	is	One of the following: • **is** • **is not**
operator-greater	greater than	One of the following: • **greater than or equal to** • **greater than**

Parameter Type	Default Text	Description of Values
operator-less	less than	One of the following: • **less than or equal to** • **less than**
percent	#	An integer value between 0 and 100; for certain values, an extended, non-integer percentage that can exceed 100 (for example, 102.4%).
qos-direction	upstream	One of the following: • **upstream** • **downstream**
qos-status	reserved	One or more of the following: • **reserved** • **committed**
seconds	#	A numeric value that specifies time in units of seconds.
string	specified	Any string.
subnet	specified subnet	An IPv4 subnet in CIDR notation (for example, 1.2.3.0/24); or an IPv6 subnet (for example, fc00::1006/64).

Conditions Available for Writing Policy Rules

The policy wizard supports a large number of conditions that can be used for constructing policy rules. To help you find the conditions you want, the conditions are organized into different categories, which are summarized in *Table 7: Policy Condition Categories*.

Table 7: Policy Condition Categories

Category	Description
Request	Conditions that are based on information that is explicitly contained within or related to the protocol message (request) that triggered the policy rule execution.
Application	Conditions related to the application associated with the request.
Network Device Identity	Conditions related to the specific network device for which the policy rule is being evaluated. This includes conditions based on the network device type, as well as those that refer to specific unique identifiers for network devices.

Category	Description
Network Device Usage	Conditions related to the calculated usage for the network device for which the policy rule is being evaluated. This usage includes device-level tracking of both bandwidth and flow/session counts.
Mobility	Conditions that are based on information associated with networks that include mobile subscribers (such as a wireless network).
User	Conditions related to the subscriber, or subscriber account, that is associated with the protocol message that triggered the policy rule execution. This includes subscriber-level and account-level tracking of usage.
User State	Conditions related to subscriber properties
Policy Context Properties	Conditions related to the context in which a policy is evaluated.
Time of Day	Conditions related to the time at which the policy rules are being executed.

The conditions that are included within each of these categories are described in the sections that follow. Conditions are listed in alphabetical order. The parameters that can be modified within each condition are also summarized, with detailed descriptions of these parameters being described later in this section.

Request Conditions

Request conditions are based on information that is explicitly contained within, or related to, the protocol message (request) that triggered the policy rule execution. The following conditions are available.

Condition **where at least one Filter-ID AVP exists**

Description Tests whether the current request contains one or more Filter-ID AVPs.

Condition **where at least one Final-Unit-Action matches Final-Unit-Action to match**

Parameters where at least one Final-Unit-Action matches *action*

action — One of the following:

- **ACTION_TERMINATE**
- **ACTION_REDIRECT**
- **ACTION_RESTRICT_ACCESS**

Description Tests whether the current request contains an FUI AVP matching the specified Final Unit Action (FUA).

Condition **where at least one Final-Unit-Indication AVP exists**

Description Tests whether the current request contains one or more Final-Unit-Indication (FUI) AVPs.

Condition **where Filter-ID AVP does not exist**

Description Tests whether the current request contains no Filter-ID AVPs.

Condition	**where the AF-Application-ID matches one of specified value(s)**
Parameters	where the AF-Application-ID matches one of *csv* *csv* — Comma-separated list of text values.
Description	Selects protocol messages based on the Diameter AF Application Identifier field. A valid AF Application identifier is any string describing the application, for example VoIP or streaming.
Condition	**where the bearer usage is General**
Parameters	where the bearer usage is *bearer-usage* *bearer-usage* — One or more of the following: • **General** • **IMS Signaling**
Description	Selects protocol message based on the user or equipment information.
Condition	**where the enforcement session is an IP-CAN session**
Parameters	where the enforcement session is *enforcement-session-type* *enforcement-session-type* — One or more of the following: • **an IP-CAN session** • **a gateway control session**
Description	Distinguishes between different types of enforcement sessions.
Condition	**where the event trigger is one of specified trigger(s)**
Parameters	where the event trigger is one of *event-trigger* *event-trigger* — One or more of the following: • **SGSN_CHANGE** • **LOSS_OF_BEARER** • **RECOVERY_OF_BEARER** • **GW_PCEF_MALFUNCTION** • **MAX_NR_BEARERS_REACHED** • **QOS_CHANGE_EXCEEDING_AUTHORIZATION** • **ECGI_CHANGE** • **RAI_CHANGE** • **TAI_CHANGE** • **USER_LOCATION_CHANGE** • **OUT_OF_CREDIT** • **REALLOCATION_OF_CREDIT** • **REVALIDATION_TIMEOUT** • **UE_IP_ADDRESS_ALLOCATE** • **UE_IP_ADDRESS_RELEASE** • **DEFAULT_EPS_BEARER_QOS_CHANGE** • **AN_GW_CHANGE**

- **SUCCESSFUL_RESOURCE_ALLOCATION**
- **PCF_CHANGE**
- **LOSS_OF_FLOW**
- **RECOVERY_OF_FLOW**
- **AGW_MALFUNCTION**
- **ACCESS_NETWORK_PHYSICAL_ACCESS_ID_CHANGE**
- **QOS_CHANGE**
- **RAT_CHANGE**
- **TFT_CHANGE**
- **PLMN_CHANGE**
- **IP_CAN_CHANGE**
- **RESOURCES_LIMITATION**
- **USAGE_TIME_ZONE_CHANGE**
- **USAGE_THRESHOLD_REACHED**
- **USAGE_REPORT**
- **CELL_CONGESTED**
- **CELL_CLEAR**
- **SERVICE_FLOW_DETECTION**

Description Selects protocol messages based on the event trigger.

Condition **where the Filter-ID in the Final-Unit-Indication AVP as Policy Condition**

Description Provides PCRF support for constructing and executing policy conditions and rules. The Filter-ID value(s) are received in the Final-Unit-Indication AVP.

Condition **where the Filter-Ids in the Final-Unit-Indication AVPs match one or more of Filter-Ids to match and the search type is MATCH ALL FROM ANY REPORT**

Parameters where the Filter-Ids in the Final-Unit-Indication AVPs match one or more of *csv* and the search type is *search*

csv — A comma-separated list of text values

search — One of the following:

- **MATCH_ALL_FROM_ANY_REPORT**
- **MATCH_NONE**
- **MATCH_ANYONE**
- **MATCH_ALL_FROM_ONE_REPORT**

Description Provides a minimum of at least one Filter-ID in the message that must match the provisioned value or list. Each ID in the provisioned list must match what is in the message.

Condition **where Final-Unit-Indication AVP does not exist**

Description Allows for a condition that will determine if the PCRF current request contains a Final-Unit-Indication (FUI) AVP.

Condition **where the flow is an application flow**

Parameters where the flow is *flow-type*

flow-type — One or more of the following:

- **an application flow** (the default)
- **a UE flow**
- **the default flow**

Description Selects protocol messages based on the type of flow.

Condition **where the flow media type is one of specified type(s)**

Parameters where the flow media type is one of *media-type*

media-type — One or more of the following:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Description Selects protocol messages based on the flow's media type.

Condition **where the flow media type specified type(s) is one of specified status(s)**

Parameters where the flow media type *media-type* is one of *media-status*

media-type — One or more of the following media types:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

media-status — One or more of the following status types:

- **Enabled**
- **Enabled Uplink**
- **Enabled Downlink**
- **Disabled**
- **Removed**

Description Selects protocol messages that matches the flow's media type and status type.

Condition **where the flow media types Matches specified type(s)**

Parameters where the flow media type matches one of *specified type*

specified type — One or more of the following media types:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Description Selects protocol messages that match the flow's media type.

Condition **where the flow packet filter matches one of specified packet filter(s)**

Parameters where the flow packet filter *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Selects protocol messages based on the packet filters. The packet filters use IPFilterRule format, as defined in the Diameter base protocol (RFC 3588). For example: `permit in ip from 10.0.0.1 to 10.0.0.2 5060`.

Condition **where the flow usage is one of specified usage(s)**

Parameters where the flow usage is *flow-usage-type*

flow-usage-type — One or more of the following:

- **No Information**
- **RTCP**
- **AF Signaling**

Description Selects protocol messages based on the flow usage.

Condition **where the IP-CAN bearer is the primary bearer**

Parameters where the IP-CAN bearer is *bearer-type*

bearer-type — One or more of the following:

- **the primary bearer**
- **a secondary bearer**

Description Selects protocol messages based on the IP-CAN bearer type.

Condition **where the PCC rule being reinstalled contains one of specified rule name(s) and the retry is the final attempt**

Parameters where the PCC rule being reinstalled contains one of *csv* and the retry *operator-binary* the final attempt

csv — Comma-separated list of text values.

operator-binary — One of the following:

- **is**
- **is not**

Description Reinstalls the specified PCC rule depending on whether this is the final retry attempt or not.

Condition **where the QoS parameters in the flow are equal to specified value**

Parameters where the QoS parameters in the flow are equal to *profile-param*

profile-param — Names of profile parameters that are derived from internal representations of protocol messages. For the specific meaning of the fields, consult the specific protocol specifications.

- **Diameter AF Flow-Description**
- **Diameter AF Flow-Status**
- **Diameter AF Flow-Usage**
- **Diameter AF Maximum-Authorized-Data-Rate**
- **Diameter AF Media-Type**
- **Diameter AF PacketTime**
- **Diameter AF QCI**
- **Diameter AF Reservation-Priority**
- **Diameter AF RTCP RR-Bandwidth**
- **Diameter AF RTCP RS-Bandwidth**
- **Diameter APN-Aggregate-Max-Bitrate-DL**
- **Diameter APN-Aggregate-Max-Bitrate-UL**
- **Diameter Bearer ARP Priority Level**
- **Diameter Bearer Guaranteed-Bitrate-DL**
- **Diameter Bearer Guaranteed-Bitrate-UL**
- **Diameter Bearer Maximum-Requested-Bandwidth-DL**
- **Diameter Bearer Maximum-Requested-Bandwidth-UL**
- **Diameter Bearer QCI**
- **Diameter Default EPS ARP Preemption Capability**
- **Diameter Default EPS ARP Preemption Vulnerability**
- **Diameter Default EPS ARP Priority Level**
- **Diameter Default EPS Bearer QCI**
- **Diameter Enforcement Session Bearer Control Mode Selection**
- **Diameter Enforcement Session Event Triggers**
- **Diameter Credit-Control Session Trigger Type**
- **Diameter Flow-Status**
- **Diameter IP-CAN Session Bearer Control Mode**
- **Diameter IP-CAN Session Default Offline Charging**
- **Diameter IP-CAN Session Default Online Charging**
- **Diameter IP-CAN Session Primary OCS**
- **Diameter IP-CAN Session Primary OFCS**
- **Diameter IP-CAN Session Secondary OCS**
- **Diameter IP-CAN Session Secondary OFCS**

- **Diameter IP-CAN Session Usage Monitoring**
- **Diameter IP-CAN Session Usage Reporting**
- **Diameter PCC Rule AF-Charging-Identifier**
- **Diameter PCC Rule ARP Preemption Capability**
- **Diameter PCC Rule ARP Preemption Vulnerability**
- **Diameter PCC Rule ARP Priority Level**
- **Diameter PCC Rule Flow-Status**
- **Diameter PCC Rule Guaranteed-Bitrate-DL**
- **Diameter PCC Rule Guaranteed-Bitrate-UL**
- **Diameter PCC Rule Maximum-Requested-Bandwidth-DL**
- **Diameter PCC Rule Maximum-Requested-Bandwidth-UL**
- **Diameter PCC Rule Metering-Method**
- **Diameter PCC Rule Monitoring-Key**
- **Diameter PCC Rule Offline Charging**
- **Diameter PCC Rule Online Charging**
- **Diameter PCC Rule Precedence**
- **Diameter PCC Rule QCI**
- **Diameter PCC Rule Rating-Group**
- **Diameter PCC Rule Reporting-Level**
- **Diameter PCC Rule Service-Identifier**

Description Selects protocol messages based on values of specific parameters in the protocol message for which there may not be an explicit condition already.

Condition **where the quota is requested**

Parameters where the quota is *quota-change-type*

quota-change-type — One or more of the following:

- **requested**
- **debited**

Description Selects protocol messages based on the type of change to the quota. See *Managing Quotas* for information about defining quotas.

Condition **where the quota usage rating conditions changed trigger is one of specified values**

Parameters where the quota usage rating conditions changed trigger is one of *trigger-type*

trigger-type — One or more of the following:

- **CHANGE_IN_SGSN_IP_ADDRESS**
- **CHANGE_IN_QOS**
- **CHANGE_IN_LOCATION**
- **CHANGE_IN_RAT**
- **CHANGE_IN_QOS_TRAFFIC_CLASS**
- **CHANGE_IN_QOS_RELIABILITY_CLASS**
- **CHANGE_IN_QOS_DELAY_CLASS**
- **CHANGE_IN_QOS_PEAK_THROUGHPUT**

- **CHANGE_IN_QOS_PRECEDENCE_CLASS**
- **CHANGE_IN_QOS_MEAN_THROUGHPUT**
- **CHANGE_IN_QOS_MAXIMUM_BIT_RATE_FOR_UPLINK**
- **CHANGE_IN_QOS_MAXIMUM_BIT_RATE_FOR_DOWNLINK**
- **CHANGE_IN_QOS_RESIDUAL_BER**
- **CHANGE_IN_QOS_SDU_ERROR_RATIO**
- **CHANGE_IN_QOS_TRANSFER_DELAY**
- **CHANGE_IN_QOS_TRAFFIC_HANDLING_PRIORITY**
- **CHANGE_IN_QOS_GUARANTEED_BIT_RATE_FOR_UPLINK**
- **CHANGE_IN_QOS_GUARANTEED_BIT_RATE_FOR_DOWNLINK**
- **CHANGE_IN_LOCATION_MCC**
- **CHANGE_IN_LOCATION_MNC**
- **CHANGE_IN_LOCATION_RAC**
- **CHANGE_IN_LOCATION_LAC**
- **CHANGE_IN_LOCATION_CELL_ID**
- **CHANGE_IN_MEDIA_COMPOSITION**
- **CHANGE_IN_PARTICIPANTS_NMB**
- **CHANGE_IN_THRSHLD_OF_PARTICIPANTS_NMB**
- **CHANGE_IN_USER_PARTICIPATING_TYPE**
- **CHANGE_IN_SERVICE_CONDITION**
- **CHANGE_IN_SERVING_NODE**

Description Selects protocol messages based on the quota usage rating conditions changed trigger. See *Managing Quotas* for information about defining quotas.

Condition **where the quota usage reporting reason is one of specified values**

Parameters where the quota usage reporting reason is one of *reporting-reason*

reporting-reason — One or more of the following:

- **threshold reached**
- **quota holding time reached**
- **final reporting**
- **quota exhausted**
- **validity time expired**
- **other quota type reported**
- **rating condition changed**
- **forced reauthorization**
- **pool exhausted**

Description Selects protocol messages based on the quota usage reporting reason. See *Managing Quotas* for information about defining quotas.

Condition **where the request AVP name exists**

Parameters where the request AVP *avp accessibility*

avp — AVP in for format *name:vendorID*, or a full path [*avp_name1*]:*vendorID*.[*avp_name2*]:*vendorID*... for the members of the grouped AVPs

accessibility — One of the following:

- **exists**
- **does not exist**

Description Checks for the presence or absence of the third-party AVP in an incoming Diameter message.

Note: The condition supports both loaded base Diameter AVPs and third-party AVPs.

Condition **where the request AVP name is numerically equal to value**

Parameters where the request AVP *avp* is numerically *operator value*

avp — AVP in for format *name:vendorID*, or a full path [*avp_name1*]:*vendorID*.[*avp_name2*]:*vendorID*... for the members of the grouped AVPs

operator — See common parameters.

value — String value.

Description Compares a numerical AVP value against a specified number or policy context number variable value.

Note: The condition supports both loaded base Diameter AVPs and third-party AVPs.

Condition **where the request AVP name value contains one of value(s)**

Parameters where the request AVP *avp* value *containment csv*

avp — AVP in for format *name:vendorID*, or a full path [*avp_name1*]:*vendorID*.[*avp_name2*]:*vendorID*... for the members of the grouped AVPs

containment — One of the following:

- **contains one of**
- **does not contain any of**

csv — Comma-separated list of text values.

Description Performs a lookup of the sub-strings in the AVP value. It is possible to check multiple sub-string entries at once. If the operation type is changed, you can check the opposite scenario, which would not include any of the provided sub-strings.

Note: The condition supports both loaded base Diameter AVPs and third-party AVPs.

Condition **where the request AVP name value matches one of value(s)**

Parameters where the request AVP *avp* value *matches-op csv*

avp — AVP in for format *name:vendorID*, or a full path [*avp_name1*]:*vendorID*.[*avp_name2*]:*vendorID*... for the members of the grouped AVPs

matches-op — See common parameters.

csv — Comma-separated list of text values.

Description Compares the specified AVP value with the values or variables from the specified list. The condition is where the request AVP name value matches one of value(s). The values can be evaluated for equality as well as inequality. To evaluate AVP value for inequality, the condition *matches one* must be changed to *does not match any of*.

Note: The condition supports both loaded base Diameter AVPs and third-party AVPs.

Condition **where the request is creating a new flow**

Parameters where the request is *change-type*

change-type — One or more of the following:

- **creating a new flow**
- **modifying an existing flow**
- **provisioning a default flow**
- **terminating an existing flow**

Description Distinguishes between protocol messages based on the type of operation being performed on the flow.

Condition **where the request is creating a new session**

Parameters where the request is *request-type*

request-type — One or more of the following:

- **creating a new session**
- **modifying an existing session**
- **re-authorizing an existing session**
- **terminating an existing session**

Description Distinguishes between protocol messages based on the type of operation being performed on the subscriber's session.

Condition **where the request is for reserved bandwidth**

Parameters where the request is for *qos-status* bandwidth

qos-status — See common parameters.

Description Distinguishes between protocol messages based on the type of bandwidth that is being updated.

Condition **where the request is for upstream bandwidth**

Parameters where the request is for *qos-direction* bandwidth

qos-direction — See common parameters.

Description Distinguishes between protocol messages based on the direction of bandwidth that is being updated.

Condition **where the requested guaranteed upstream bandwidth is greater than # bps**

Parameters where the requested guaranteed *flow-direction* bandwidth is *operator bandwidth* bps

flow-direction — See common parameters.

operator — See common parameters.

bandwidth — See common parameters.

Description Selects protocol messages based on the amount of bandwidth being requested in a specific direction relative to a numeric value.

Condition **where the requested maximum upstream bandwidth is greater than # bps**

Parameters where the requested maximum *flow-direction* bandwidth is *operator bandwidth* bps

flow-direction — See common parameters.

operator — See common parameters.

bandwidth — See common parameters.

Description Selects protocol messages based on the maximum amount of bandwidth being requested in a specific direction relative to a numeric value.

Condition **where the requested media component description reservation priority is one of specified**

Parameters where the requested media component description reservation priority is one of *priority*

priority — One or more of the following:

- **DEFAULT**
- **PRIORITY_ONE**
- **PRIORITY_TWO**
- **PRIORITY_THREE**
- **PRIORITY_FOUR**
- **PRIORITY_FIVE**
- **PRIORITY_SIX**
- **PRIORITY_SEVEN**

Description Selects Rx protocol messages based on the requested media component description reservation priority.

Condition **where the requested QCI is one of specified**

Parameters where the requested QCI is one of *class-of-service*

class-of-service — One or more of the following:

- **1** (Conversational speech)

- **2** (Conversational)
- **3** (Streaming speech)
- **4** (Streaming)
- **5** (Interactive with priority 1 signalling)
- **6** (Interactive with priority 1)
- **7** (Interactive with priority 2)
- **8** (Interactive with priority 3)
- **9** (Background)

Description Selects protocol messages based on the QoS class identifier (QCI).

Condition **where the requested quota is one of select quota**

Parameters where the requested quota is one of *quota-name*

quota-name — Names of quotas that are defined in the CMP.

Description Selects protocol messages based on the requested quotas. See *Managing Quotas* for information about defining quotas.

Condition **where the requested rating group is one of select rating group**

Parameters where the requested rating group is one of *rating-group-name*

rating-group-name — Names of rating groups that are defined in the CMP.

Description Selects protocol messages based on the subscriber's rating group. See *Managing Services and Rating Groups* for information on services.

Condition **where the requested service(s) are select service**

Parameters where the requested services are *service-profile-name*

service-profile-name — Names of service profiles that are defined in the CMP.

Description Selects protocol messages based on the services in the request. See *Managing Services and Rating Groups* for information on services.

Condition **where the requested session reservation priority is one of specified**

Parameters where the requested session reservation priority is one of *priority*

priority — One or more of the following:

- **DEFAULT**
- **PRIORITY_ONE**
- **PRIORITY_TWO**
- **PRIORITY_THREE**
- **PRIORITY_FOUR**
- **PRIORITY_FIVE**
- **PRIORITY_SIX**
- **PRIORITY_SEVEN**

Description Selects Rx protocol messages based on the requested session reservation priority.

Condition **where the requested upstream APN aggregate maximum bitrate is greater than # bps**

Parameters where the requested *flow-direction* APN aggregate maximum bitrate is *operator bandwidth* bps

flow-direction — See common parameters.

operator — See common parameters.

bandwidth — See common parameters.

Description Selects protocol messages based on the maximum bitrate being requested in a specific direction relative to a numeric value.

Condition **where the rule report contains one of specified rule name(s) and the final unit action is one of ACTION_TERMINATE and the rule status is active**

Parameters where the rule report contains one of *csv* and the final unit action is one of *action* and the rule status is *field*

csv — Comma-separated list of text values.

action — One of the following:

- **ACTION_TERMINATE**
- **ACTION_REDIRECT**
- **ACTION_RESTRICT_ACCESS**

field — One of the following:

- **active**
- **inactive**
- **temporarily_inactive**

Description Selects protocol messages based on the rule name, reported final unit action, and status received in a rule report.

Condition **where the rule report contains one of specified rule name(s) and the rule status is active**

Parameters where the rule report contains one of *csv* and the rule status is *field*

csv — Comma-separated list of text values.

field — One of the following:

- **active**
- **inactive**
- **temporarily_inactive**

Description Selects protocol messages based on the rule name and status received in a rule report.

Condition **where the rule report contains one of specified rule name(s) and the rule status is active and the rule failure code is one of specified failure code(s)**

Parameters where the rule report contains one of *csv* and the rule status is *field* and the rule failure code is one of *failcode*

csv — Comma-separated list of text values.

field — One of the following:

- **active**
- **inactive**
- **temporarily_inactive**

failcode — One of the following:

- **UNKNOWN_RULE_NAME**
- **RATING_GROUP_ERROR**
- **SERVICE_IDENTIFICATION_ERROR**
- **GW_PCEF_MALFUNCTION**
- **RESOURCES_LIMITATION**
- **MAX_NR_BEARERS_REACHED**
- **UNKNOWN_BEARER_ID**
- **MISSING_BEARER_ID**
- **MISSING_FLOW_DESCRIPTION**
- **RESOURCE_ALLOCATION_FAILURE**
- **UNSUCCESSFUL_QOS_VALIDATION**

Description Selects protocol messages based on the rule name, status, and failure code received in a rule report.

Condition **where the rule report contains one of specified rule name(s) and the rule status is active and the rule failure code is one of specified failure code(s) and the maximum retry count is reached**

Parameters where the rule report contains one of *csv* and the rule status is *field* and the rule failure code is one of *failcode* and the maximum retry count *operator-binary* reached

csv — Comma-separated list of text values.

field — One of the following:

- **active**
- **inactive**
- **temporarily_inactive**

failcode — One of the following:

- **UNKNOWN_RULE_NAME**
- **RATING_GROUP_ERROR**
- **SERVICE_IDENTIFICATION_ERROR**
- **GW_PCEF_MALFUNCTION**
- **RESOURCES_LIMITATION**
- **MAX_NR_BEARERS_REACHED**
- **UNKNOWN_BEARER_ID**
- **MISSING_BEARER_ID**
- **MISSING_FLOW_DESCRIPTION**
- **RESOURCE_ALLOCATION_FAILURE**
- **UNSUCCESSFUL_QOS_VALIDATION**

operator-binary — One of the following:

- **is**
- **is not**

Description Selects protocol messages based on the rule name, status, failure code, and retry count received in a rule report.

Condition **where the select type is contained in Match List(s) select list(s)**

Parameters where the *field* is contained in Match List(s) *match-list*

field — One or more of the following:

- **Serving Gateway Address** — IP address of the serving gateway
- **APN** — Access Point Name
- **User Equipment Identity**
- **USER IMSI** — User International Mobile Subscriber Identity
- **USER E.164** — User E164 phone number
- **User SIP URI** — User Session Initiation Protocol Uniform Resource Identifier
- **User NAI** — User Network Access Identifier
- **Endpoint IP Address** — IP address of the endpoint
- **Serving MCC-MNC** — Serving Mobile Country Code, Mobile Network Code
- **Cell Identifier**
- **Location Area Code** — Unique identifier of a location area
- **Serving Area Code**
- **Routing Area Code** — Identifies a routing area within a location area
- **Routing Area Identifier** — Combination of the location area code and routing area code
- **Tracking Area Code**
- **E-UTRAN Cell Identifier** — Identifies cells within a PLMN
- **Entitlements** — A defined entitlement

match-list — See common parameters.

Description Selects protocol messages based on whether the messages or associated sessions match any of the values in a match list. Any of the types can be selected in combination. The order will match the list from top to bottom. See *Managing Match Lists* for information about defining match lists.

Example

```
where the
USER_IMSI,LAC,SAC is contained in Match List(s)
select lists(s)
```

Condition **where the select type is not contained in Match List(s) select list(s)**

Parameters where the *field* is not contained in Match List(s) *match-list*

field — One or more of the following:

- **Serving Gateway Address**
- **APN** — Access Point Name

- **User Equipment Identity**
- **USER IMSI** — User International Mobile Subscriber Identity
- **USER E.164** — User E164 phone number
- **User SIP URI** — User Session Initiation Protocol Uniform Resource Identifier
- **User NAI** — User Network Access Identifier
- **Endpoint IP Address** — IP address of the endpoint
- **Serving MCC-MNC** — Serving Mobile Country Code, Mobile Network Code
- **Cell Identifier**
- **Location Area Code** — Unique identifier of a location area
- **Serving Area Code**
- **Routing Area Code** — Identifies a routing area within a location area
- **Routing Area Identifier** — Combination of the location area code and routing area code
- **Tracking Area Code**
- **E-UTRAN Cell Identifier** — Identifies cells within a PLMN
- **Entitlements** — A defined entitlement

match-list — See common parameters.

Description Selects protocol messages based on whether the messages or associated sessions do not match any of the values in a match list. Any of the types can be selected in combination. The order will match the list from top to bottom. See *Managing Match Lists* for information about defining match lists.

Example

```
where the USER IMSI,LAC,RAC is not contained in Match List(s)
select lists(s)
```

Condition **where the service info status is one of specified**

Parameters where the service info status is one of *status*

status — One or more of the following:

- **FINAL_SERVICE_INFORMATION**
- **PRELIMINARY_SERVICE_INFORMATION**

Description Selects Rx protocol messages based on the service information status.

Condition **where the Service-URN is one of specified value(s)**

Parameters where the Service-URN is one of *csv*

csv — A comma-separated list of text values

Description Selects Rx protocol messages based on the value of the Service-URN field.

Condition **where the session is an enforcement session**

Parameters where the session is *session-type*

session-type — One of the following:

- **an enforcement session**
- **an application session**

- **a credit control session**

Description	Distinguishes between protocol messages that are operating on different sessions.
Condition	**where the TDF-Application-Identifier matches one of specified TDF application id(s)**
Parameters	where the TDF-Application-Identifier matches one of *csv* *csv* — Comma-separated list of text values.
Description	Selects protocol messages based on the Traffic Detection Function (TDF) Application Identifier field. A valid TDF application identifier is any string describing the TDF.

Application Conditions

Application conditions are related to the application associated with the request. See *Managing Application Profiles* for information on creating and managing application profiles. The following conditions are available.

Condition	**where the application is latency sensitive**
Description	Triggers a policy when the associated application is latency sensitive (can be set in the CMP when applications are defined).
Condition	**where the application is one of specified name**
Parameters	where the application *operator-binary* one of *app-name* *operator-binary* — See common parameters. *app-name* — Names of applications that are defined in the CMP.
Description	Triggers a policy based on the associated application.
Condition	**where the application will be using greater than # bps upstream reserved bandwidth**
Parameters	where the application will be using *operator-greater bandwidth* bps *qos-direction qos-status* bandwidth *operator-greater* — See common parameters. *bandwidth* — See common parameters. *qos-direction* — See common parameters. *qos-status* — See common parameters.
Description	Triggers a policy based on the total amount of bandwidth used by the associated application as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the amount of bandwidth that is allocated if the current request is approved.
Condition	**where the application will be using greater than # upstream reserved flows**
Parameters	where the application will be using *operator-greater bandwidth qos-direction qos-status* flows

operator-greater — See common parameters.

bandwidth — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

Description Triggers a policy based on the total number of flows used by the associated application as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the flows. The total represents the number of flows that is allocated if the current request is approved.

Condition **where there is no application associated with the request**

Description Triggers a policy when there is no associated application.

Network Device Identity Conditions

Network Device Identity conditions are related to the specific network device for which the policy rule is being evaluated. This includes conditions based on the network device type, as well as those that refer to specific unique identifiers for network devices. See *Managing Network Elements* for information on defining the network elements available. The following conditions are available.

Condition **where the device name matches one of specified name(s)**

Parameters where the device name matches one of *match-list*

match-list — See common parameters.

Description Triggers a policy based on whether the device name matches one or more wildcard match patterns.

Condition **where the device type is specified type**

Parameters where the device type *operator-binary device-type*

operator-binary — See common parameters.

device-type — One or more of the following:

- **PDSN**
- **GGSN**
- **HomeAgent**
- **HSGW**
- **PGW**
- **SGW**
- **DPI**

Description Triggers a policy based on the device type for which it is evaluated.

Condition **where the endpoint IP address is in specified subnet**

Parameters where the endpoint IP address is in *subnet*

subnet — See common parameters.

Description Triggers a policy that is only evaluated for endpoints whose IP address falls within a specific subnet.

Condition	**where the endpoint IP address is specified address**
Parameters	where the endpoint IP address is *ip-address* *ip-address* — See common parameters.
Description	Triggers a policy that is only evaluated for a specific endpoint (based on its IP address).
Condition	**where the network element name matches one of specified name(s)**
Parameters	where the network element name *matches-op csv* *matches-op* — See common parameters.
Description	Triggers a policy based on the name of the network element for which it is being evaluated.
Condition	**where the network element type is specified type**
Parameters	where the network element type *operator-binary element-type* *operator-binary* — See common parameters. *element-type* — One or more of the following: • **GGSN** • **PDSN** • **HomeAgent** • **HSGW** • **PGW** • **SGW** • **DPI**
Description	Triggers a policy based on the type of network element for which it is being evaluated. Note that if the policy is being evaluated for a device that is not a network element but is contained within a network element (such as an interface within a router) then the network element "container" is used as the basis of comparison.
Condition	**where the network element's description field is equal to specified description(s)**
Parameters	where the network element's description field is equal to *description* *description* — string.
Description	Triggers a policy that is only evaluated if the **Description** field of the network element matches the specified string.
Condition	**where the User Equipment ESN matches one of specified ESN value(s)**
Parameters	where the User Equipment ESN *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific ESN values (based on matching wildcard patterns). A valid ESN value has eight

hexadecimal digits, representing the 32 bits of the ESN; for example: A01F3D45.

Condition	**where the User Equipment IMEISV matches one of specified IMEISV value(s)**
Parameters	where the user equipment IMEISV *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific IMEISV values (based on matching wildcard patterns). A valid IMEISV value has 16 decimal digits, as defined in the 3GPP TS 23.003 standard.
Condition	**where the User Equipment MEID matches one of specified MEID value(s)**
Parameters	where the User Equipment MEID *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific MEID values (based on matching wildcard patterns). A valid MEID value has 14 hexadecimal characters; for example: 123456789abcde.

Network Device Usage Conditions

Network Device Usage conditions are related to the calculated usage for the network device for which the policy rule is being evaluated. This usage includes device-level tracking of both bandwidth and flow/session counts. The following conditions are available.

Condition	**where the device will be handling greater than # bps upstream reserved bandwidth**
Parameters	where the device will be handling *operator bandwidth* bps *qos-direction qos-status* bandwidth *operator* — See common parameters. *bandwidth* — See common parameters. *qos-direction* — See common parameters. *qos-status* — See common parameters.
Description	Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.
Condition	**where the device will be handling greater than # bps upstream reserved bandwidth in total for specified application**
Parameters	where the device will be handling *operator bandwidth* bps *qos-direction qos-status* bandwidth in total for *app-name* *operator* — See common parameters.

bandwidth — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

app-name — Names of the applications that are defined in the CMP.

Description Triggers a policy based on the total amount of bandwidth allocated for specific applications by the current device as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

Condition **where the device will be handling greater than # percent of upstream reserved capacity**

Parameters where the device will be handling *operator percent* percent of *qos-direction qos-status* capacity

operator — See common parameters.

percent — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

Description Triggers a policy based on the percent of bandwidth capacity used by the current device as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

Condition **where the device will be handling greater than # percent of upstream reserved capacity for specified application**

Parameters where the device will be handling *operator percent* percent of *qos-direction qos-status* capacity for *app-name*

operator — See common parameters.

percent — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

app-name — Names of the applications that are defined in the CMP.

Description Triggers a policy based on the percent of bandwidth capacity allocated for specific applications by the current device as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

Condition **where the device will be handling greater than # upstream reserved flows**

Parameters where the device will be handling *operator number qos-direction qos-status* flows

operator — See common parameters.

number — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

Description Triggers a policy based on the total number of flows used by the current device as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the flows. The total represents the number of flows that are allocated if the current request is approved.

Condition **where the device will be handling greater than # upstream reserved flows in total for specified application**

Parameters where the device will be handling *operator number qos-direction qos-status* flows in total for *app-name*

operator — See common parameters.

number — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

app-name — Names of the applications that are defined in the CMP.

Description Triggers a policy based on the total number of flows for specific applications used by the current device as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the flows. The total represents the number of flows that are allocated if the current request is approved.

Mobility Conditions

Mobility conditions are based on information associated with networks that include mobile subscribers (such as a wireless network). The following conditions are available.

Condition **where network initiated requests are supported**

Parameters where network initiated requests are *network-request-support*

network-request-support — One of the following:

- **not supported**
- **supported**

Description Triggers a policy that is only evaluated when network initiated requests are or are not supported.

Condition **where the APN matches one of specified APN value(s)**

Parameters where the APN *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific APN values (based on matching wildcard patterns). A valid APN value is any domain name; for example: `network.operator.com`.

Condition **where the BSID matches one of specified BSID value(s)**

Parameters where the BSID *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific BSID values (based on matching wildcard patterns).

Condition **where the Cell Identifier matches one of specified CI value(s)**

Parameters where the Cell Identifier *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific Cell Identifier values (based on matching wildcard patterns). A valid Cell Identifier is an integer between 0 and 65535.

Condition **where the cell state is specified**

Parameters where the cell state is *state*

state — One of the following:

- **congested**
- **not congested**

Description Triggers a policy that is evaluated based on the level of congestion in the cell.

Condition **where the E-UTRAN Cell Identifier matches one of specified ECI value(s)**

Parameters where the E-UTRAN Cell Identifier *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific E-UTRAN Cell Identifier values (based on matching wildcard patterns).

Condition **where the IP address of the Serving Gateway matches one of specified address(es)**

Parameters where the IP address of the Serving Gateway *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific Serving Gateway addresses (based on matching wildcard patterns).

Condition **where the IP-CAN type is specified**

Parameters where the IP-CAN type is *ip-can-type*

ip-can-type — One or more of the following:

- **3GPP GPRS**
- **3GPP EPS**
- **3GPP2**

- **WiMAX**
- **DOCSIS**
- **xDSL**

Description Triggers a policy that is only evaluated for a protocol message with a specific IP-CAN type.

Condition **where the IP address of the Serving PCF matches one of specified address(es)**

Parameters where the IP address of the Serving PCF *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific Serving PCF addresses (based on matching wildcard patterns).

Condition **where the IP address of the Home Agent matches one of specified address(es)**

Parameters where the IP address of the Home Agent *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more Home Agent addresses (based on matching wildcard patterns).

Condition **where the IP address of the Foreign Agent matches one of specified address(es)**

Parameters where the IP address of the Foreign Agent *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more Foreign Agent addresses (based on matching wildcard patterns).

Condition **where the Location Area Code matches one of specified LAC value(s)**

Parameters where the Location Area Code *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific Location Area Code values (based on matching wildcard patterns). A valid Location Area Code is an integer between 0 and 65535.

Condition **where the MSTimezone DST is configured daylight savings in hours**

Parameters where the MSTimezone DST is *offset*

offset — Select one of the following:

- **0 hour**

- **1 hour**
- **2 hours**

Description Triggers a policy that is only evaluated if the applied Daylight Savings Time offset for the location of a mobile subscriber/mobile station (MS) matches the parameter.

Condition **where the MSTimezone offset is configured timezone offset**

Parameters where the MSTimezone offset is *offset*

offset — A Greenwich Mean Time (GMT) timezone offset.

Description Triggers a policy that is only evaluated if the applied time zone for a mobile subscriber/mobile station (MS) matches the parameter.

Condition **where the RAT type is specified**

Parameters where the RAT type is *rat-type*

rat-type — One or more of the following:

- **GERAN**
- **UTRAN**
- **HSPA Evolution**
- **UMA/GAN**
- **EUTRAN**
- **WLAN**
- **CDMA2000 1x**
- **HRPD**
- **UMB**

Description Triggers a policy that is only evaluated for a protocol message with a specific Radio Access Technology (RAT) type.

Example The following example changes usage tracking when a user goes into an HRPD RAT type:

```
where the RAT type is HRPD
   and where the event trigger is one of RAT CHANGE
   and where the request is modifying an existing session

grant total volume to 100 percent used for hrpd using key3
continue processing message
```

Condition **where the Routing Area Code matches one of specified RAC value(s)**

Parameters where the Routing Area Code *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific RAC values (based on matching wildcard patterns).

Condition **where the Routing Area Identifier matches one of specified RAI value(s)**

Parameters	where the Routing Area Identifier *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific Routing Area Identifier values (based on matching wildcard patterns). For a description of the format of a Routing Area Identifier, refer to the 3GPP TS 23.003 standard.
Condition	**where the Service Area Code matches one of specified SAC value(s)**
Parameters	where the Service Area Code *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific Service Area Code values (based on matching wildcard patterns). A valid Service Area Code is an integer between 0 and 65535.
Condition	**where the Serving MCC-MNC matches one of specified MCC-MNC value(s)**
Parameters	where the Serving MCC-MNC *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific mobile country code (MCC)-mobile network code (MNC) values (based on matching wildcard patterns). A valid value consists of a 3-digit mobile country code and a 2- or 3-digit mobile network code, such as "123045." See *Managing Serving Gateways to MCCs/MNCs* for information on mapping serving gateways to MCCs and MNCs.
Condition	**where the Tracking Area Code matches one of specified TAC value(s)**
Parameters	where the Tracking Area Code *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific Tracking Area Code values (based on matching wildcard patterns).

User Conditions

User conditions are related to the subscriber, subscriber account, or quota pool that is associated with the protocol message that triggered the policy rule execution. This includes subscriber-level and account-level tracking of usage. The following conditions are available.

Condition	**where the subscriber or pool field + 0 days rounded up with same granularity is after now using configured local time**

Parameters

where the *subscriber field-name direction duration granularity*$_1$ rounded *rounding* with *granularity*$_2$ granularity is *datetime-compare datetime* using *time-zone*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

field-name — String representing a datetime.

direction — One of the following, indicating future or past:

- **+**
- **-**

duration — Positive integer.

granularity$_1$ — The calculated datetime is expressed in this granularity:

- **days**
- **months**
- **hours**
- **minutes**

rounding — One of the following, indicating rounding up or down:

- **up**
- **down**

granularity$_2$ — Rounding, either up or down, is expressed in this granularity:

- **same** (same as *granularity*$_1$)
- **months**
- **days**
- **hours**
- **minutes**

datetime-compare — One of the following:

- **after**
- **before**
- **at or before**
- **at or after**

datetime — One of the following:

- The local date-time **now** (the default)
- A policy variable
- A date-time in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*+*UTCoffset*

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device
- **system local time** — Calculate the time from the location of this MPE device
- **user local time** — Calculate the time from the location of the user equipment

Description

Triggers a policy that is evaluated based on the result of a comparison between a base date-time value and an offset against either the current date and time or another date-time for the subscriber or quota pool. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location. For information on quota pools, see *Managing Quotas*.

Example

```
where the FamilyPlanGold PromoEnrollTime + 10 days rounded up with
 same granularity is before now using configured local time
```

Condition

where the subscriber or pool field exists

Parameters

where the *subscriber field-name accessibility*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

field-name — String.

accessibility — One of the following:

- **exists** (the default)
- **does not exist**

Description

Triggers a policy that is evaluated if the specified field either exists or does not exist within the subscriber or quota pool data. For information on quota pools, see *Managing Quotas*.

Condition

where the subscriber or pool field is in the current billing cycle using configured local time

Parameters

where the *subscriber field-name* is *comparison-op* the current billing cycle using *time-zone*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

field-name — String.

comparison-op — One of the following:

- **in** (the default)
- **not in**
- **before**
- **after**

time-zone — One of the following:

- **CONFIGURED LOCAL TIME** (the default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location of the user equipment

Description

Triggers a policy that is evaluated based on the comparison of the specified timestamp value and the current billing cycle for the subscriber or quota pool. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location. For information on quota pools, see *Managing Quotas*.

Note: When the user local time context is in effect, the MPE device ends the billing cycle or resets the quota based on the user local time. If user equipment enters a different time zone near the end of a billing cycle, the subscriber may find that the billing cycle ended earlier than expected, or the service provider may find that the billing cycle ended later than expected.

Condition **where the subscriber or pool field is numerically equal to value**

Parameters

where the *subscriber field-name* is numerically *operator value*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

field-name — String.

operator — See common parameters.

value — Integer value in the inclusive range of -9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 (that is, -2^{63} to $2^{63}-1$).

Description

Triggers a policy that is evaluated based on the result of a comparison between the value of a specified field and a numerical value for the subscriber or quota pool. For information on quota pools, see *Managing Quotas*.

Example

```
where the FamilyPlanGold total-session-count is numerically less
than 5
```

Condition **where the subscriber or pool field matches one of specified value(s)**

Parameters

where the *subscriber field-name matches-op match-list*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

field-name — String.

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is evaluated based on the result of a comparison between the value of a specified field and a list of specified values (based on matching wildcard patterns) for the subscriber or quota pool. For information on quota pools, see *Managing Quotas*.

Example

```
where the FamilyPlanGold ISP matches one of GalacTel, LocalTel,
Vf*
```

Condition **where the subscriber or pool profile data is available**

Parameters where the *subscriber* profile data *operator* is available

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

operator — See common parameters.

Description Triggers a policy based on whether subscriber or quota pool data is or is not available. For information on quota pools, see *Managing Quotas*.

Condition **where the subscriber profile data expiration timestamp field for day pass in millis is less than hours from expiration hours from expiring**

Parameters where the subscriber profile data *field-name* is less than *number* hours from expiring

field-name — String.

number — See common parameters.

Description Triggers a policy based on whether the value of a subscriber profile timestamp field is less than the specified number of hours away.

Condition **where the tier is one of specified tier(s)**

Parameters where the tier *operator* one of *tier*

operator — See common parameters.

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is or is not evaluated for one or more specific tiers. See *Managing Subscribers* for information on tiers.

Condition **where the user does not have any of the named entitlements**

Parameters where the user does not have any of the *csv* entitlements

csv — Comma-separated list of text values.

Description Triggers a policy that is evaluated as true for users who do not have any of the specified entitlements. The user must have none of the entitlements in the specified list.

Condition **where the user does not have at least one of the named entitlements**

Parameters where the user does not have at least one of the *csv* entitlements

csv — Comma-separated list of text values.

Description Triggers a policy that is evaluated as true for users who do not have all of the specified entitlements. False if the user has all of the entitlements in the specified list.

Condition **where the user E.164 phone number matches one of specified number(s)**

Parameters where the E.164 phone number *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific E.164 phone numbers (based on matching wildcard patterns). A valid E.164 phone number is any phone number.

Condition **where the user has all of the named entitlements**

Parameters where the user has all of the *csv* entitlements

csv — Comma-separated list of text values.

Description Triggers a policy that is only evaluated for users that have specific entitlements. The user must have all the entitlements in the specified list.

Condition **where the user has at least one of the named entitlements**

Parameters where the user has at least one of the *csv* entitlements

csv — Comma-separated list of text values.

Description Triggers a policy that is evaluated as true for users that have specific entitlements. The user must have one of the entitlements in the specified list.

Condition **where the user IMSI matches one of specified number(s)**

Parameters where the user IMSI *matches-op match-list*

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy that is only evaluated for one or more specific IMSI values (based on matching wildcard patterns). A valid IMSI value is not more than 15 digits, including the mobile country code (3 digits), mobile network code (2 to 3 digits), and the mobile station identification number. For example: 310150123456789.

Condition **where the user is using greater than # bytes in total volume for selected quota**

Parameters where the user is using *operator number* bytes in *quota-type* volume for *quota-name* quota

operator — See common parameters.

number — See common parameters.

quota-type — One of the following:

quota-name — Names of quotas that are defined in the CMP.

Description Triggers a policy based on the amount of the byte-based quota used by the subscriber as it relates to a defined threshold. The usage is either uplink, downlink, or total (the default). See *Managing Quotas* for information on quotas.

Condition **where the user is using greater than # percent and less than # percent of select type for selected quota**

Parameters where the user is using *operator extended-percent* percent and *operator percent* percent of *quota-type* for *quota-name* quota

operator — See common parameters.

extended-percent — See common parameters.

quota-type — One of the following:

- **time**
- **total volume**
- **uplink volume**
- **downlink volume**

quota-name — Names of quotas that are defined in the CMP.

Description Triggers a policy based on the percent of the specific quota used by the subscriber as it relates to a range. The total represents the quota that is allocated if the current request is approved. See *Managing Quotas* for information on quotas.

Condition **where the user is using greater than # percent of select type for selected quota**

Parameters where the user is using *operator extended-percent* percent of *quota-type* for *quota-name* quota

operator — See common parameters.

extended-percent — See common parameters.

quota-type — One of the following:

- **time**
- **total volume**
- **uplink volume**
- **downlink volume**

quota-name — Names of quotas that are defined in the CMP.

Description Triggers a policy based on the percent of the specific quota used by the subscriber as it relates to a defined threshold. The total represents the quota that is allocated if the current request is approved. See *Managing Quotas* for information on quotas.

Condition **where the user is using greater than # seconds in total for selected quota**

Parameters where the user is using *operator seconds* seconds in total for *quota-name* quota

operator — See common parameters.

seconds — See common parameters.

quota-name — Names of quotas that are defined in the CMP.

Description	Triggers a policy based on the amount of the time-based quota used by the subscriber as it relates to a defined threshold. The total represents the quota that is allocated if the current request is approved. See *Managing Quotas* for information on quotas.
Condition	**where the user is using greater than # service-specific units for selected quota**
Parameters	where the user is using *operator number* service-specific units for *quota-name* quota *operator* — See common parameters. *number* — See common parameters. *quota-name* — Names of quotas that are defined in the CMP.
Description	Triggers a policy based on the amount of the service-based quota used by the subscriber as it relates to a defined threshold. The total represents the quota that is allocated if the current request is approved. See *Managing Quotas* for information on quotas.
Condition	**where the user NAI matches one of specified id(s)**
Parameters	where the user NAI *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific NAI values (based on matching wildcard patterns).
Condition	**where the user realm matches one of specified realm(s)**
Parameters	where the user realm *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific realms (based on matching wildcard patterns).
Condition	**where the user SIP URI matches one of specified URI(s)**
Parameters	where the user SIP URI *matches-op match-list* *matches-op* — See common parameters. *match-list* — See common parameters.
Description	Triggers a policy that is only evaluated for one or more specific SIP URI values (based on matching wildcard patterns).
Condition	**where the user will be using greater than # bpsupstream reserved bandwidth**
Parameters	where the user will be using *operator bandwidth* bps *qos-direction qos-status* bandwidth *operator* — See common parameters. *bandwidth* — See common parameters. *qos-direction* — See common parameters.

qos-status — See common parameters.

Description Triggers a policy based on the total amount of bandwidth used by the associated subscriber as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

Condition **where the user will be using greater than # bps upstream reserved bandwidth in total for specified application**

Parameters where the user will be using *operator bandwidth* bps *qos-direction qos-status* bandwidth in total for *app-name*

operator — See common parameters.

bandwidth — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

app-name — Names of applications that are defined in the CMP.

Description Triggers a policy based on the total amount of bandwidth allocated for specific applications by the associated subscriber as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved. See *Managing Application Profiles* for information on applications.

Condition **where the user will be using greater than # upstream reserved flows**

Parameters where the user will be using *operator number qos-direction qos-status* flows

operator — See common parameters.

number — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

Description Triggers a policy based on the total number of flows used by the associated subscriber as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of these flows. The total represents the number of flows that are allocated if the current request is approved.

Condition **where the user will be using greater than # upstream reserved flows in total for specified application**

Parameters where the user will be using *operator number qos-direction qos-status* flows in total for *app-name*

operator — See common parameters.

number — See common parameters.

qos-direction — See common parameters.

qos-status — See common parameters.

app-name — Names of applications that are defined in the CMP.

Description Triggers a policy based on the total number of flows for specific applications used by the associated subscriber as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the flows. The total represents the number of flows that are allocated if the current request is approved. See *Managing Application Profiles* for information on applications.

Condition **where the User's Tier upstream bandwidth limit is between # bps and # bps**

Parameters where the User's Tier *qos-direction* bandwidth limit is between *bandwidth* bps and *bandwidth* bps

qos-direction — See common parameters.

bandwidth — See common parameters.

Description Triggers a policy that is evaluated for a user tier based on the bandwidth limit. This can be further qualified by the direction of the bandwidth. See *Managing Subscribers* for information on tiers.

Example

```
where the User's Tier downstream bandwidth limit is between 2M bps
 and 25M bps
```

Condition **where the User's Tier upstream bandwidth limit is greater than # bps**

Parameters where the User's Tier *qos-direction* bandwidth limit is *operator bandwidth* bps

qos-direction — See common parameters.

operator — See common parameters.

bandwidth — See common parameters.

Description Triggers a policy that is evaluated for a user tier based on the comparison between the bandwidth limit and a numerical value. This can be further qualified by the direction of the bandwidth. See *Managing Subscribers* for information on tiers.

Example

```
where the User's Tier downstream bandwidth limit is less than or
equal to 25M bps
```

User State Conditions

User state conditions are related to the value of subscriber properties, retrieved by name from a Subscriber Profile Repository (SPR), when the policy rules are being executed. The following conditions are available.

Condition **where the subscriber or pool property name + 0 days rounded up with same granularity is after now using configured local time**

Parameters where the *subscriber* property *property-name direction duration* $granularity_1$ rounded *rounding* with $granularity_2$ granularity is *datetime-compare datetime* using *time-zone*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

direction — One of the following, indicating future or past:

- **+**
- **-**

duration — Positive integer.

granularity$_1$ — The calculated datetime is expressed in this granularity:

- **days**
- **months**
- **hours**
- **minutes**

rounding — One of the following, indicating rounding up or down:

- **up**
- **down**

granularity$_2$ — Rounding, either up or down, is expressed in this granularity:

- **same** (same as *granularity*$_1$)
- **months**
- **days**
- **hours**
- **minutes**

datetime-compare — One of the following:

- **after** (the default)
- **before**
- **at or before**
- **at or after**

datetime — One of the following:

- The local date-time **now** (the default)
- A policy variable
- A date-time in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*+*UTCoffset*

time-zone — One of the following:

- **CONFIGURED LOCAL TIME** (the default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location of the user equipment

Description Triggers a policy that is evaluated for a subscriber or quota poolbased on the result of a comparison between a base date-time value and an offset against either the

current date-time or another date-time. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location. For information on quota pools, see *Managing Quotas*.

Example

```
where the FamilyPlanGold property maintenance-time + 0 minutes is at
 or after 2011-10-24T01:00 using configured local time
```

```
where the FamilyPlanGold property maintenance-time + 0 minutes is at
 or before 2011-10-24T02:00:00-05:00 using configured local time
```

Condition **where the subscriber or pool property name exists**

Parameters where the *subscriber* or pool property *property-name accessibility*

subscriber — One of the following:

property-name — String.

accessibility — One of the following:

- **exists** (the default)
- **does not exist**

Description Triggers a policy based on whether or not the specified property exists within the subscriber or quota pool profile. For information on quota pools, see *Managing Quotas*.

Condition **where the subscriber or pool property name is in the current billing cycle using configured local time**

Parameters where the *subscriber* property *property-name* is *comparison-op* the current billing cycle using *time-zone*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

comparison-op — One of the following:

time-zone — One of the following:

- **CONFIGURED LOCAL TIME** (the default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location of the user equipment

Description Triggers a policy that is evaluated based on the comparison between the timestamp value of the specified subscriber or pool property and the current billing cycle. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location. For information on quota pools, see *Managing Quotas*.

Note: When the user local time context is in effect, the MPE device ends the billing cycle or resets the quota based on the user local time. If user equipment enters a different time zone near the end of a billing cycle, the subscriber may find that the billing cycle ended earlier than expected, or the service provider may find that the billing cycle ended later than expected.

Example

```
where the FamilyPlanGold property last-connect-time is in the current
 billing cycle using configured local time
```

Condition **where the subscriber or pool property name is numerically equal to value**

Parameters where the *subscriber* property *property-name* is numerically *operator value*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

operator — See common parameters.

value — Integer value in the inclusive range of -9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 (that is, -2^{63} to $2^{63}-1$).

Description Triggers a policy based on a numerical comparison between the specified subscriber or quota pool property value and a specified value. For information on quota pools, see *Managing Quotas*.

Condition **where the subscriber or pool property name is the current mobile country code**

Parameters where the *subscriber* property *property-name operator-binary* the current mobile country code

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

operator-binary — See common parameters.

Description Triggers a policy that is evaluated based on the comparison between the value of the specified subscriber or quota pool property and the current mobile country code. For information on quota pools, see *Managing Quotas*.

Example

```
where the FamilyPlanGold property current-mcc is not the current
mobile country code
```

Condition **where the subscriber or pool property name matches one of `value(s)`**

Parameters where the *subscriber* property *property-name matches-op 'match-list'*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy based on whether the specified subscriber or quota pool property value matches a list of specified values (based on matching wildcard patterns). For information on quota pools, see *Managing Quotas*.

Policy Context Properties

Policy context properties are related to policy contexts. The following conditions are available.

Condition **where the policy context property name exists**

Parameters where the policy context property *property-name accessibility*

property-name — String.

accessibility — One of the following:

- **exists**
- **does not exist**

Description Triggers a policy based on whether or not the specified policy context property exists.

Condition **where the policy context property name is numerically equal to value**

Parameters where the policy context property *property-name* is numerically *operator value*

property-name — String.

operator — See common parameters.

value — Integer value in the inclusive range of -9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 (that is, -2^{63} to $2^{63}-1$).

Description Triggers a policy based on a numerical comparison between the specified policy context property value and a specified value.

Condition **where the policy context property name matches one of `value(s)`**

Parameters where the policy context property *property-name matches-op 'match-list'*

property-name — String.

matches-op — See common parameters.

match-list — See common parameters.

Description Triggers a policy based on whether the specified policy context property value matches a list of specified values (based on matching wildcard patterns).

Time-of-Day Conditions

Time-of-Day conditions are related to the time at which the policy rules are being executed. The following conditions are available.

Condition **where the current time is between start time and end time using configured local time**

Parameters where the current time *operator-binary* between *time-of-day* and *time-of-day* using *time-zone*

operator-binary — See common parameters.

time-of-day — A time, in the format of "*HH*:*MM*," where "*HH*" is a number in the range from 0 to 23.

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device
- **system local time** — Calculate the time from the location of this MPE device
- **user local time** — Calculate the time from the location of the user equipment

Description Triggers a policy based on time. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Condition **where the current time is within the specified time period(s)**

Parameters where the current time *operator-binary* within the *time-period* time periods

operator-binary — One of the following:

- **is**
- **is not**

time-period — Names of one or more time periods that are defined in the CMP.

Description Triggers a policy based on the time periods that are defined within the CMP.

Condition **where today is a week day using configured local time**

Parameters where today is a week day using *time-zone*

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device
- **system local time** — Calculate the time from the location of this MPE device
- **user local time** — Calculate the time from the location of the user equipment

Description Triggers a policy based on the day of the week. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Condition **where today is a weekend day using configured local time**

Parameters where today is a weekend day using *time-zone*

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device

- **system local time** — Calculate the time from the location of this MPE device
- **user local time** — Calculate the time from the location of the user equipment

Description Triggers a policy based on the day of the week. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Condition **where today is day using configured local time**

Parameters where today is *day-of-week* using *time-zone*

day-of-week — One or more of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device
- **system local time** — Calculate the time from the location of this MPE device
- **user local time** — Calculate the time from the location of the user equipment

Description Triggers a policy based on the day of the week. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Actions Available for Writing Policy Rules

The policy wizard supports a large number of actions that can be used for constructing policy rules. There are two types of actions:

- **Mandatory policy-processing actions** — This action defines what should happen when the current policy is through executing. When you are creating a policy rule in the policy wizard, these actions are displayed at the top of the list of available actions with a radio button that forces you to select only one of these actions.
- **Optional actions** — This action contains a list of optional actions that you can add to your policy rule. These actions are then executed when the policy rule's conditions have been met. You can select anywhere from 0 to all of these optional actions, although each action is limited, so that it can be executed only once per policy rule.

In the same way that you can customize the conditions by editing parameters, many of these actions can be customized by specifying parameter values as well. Actions are listed in alphabetical order. Actions also may be affected by the current mode; hence, some of the actions documented here may not be available in your policy wizard.

Mandatory Policy-Processing Actions

Policy-processing actions define what the Policy Engine should do when the current policy is through executing. The following are the mandatory policy-processing actions; one of these actions must be selected in each policy.

Action	**accept message**
Description	After executing the current policy rule, the Policy Engine continues with the normal processing of the protocol message but no further policy rules are evaluated.
Action	**break from policy level**
Description	Stop evaluating the current policy and continue policy evaluation with the next policy at the parent's level. You should use this action only in reference policies.
Action	**continue processing message**
Description	After executing the current policy rule, the Policy Engine continues with the next policy rule.
Action	**reject message**
Description	After executing the current policy rule, the Policy Engine terminates all policy-rule processing and rejects the current protocol message. The specific interpretation of “rejecting” the message varies depending on the associated protocol. For most application-level requests this translates into some type of error being sent back to the application.
Action	**skip to next device**
Description	Stop evaluating policies for the current device and continue policy evaluation with the next device. If there is no next device, policy execution ends.
Action	**skip to next flow**
Description	Stop evaluating policies for the current flow and continue policy evaluation with the next flow. If there is no next flow, evaluation continues with the next device; if there is no next device, policy execution ends.

Optional Actions

The following optional actions are available.

Action	**Add custom grouped AVP name and send always**
Parameters	add custom grouped AVP *name* and send *always* *name* — Select an existing grouped third party AVP Name and Vender ID, or an AVP name from an existing Policy Table. *always* — Select send mode: • **always** • **unless rejected**

- **if rejected**
- or send mode from an existing **Policy Table**

Description Add or send new custom grouped AVP to the current reply. A condition can be set specifying that the AVP is *always* set to send mode. If you are defining a new grouped third party AVP with members, the grouped AVP has to appear first in the policy. If you are adding a new member AVP that does not have its parent AVP added yet, the policy attempts to locate this grouped AVP in the rest of the policy. If you are including a grouped AVP multiple times in the same message, you have to follow the order in which it appears in the message.

Action **Advanced: set values for QoS and Charging parameters to specified value**

Parameters Advanced: set values for QoS and Charging parameters to *profile-param*

profile-param — Names of profile parameters that are derived from internal representations of protocol messages. This list is lengthy and subject to change as new protocols are supported, and therefore is not given here. The CMP policy wizard includes a customized dialog to help you in the selection of valid values. For the specific meaning of the fields it may be necessary to consult protocol specifications.

Description Overwrites the corresponding settings in the current protocol message. If you specify settings that are not relevant in the current protocol message, they are ignored. If you select Diameter Enforcement Session Event Triggers, you are presented with another dialog where you can select ECGI_CHANGE and TAI_CHANGE, in addition to the list of previous triggers.

Action **apply specified profile(s) to all flows in the request**

Parameters apply *traffic-profile* to all flows in the request

traffic-profile — One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

Description This parameter allows you to choose different traffic profiles to apply to different types of calls.

Action **apply specified profile(s) to request**

Parameters apply *traffic-profile* to request

traffic-profile — One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

Description Overwrites the corresponding settings in the current protocol message. If multiple traffic profiles are selected they are applied in the order in which they are specified. If the traffic profile contains settings that are not relevant in the current protocol message, then they are simply ignored.

Action **apply specified profile(s) to selected specified type(s) flows in the request**

Parameters apply *traffic-profile* to selected *specified type(s)* flows in the request

traffic-profile — One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

specified type(s) — One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Description Overwrites the corresponding settings in the protocol messages of the specified type. If multiple traffic profiles are selected they are applied in the order in which they are specified. If the traffic profile contains settings that are not relevant in the current protocol message, then they are simply ignored. The second parameter lets you choose different traffic profiles to apply to different types of call.

Action **clear alarm with severity `severity level`, id `unique alarm identifier` and message `message text`**

Parameters clear alarm with severity `*level*`, id `*alarm-id*` and message `*message*`

level — One of the following, used to determine which alarm ID is cleared:

- **Critical** (ID 74000)
- **Major** (ID 74001)
- **Minor** (ID 74002)

alarm-id — The alarm ID. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

Description Clears an alarm on the CMP Active Alarms display containing the specified severity level and message text. This notification is written to the Alarm History Report with severity Clear. To be cleared, a notification must be uniquely identified by severity and alarm ID. For more information, see *Viewing Active Alarms*.

Action **disable forwarding to next hop gateway**

Description Disables forwarding to the next hop gateway.

Action **disable monitoring key**

Parameters disable *mon-key*

mon-key — Name(s) of a monitoring key.

Description Disables usage monitoring from the PCEF. This sets the value of the Usage-Monitoring-Information AVP sent to the MPE device to USAGE_MONITORING_DISABLED. The MPE device will send a usage report. See *Managing Monitoring Keys* for information on monitoring keys.

Action **disable VLAN tagging**

Description Disables VLAN tagging.

Action **enable forwarding to next hop gateway with address none**

Parameters enable forwarding to next hop gateway with address *ip-address*

ip-address — Gateway address in IPv4 or IPv6 format.

Description Forwards to the next hop gateway with the specified IP address.

Action **enable subscription for notification of user profile changes**

Description The MPE device subscribes to an SPR system for notification of user profile changes.

Action **enable subtracting usage from select quota for monitoring key**

Parameters *volume-type* subtracting usage from *quota-name* for *mon-key*

volume-type — One of the following:

- **enable** (the default)
- **disable**

quota-name — Name(s) of quota defined in the CMP.

mon-key — Name(s) of a monitoring key.

Description Allows or disallows subtraction of the usage reported by the specified monitoring key(s) from the specified quota(s). See *Managing Quotas* for information on quotas. See *Managing Monitoring Keys* for information on monitoring keys.

Example In this example, to implement a free promotion, quota granted for a video session is subtracted from the total used at the session level:

```
where the request is creating a new session
   install video PCC rule(s) for session
   grant total volume to 100 percent used for video1 using key2
   grant total volume to 100 percent used for quota1
enable subtracting usage from quota1 for key2
```

Action **enable VLAN tagging with Id specified**

Parameters enable VLAN tagging with Id *id*

id — VLAN ID

Description Enables VLAN tagging.

Action **establish traffic detection session using the IP-CAN TDF information**

Parameters None.

Description On a IP-CAN session establishment, the policy action will trigger a TSR command that is sent to the TDF device. This information is received in the TDF-information AVP within the IP-CAN session request.

Action **establish traffic detection session with select network element identity**

Parameters establish traffic detection session with *tdf*

tdf — one or more TDF network elements defined in the CMP database.

Description On a IP-CAN session establishment, the policy action will trigger a TSR command that is sent to the selected TDF device to establish an Sd session.

Action **evaluate policy group select policy group**

Parameters evaluate policy group *group-name*

group-name — Name of a policy group defined in the CMP.

Description If the conditions evaluates to true, evaluate the rules in a policy group. When you click on the **select policy group** parameter, a pop-up window opens so you can select an existing policy group.

Action **evaluate policy select policy**

Parameters evaluate policy *policy-name*

policy-name — Name of a policy defined in the CMP.

Description If the conditions evaluate to true, evaluate a policy. When you click on the **select policy** parameter, a pop-up window opens, giving you the choice of selecting an existing policy or creating a new policy. If you click **Create**, a new Policy Wizard tab opens so you can create the new policy. When you save the new policy, it is added to the list of policies available for selection at this point.

Action **grant # bytes for quota**

Parameters grant *number* bytes for quota

number — See common parameters.

Description Grants a user the specified number of bytes for the requested service. See *Managing Quotas* for information on quotas.

Action **grant # percent in service-specific units for quota**

Parameters grant *extended-percent* percent in service-specific units for quota

extended-percent — See common parameters.

Description Grants a user the specified percentage of the service-specific unit limit for the requested service.

Action **grant # percent in time for quota**

Parameters grant *extended-percent* percent in time for quota

extended-percent — See common parameters.

Description Grants a user the specified percentage of the initial time limit (in seconds) for the requested service.

Action **grant # percent in volume for quota**

Parameters grant *extended-percent* percent in volume for quota

extended-percent — See common parameters.

Description Grants a user the specified percentage of their volume limit (in bytes) for the requested service.

Action **grant # percent of select type for select quota**

Parameters grant *number* percent of *type* for *quota-name*

number — See common parameters.

type — One of the following:

- **Time**
- **Volume**
- **Service Specific**

quota-name — Names of quotas defined in the CMP.

Description Provisions the usage threshold to the specified percentage of time, volume, or service-specific quantity for the selected quota profile(s). See *Managing Quotas* for information on quotas.

Example

```
grant 100 percent of remaining on Volume for
GoldDailyVol,GoldWeeklyVol,GoldMonthlyVol
```

Action **grant # percent of select units for select quota**

Parameters grant *number* percent of *unit* for *quota-name*

number — See common parameters.

unit — One of the following:

- **Seconds**
- **Bytes**
- **Service Specific**

quota-name — Names of quotas defined in the CMP.

Description Provisions the usage threshold to the specified percentage of units for the selected quota profile(s). See *Managing Quotas* for information on quotas.

Example

```
grant 40 percent of Bytes for DailyVol,MonthlyVol
```

Action **grant # seconds for quota**

Parameters grant *number* seconds for quota

number — See common parameters.

Description Grants a user the specified amount of time (in seconds) for the requested service. See *Managing Quotas* for information on quotas.

Action **grant # service-specific units for quota**

Parameters grant *number* service-specific units for quota

number — See common parameters.

Description Grants a user the specified service-specific units for the requested service. See *Managing Quotas* for information on quotas.

Action **grant session time limit to # percent of select quota**

Parameters grant session time limit to *extended-percent* percent of *quota-name*

extended-percent — See common parameters.

quota-name — Name of quota defined in the CMP database.

Description Provisions the session time limit based on a percentage of the time limit, retrieved from the up to five, for the named quota profile. See *Managing Quotas* for information on quotas.

Action **grant total volume to # bytes for select quota**

Parameters grant *volume-type* volume to *number* bytes for *quota-name*

volume-type — One of the following:

- **total** (the default)
- **uplink**
- **downlink**

number — See common parameters.

quota-name — Name of quota defined in the CMP database.

Description Provisions the session volume limit in bytes for the named quota profile. See *Managing Quotas* for information on quotas.

Action **grant total volume to # bytes of select quota using monitoring key**

Parameters grant *volume-type* volume to *number* bytes of *quota-type* using *mon-key*

volume-type — One of the following:

- **total** (the default)
- **uplink**
- **downlink**

number — See common parameters.

quota-type — One of the following:

- **used** (the default) — Calculates the quota to grant by subtracting the specified amount in bytes from the initial quota limit minus the quota used so far.
- **initial** — Calculates the quota to grant by subtracting the specified amount in bytes from the initial quota limit.

mon-key — Name(s) of a monitoring key.

Description Allows quota profiles to be associated with one or more monitoring keys. This action can be used at the session and rule levels. If two policy actions grant usage for the same monitoring key or usage instance, the last action takes precedence, unless an action grants uplink volume followed by an action that grants downlink volume (or vice versa), which case the actions are grouped as one action when the message is processed. A policy that grants quota for a monitoring key will overwrite any previous grant of quota for that same monitoring key. This includes any subtraction previously enabled for the same monitoring key. See *Managing Quotas* for information on quotas. See *Managing Monitoring Keys* for information on monitoring keys.

Action **grant total volume to # percent used for select quota**

Parameters grant *volume-type* volume to *extended-percent* percent *quota-type* for *quota-name*

volume-type — One of the following:

- **total** (the default)
- **uplink**
- **downlink**

extended-percent — See common parameters.

quota-type — One of the following:

- **used** (the default) — Calculates the quota to grant by multiplying the percentage times the initial quota limit minus the quota used so far.
- **initial** — Calculates the quota to grant by multiplying the percentage times the initial quota limit.

quota-name — Name(s) of quota defined in the CMP.

Description Provisions the session volume limit based on a percentage of the volume used, retrieved from the SPR, for the named quota profile. This action can only be used at the session level. See *Managing Quotas* for information on quotas.

Action **grant total volume to # percent used for select quota using monitoring key**

Parameters grant *volume-type* volume to *extended-percent* percent *quota-type* for *quota-name* using *mon-key*

volume-type — One of the following:

- **total** (the default)
- **uplink**
- **downlink**

extended-percent — See common parameters.

quota-type — One of the following:

- **used** (the default) — Calculates the quota to grant by multiplying the percentage times the the initial quota limit minus the quota used so far.
- **initial** — Calculates the quota to grant by multiplying the percentage times the the initial quota limit.

quota-name — Name(s) of quota defined in the CMP.

mon-key — Name(s) of a monitoring key.

Description Allows quota profiles to be associated with one or more monitoring keys. This action can be used at the session and rule levels. If two policy actions grant usage for the same monitoring key or usage instance, the last action takes precedence, unless an action grants uplink volume followed by an action that grants downlink volume (or vice versa), which case the actions are grouped as one action when the message is processed. A policy that grants quota for a monitoring key will overwrite any previous grant of quota for that same monitoring key. This includes any subtraction previously enabled for the same monitoring key. See *Managing Quotas* for information on quotas. See *Managing Monitoring Keys* for information on monitoring keys.

Example

```
where the request is creating a new session
   grant total volume to 100 percent used for Monthly1,Daily1 using
 key1

continue processing message
```

Action **install specified PCC rule(s) for select scope**

Parameters install *pcc-rule* PCC rule(s) for *pcc-rule-scope-install*

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**

Description The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile.

Action **install specified PCC rule(s) for select scope active between start time and end time**

Parameters install *pcc-rule* PCC rule(s) for *pcc-rule-scope-install* active between *start-time* and *end-time*

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**

start-time and *end-time* — Specifies the start and end time for rule to be active. If start time is not specified, the rule becomes active immediately. If end time is not specified, the rule never deactivates. Select either absolute time or relative time for both start-time and end-time:

- **Absolute time but no date** — Specifies the time to start/end in the form HH:mm:ss. The date is calculated to be the minimum future date for that time.
- **Absolute time and date** — Specifies the time and date to start/end in the form YYYY-MM-ddTHH:mm:ss.
- **Relative time** — Specifies the number of hours, minutes, or seconds from the current time to start/end. Variables include:

- Date
- Time
- UTC Offset — select number of hours before or after UTC time to start/end.
- Now — check mark to start/end now.
- Time only — check mark to ignore date selected.

Description The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile, and is active between the specified start and end times.

Action **install specified PCC rule(s) for select scope active within Time Period**

Parameters install *pcc-rule* PCC rule(s) for *pcc-rule-scope-install* active within *time-period*

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**

time-period — Specifies the time period when the rule is active. When that time period begins the rule activates, and when the time period ends the rule deactivates. Select one of the following:

- **Time Period** — Select pre-defined time period
- **Policy Table Field** — Select time-related field from Policy Table selected for this Policy.

Description The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile, and the rule is active for the specified time period. Note that when a Time Period is used in a policy, the user cannot delete that time period.

Action **install specified PCC rule(s) for select scope for specified retry profile active within Time Period**

Parameters install *pcc-rule* PCC rule(s) for *pcc-rule-scope-install* with *retryprofile* active within *time-period*

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**

retryprofile — Name of a retry profile that is defined in the CMP. (See *Managing Retry Profiles* for more information.)

time-period — Specifies the time period when the rule is active. When that time period begins the rule activates, and when the time period ends the rule deactivates. Select one of the following:

- **Time Period** — Select pre-defined time period
- **Policy Table Field** — Select time-related field from Policy Table selected for this Policy.

Description The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile and the associated retry profile, and the rule is active for the specified time period.

Action **install specified PCC rule(s) for select scope for specified retry profile active between start time and end time**

Parameters install *pcc-rule* PCC rule(s) for *pcc-rule-scope-install* with *retryprofile* active between *start-end-time*

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**

retryprofile — Name of a retry profile that is defined in the CMP. (See *Managing Retry Profiles* for more information.)

start-end-time — Specifies the start and end time for rule to be active. If start time is not specified, the rule becomes active immediately. If end time is not specified, the rule never deactivates. Select either absolute time or relative time for both start-time and end-time:

- **Absolute time but no date** — Specify the time to start/end in the form HH:mm:ss. The date is calculated to be the minimum future date for that time.
- **Absolute time and date** — Specify the time and date to start/end in the form YYYY-MM-ddTHH:mm:ss.
- **Relative time** — Specify the number of hours, minutes, or seconds from the current time to start/end. Variables include:
  - Date
  - Time
  - UTC Offset — select number of hours before or after UTC time to start/end.

- Now — check mark to start/end now.
- Time only — check mark to ignore date selected.

Description The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile and the associated retry profile, and is active between the specified start and end times.

Action **install specified PCC rule(s) for select scope with specified retry profile**

Parameters install *pcc-rule* PCC rule(s) for *pcc-rule-scope-install* with *retryprofile*

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**

retryprofile — Name of a retry profile that is defined in the CMP. (See *Managing Retry Profiles* for more information.)

Description The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile and the associated retry profile.

Action **mark request AVP name as failed if exists and send always**

Parameters mark request AVP *name* as failed if exists and send *always*

name — String representing existing AVP name, entered in this format -- AVP Name:VendorID, or for nested AVP names in an AVP group, entered in this format -- AVP Name 1:VendorID.AVP Name 2:VendorID. An AVP name can also be selected from an existing Policy Table. There is also the option to evaluate as an expression (click to select check box).

always — Send mode:

- **always** (the default)
- **unless rejected**
- **if rejected**
- or send mode from an existing Policy Table

Description Marks a request AVP as failed in the reply message, and notifies the opposite peer of the failed AVP validation. This action supports both loaded base Diameter AVPs and third-party AVPs.

Action **re-authorize all credit control sessions associated with User**

Description Triggers reauthorization for PCEF sessions for all the user's sessions.

Action **re-authorize all PCEF sessions associated with select scope**

Parameters re-authorize all PCEF sessions associated with *pcef-scope-install*

pcef-scope-install— One of the following:

- **IP-CAN session**
- **user**

Description Triggers reauthorization for PCEF sessions, either within the IP-CAN session associations (that is, all Gx sessions sharing the same IP address and APN) or for all the user's sessions (that is, all Gx sessions sharing the same user ID). Each reauthorization request contains the original event that triggered the reauthorization action, so information from this event can be evaluated by the policy engine during the evaluation of the request. For example, an event trigger received in a CCR on one interface, such as RAT_CHANGE, can be used in the evaluation of the reauthorization request triggered by this CCR. This action is valid regardless of whether Gx correlation is enabled or disabled.

Action **release all credit control sessions associated with User**

Description Triggers release of credit control sessions for all the user's sessions.

Action **release all PCEF sessions associated with select scope**

Parameters release all PCEF sessions associated with *pcef-scope-install*

pcef-scope-install— One of the following:

- **IP-CAN session**
- **user**

Description Triggers release of PCEF sessions, either within the IP-CAN session associations (that is, all Gx sessions sharing the same IP address and APN) or for all the user's sessions (that is, all Gx sessions sharing the same user ID).

Action **release the session**

Description Releases the session.

Action **remove all policy context properties**

Description Removes all subscriber properties in the SPR.

Action **remove all the subscriber or pool properties and save always**

Parameters remove all the *subscriber* properties and save *save-mode*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

save-mode — One of the following:

- **always** (the default)
- **unless rejected**

Description Deletes all the properties for a subscriber or pool quota from the SPR. You can specify that the properties are not deleted if the policy rejects the message.

Action **remove custom AVP name from reply always**

Parameters remove custom AVP *name* from reply *always*

name — An existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

always — Send mode:

- **always** (the default)
- **unless rejected**
- **if rejected**
- or send mode from an existing Policy Table

Description Removes the custom AVP name previously set from the reply message.

Action **remove PCC rule type(s) select type(s) of rules for select scope**

Parameters remove PCC rule type(s) *pcc-rule-type* for *pcc-rule-scope-install*

pcc-rule-type — One or more of the following:

- **none**
- **predefined**
- **predefined base**
- **dynamically provisioned**
- **all**

pcc-rule-scope-install — One of the following:

- **flow**
- **session**
- **all**

Description Removes the policy and charging control rules from the current flow/session based on their type.

Action **remove policy context property name**

Parameters remove policy context property *property-name*

property-name — String. May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

Description Removes a subscriber property in the SPR.

Action **remove specified PCC rule(s)**

Parameters remove *pcc-rule* PCC rule(s)

pcc-rule — Names of policy and charging control profiles that are defined in the CMP. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Description Removes the PCC rules from the current flow/session.

Action **remove the subscriber or pool property name and save always**

Parameters remove the *subscriber* property *property-name* and save *save-mode*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

save-mode — One of the following:

- **always** (the default)
- **unless rejected**

Description Deletes a subscriber or quota pool property from the SPR. You can specify that the property is not deleted if the policy rejects the message.

Example

```
remove the FamilyPlanGold property stc-approved and save unless
rejected
```

Action **request usage report for monitoring key**

Parameters request usage report for *mon-key*

mon-key — Name of a monitoring key.

Description Requests a usage report from the PCEF. This sets the value of the Usage-Monitoring-Information AVP sent to the MPE device to USAGE_MONITORING_REPORT_REQUIRED. See *Managing Monitoring Keys* for information on monitoring keys.

Action **reset all quota usage**

Description Resets all quotas for the subscriber.

Action **reset usage for select quota**

Parameters reset usage for *quota-name*

quota-name — Name of quota defined in the CMP.

Description Resets the selected quota. See *Managing Quotas* for information on quotas.

Action **revalidate the session at datetime using configured local time**

Parameters revalidate the session at *datetime* using *time-zone*

datetime — A policy rule variable or a timestamp in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*+*UTCoffset*. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device
- **system local time** — Calculate the time from the location of this MPE device

- **user local time** — Calculate the time from the location of the user equipment

Description Revalidates the session at the specified time. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Example

```
revalidate the session at {User.State.end-time} using configured
local time
```

Action **send notification to syslog with `message text` and severity `severity level`**

Parameters send notification to syslog with `*message*` and severity `*level*`

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

level — The sevlog severity. One of the following:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

Description Writes a message to the syslog file containing the specified message text and severity level.

Note: Policies written before V7.5 that used the action **send alert with `text` and severity `severity level`** will be converted to use this action instead, which will send a notification to syslog instead of an alarm to the CMP.

Action **send notification to trace log with `message text` and severity `severity level`**

Parameters send notification to trace log with `*message*` and severity `*level*`

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

level — One of the following:

- **Emergency** (ID 4560)
- **Alert** (ID 4561)
- **Critical** (ID 4562)
- **Error** (ID 4563)
- **Warning** (ID 4564)
- **Notice** (ID 4565)
- **Info** (ID 4566)

- **Debug** (ID 4567)

Description Sends a message to the trace log containing the specified message text and at the specified severity level. If the configured minimum notification severity level is higher than that specified in the policy action, then the policy action does not generate the notification.

Note: Policies written before V7.5 that used the action **write `text` to the log file** will be converted to use this action instead, with the severity Info.

Action **send SMS `specified` to `default` destination address, `default` TON and `default` NPI from `default` source address, `default` TON and `default` NPI. Request delivery receipt `default`.**

Parameters send SMS `*message*` to `*dest_address*` destination address, `*ton*` TON and `*npi*` NPI from `*source_address*` source address, `*ton*` TON and `*npi*` NPI. Request delivery receipt `*receipt*`.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

dest_address — String. If not the default, this overrides the configured address. You can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile. A maximum of five comma-separated values can be entered.

ton — If not the default, this overrides the configured Type of Number. One of the following:

- **default**
- **UNKNOWN**
- **INTERNATIONAL**
- **NATIONAL**
- **NETWORK SPECIFIC**
- **SUBSCRIBER NUMBER**
- **ALPHANUMERIC**
- **ABBREVIATED**

npi — If not the default, this overrides the configured Number Plan Indicator. One of the following:

- **default**
- **UNKNOWN**
- **ISDN (E163/E164)**
- **DATA (X.121)**
- **TELEX (F.69)**
- **LAND MOBILE (E.212)**
- **NATIONAL**
- **PRIVATE**
- **ERMES**
- **INTERNET (IP)**
- **WAP CLIENT ID**

source_address — String. If not the default, this overrides the configured address.

receipt — One of the following:

- **default** — Use global default configured for this MPE device.
- **No Delivery Receipt** (the default)
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Description

Sends an SMS text message, with the specified text, to the subscriber associated with the message. In SMPP mode, messages can be up to 254 characters long. The default source and destination address, TON, and NPI configured on the MPE device can be used or overridden.

To send notifications to multiple destinations, you can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile. Destinations must all be of the same type; this ensures that the same TON and NPI settings configured in the policy action will apply to all destinations. No transformations are performed on the subscriber's profile data by the MPE device, so custom fields used as alternate destinations must contain values formatted as required by the SMSC. Multivalued fields (LDAP attributes) are not supported.

If the address(es) specified are not available (for example, if a custom field is not populated in the subscriber database), then the global default is used; if the global default is not configured, then the SMS message is sent to the subscriber's MSISDN; if the subscriber's MSISDN cannot be determined, then no SMS message is sent and a trace log alert is generated.

You can request a receipt from the SMSC server, which will be logged in the file SMPP.log, when the message is delivered to the subscriber. You can request a receipt on success, failure, or either. See *Configuring Protocol Options on the Policy Server* for information on configuring delivery receipt default behavior.

Example

```
send SMS `you have reached 80%% of your quota` to
`{User.MSISDN},{User.AltDest1},{User.AltDest2}` destination address,
 `default` TON and `default` NPI from `614` source address, `default`
 TON and `default` NPI. Request delivery receipt `Default`.
```

Action

send SMS `specified` to `default` destination address, `default` TON and `default` NPI from `default` source address, `default` TON and `default` NPI on user billing day. Request delivery receipt `default`.

Parameters

send SMS `*message*` to `*dest_address*` destination address, `*ton*` TON and `*npi*` NPI from `*source_address*` source address, `*ton*` TON and `*npi*` NPI on user billing day. Request delivery receipt `*receipt*`.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

dest_address — String. If not the default, this overrides the configured address. You can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile.

ton — If not the default, this overrides the configured Type of Number. One of the following:

- **default**
- **UNKNOWN**
- **INTERNATIONAL**
- **NATIONAL**
- **NETWORK SPECIFIC**
- **SUBSCRIBER NUMBER**
- **ALPHANUMERIC**
- **ABBREVIATED**

npi — If not the default, this overrides the configured Number Plan Indicator. One of the following:

- **default**
- **UNKNOWN**
- **ISDN (E163/E164)**
- **DATA (X.121)**
- **TELEX (F.69)**
- **LAND MOBILE (E.212)**
- **NATIONAL**
- **PRIVATE**
- **ERMES**
- **INTERNET (IP)**
- **WAP CLIENT ID**

source_address — String. If not the default, this overrides the configured address.

receipt — One of the following:

- **default** — Use global default configured for this MPE device.
- **No Delivery Receipt** (the default)
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Description

Sends an SMS text message, with specified text, to the subscriber associated with the message on the subscribers billing day. In SMPP mode, messages can be up to 254 characters long. The default source and destination address, TON, and NPI configured on the MPE device can be used or overridden.

To send notifications to multiple destinations, you can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile. Destinations must all be of the same type; this ensures that the same TON and NPI settings configured in the policy action will apply to all destinations. No transformations are performed on the subscriber's profile data by the MPE device, so custom fields used as alternate destinations must contain values formatted as required by the SMSC. Multivalued fields (LDAP attributes) are not supported.

If the address(es) specified are not available (for example, if a custom field is not populated in the subscriber database), then the global default is used; if the global default is not configured, then the SMS message is sent to the subscriber's MSISDN;

if the subscriber's MSISDN cannot be determined, then no SMS message is sent and a trace log alert is generated.

You can request a receipt from the SMSC server, which will be logged in the file SMPP.log, when the message is delivered to the subscriber. You can request a receipt on success, failure, or either. See *Configuring Protocol Options on the Policy Server* for information on configuring delivery receipt default behavior.

Example

```
send SMS `you have reached 80%% of your quota` to
`{User.MSISDN},{User.AltDest1},{User.AltDest2}` destination address,
 `default` TON and `default` NPI from `614` source address, `default`
 TON and `default` NPI on user billing day. Request delivery receipt
 `Default`.
```

Action

send SMS `specified` to `default` destination address from `default` source address. Request delivery receipt `default`.

Parameters

send SMS `*message*` to `*dest_address*` destination address from `*source_address*` source address. Request delivery receipt `*receipt*`.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

dest_address — String. If not the default, this overrides the configured address. You can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile.

source_address — String. If not the default, this overrides the configured address.

receipt — One of the following:

- **default** — Use global default configured for this MPE device.
- **No Delivery Receipt** (the default)
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Description

Sends an SMS text message, with the specified text, to the subscriber associated with the message. In SMPP mode, messages can be up to 254 characters long. The default source and destination address can be used or overridden.

To send notifications to multiple destinations, you can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile. Destinations must all be of the same type; this ensures that the same TON and NPI settings configured in the policy action will apply to all destinations. No transformations are performed on the subscriber's profile data by the MPE device, so custom fields used as alternate destinations must contain values formatted as required by the SMSC. Multivalued fields (LDAP attributes) are not supported.

If the address(es) specified are not available (for example, if a custom field is not populated in the subscriber database), then the global default is used; if the global default is not configured, then the SMS message is sent to the subscriber's MSISDN; if the subscriber's MSISDN cannot be determined, then no SMS message is sent and a trace log alert is generated.

You can request a receipt from the SMSC server, which will be logged in the file SMPP.log, when the message is delivered to the subscriber. You can request a receipt on success, failure, or either. See *Configuring Protocol Options on the Policy Server* for information on configuring delivery receipt default behavior.

Example

```
send SMS `you have reached 80%% of your quota` to
`{User.MSISDN},{User.AltDest1},{User.AltDest2}`
destination address from `614` source address. Request delivery
receipt `Default`.
```

Action

send SMS `specified` to `default` destination address from `default` source address on user billing day. Request delivery receipt `default`.

Parameters

send SMS `*message*` to `*dest_address*` destination address from `*source_address*` source address on user billing day. Request delivery receipt `*receipt*`.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

dest_address — String. If not the default, this overrides the configured address. You can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile.

source_address — String. If not the default, this overrides the configured address.

receipt — One of the following:

- **default** — Use global default configured for this MPE device.
- **No Delivery Receipt** (the default)
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Description

Sends an SMS text message, with specified text, to the subscriber associated with the message on the subscriber's billing day. In SMPP mode, messages can be up to 254 characters long. The default source and destination address can be used or overridden.

To send notifications to multiple destinations, you can specify *dest_address* as one or more comma-separated static values, or as one or more comma-separated references to custom fields in the subscriber profile. Destinations must all be of the same type; this ensures that the same TON and NPI settings configured in the policy action will apply to all destinations. No transformations are performed on the subscriber's profile data by the MPE device, so custom fields used as alternate destinations must contain values formatted as required by the SMSC. Multivalued fields (LDAP attributes) are not supported.

If the address(es) specified are not available (for example, if a custom field is not populated in the subscriber database), then the global default is used; if the global default is not configured, then the SMS message is sent to the subscriber's MSISDN; if the subscriber's MSISDN cannot be determined, then no SMS message is sent and a trace log alert is generated.

You can request a receipt from the SMSC server, which will be logged in the file SMPP.log, when the message is delivered to the subscriber. You can request a receipt on success, failure, or either. See *Configuring Protocol Options on the Policy Server* for information on configuring delivery receipt default behavior.

Example

```
send SMS `you have reached 80%% of your quota` to
`{User.MSISDN},{User.AltDest1},{User.AltDest2}` destination address
 from `614` source address on user billing day. Request delivery
receipt `Default`.
```

Action **send SMS `specified` to user. Request delivery receipt `default`.**

Parameters send SMS `*message*` to user. Request delivery receipt `*receipt*`.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

receipt — One of the following:

- **default** — Use global default configured for this MPE device.
- **No Delivery Receipt** (the default)
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Description Sends an SMS text message, with specified text, to the subscriber associated with the message. In SMPP mode, messages can be up to 254 characters long.

You can request a receipt from the SMSC server, which will be logged in the file SMPP.log, when the message is delivered to the subscriber. You can request a receipt on success, failure, or either. See *Configuring Protocol Options on the Policy Server* for information on configuring delivery receipt default behavior.

Example

```
send SMS `you have reached 80%% of your quota` to user. Request
delivery receipt `Default`.
```

Action **send SMS `specified` to user on their Billing Day. Request delivery receipt `default`.**

Parameters send SMS `*message*` to user on their Billing Day. Request delivery receipt `*receipt*`.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

receipt — One of the following:

- **default** — Use global default configured for this MPE device.
- **No Delivery Receipt** (the default)
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Description Sends an SMS text message, with specified text, to the subscriber associated with the message on the subscriber's billing day. In SMPP mode, messages can be up to 254 characters long.

You can request a receipt from the SMSC server, which will be logged in the file SMPP.log, when the message is delivered to the subscriber. You can request a receipt

on success, failure, or either. See *Configuring Protocol Options on the Policy Server* for information on configuring delivery receipt default behavior.

Action

send SMTP message with the following text/plain content:

To: to_address CC: default BCC: default

From: default Reply-To: default

Subject: subject

Text: message content

Signature: default

Parameters

send SMTP message with the following *format* content:

To: *to_address* CC: *cc_address* BCC: *bcc_address*

From: *from_address* Reply-To: *reply_address*

Subject: *subject*

Text: *message*

Signature: *signature*

format — One of the following:

- **text/plain** (the default) — The email is in plain-text format.
- **text/html** — The email includes HTML formatting.

to_address — String. If not the default, this overrides the configured address. You can specify up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile.

cc_address — String. If not the default, this overrides the configured address. You can specify up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile.

bcc_address — String. If not the default, this overrides the configured address. You can specify up to five comma-separated static values, or up to five comma-separated references to custom fields in the subscriber profile.

from_address— String. The address of the author who sent the mail.

Note: You may not necessarily want the reply to come back from this address. This can be configured globally to a default value.

reply_address — String. If not the default, this overrides the configured address.

subject — String.

message — String. Body of the message.

signature — String. If not the default, this overrides the configured signature block.

Description

Sends an email message, with the specified text and signature block, to the subscriber associated with the address. The message is sent through an SMS Relay (SMSR) interface.

To send email to multiple destinations, you can specify up to five addresses (any combination of *to_address*, *cc_address*, or *bc_address*) as comma-separated static values, or as comma-separated references to custom fields in the subscriber profile. You can specify up to five addresses. Destinations must all be of the same type. No transformations are performed on the subscriber's profile data by the MPE device, so custom fields used as alternate destinations must contain values formatted as required by the SMSR. Multivalued fields (LDAP attributes) are not supported.

If the address(es) specified are not available (for example, if a custom field is not populated in the subscriber database), then the global default is used; if the global default is not configured, then no SMTP message is sent and an SMTP log alert is generated. See *Configuring Protocol Options on the Policy Server* for information on configuring SMTP default values.

Action **set alarm with severity `severity level`, id `unique alarm identifier` and message `message text`**

Parameters set alarm with severity `*level*`, id *alarm-id*` and message `*message*`

level — One of the following:

- **Critical** (ID 74000)
- **Major** (ID 74001)
- **Minor** (ID 74002)

alarm-id — The alarm ID. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

message — String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

Description Sends an alarm to the CMP containing the specified severity level and message text. This alarm is written to the Alarm History Report, and will appear in the Active Alarms display for one hour, until cleared, or unless the server fails over, whichever comes first. Alarms generated by policy actions do not affect the HA score of a server, and will not cause a failover. For more information, see *Viewing Active Alarms*.

Action **set authorization validity time to # seconds**

Parameters set authorization validity time to *seconds* seconds

seconds — See common parameters.

Description Sets the authorization expiration time (in seconds) after which the enforcement device requests re-authorization from the MPE device for the requested user's service.

Action **set authorization validity time to datetime**

Parameters set authorization validity time to *datetime*

datetime — Either the local date-time **now** (the default) or a timestamp in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*+*UTCoffset*.

Description Sets the authorization expiration time (to the quarter hour) after which the enforcement device requests re-authorization from the MPE device for the requested user's service.

Action **set authorization validity time to time on day using configured local time**

Parameters set authorization validity time to *time* on *day-of-week* using *time-zone*

time — A time, in the format *hh*:*mm* (limited to 15-minute intervals).

day-of-week — One or more of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

time-zone — One of the following:

- **CONFIGURED LOCAL TIME** (the default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location of the user equipment

Description Sets the authorization expiration time (to the quarter hour) after which the enforcement device requests re-authorization from the MPE device for the requested user's service. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Action **set charging server(s) for the IP-CAN session to specified values**

Parameters set charging server(s) for the IP-CAN session to *charging-server-name*

charging-server-name — Names of charging servers that are defined in the CMP.

Description Sets the charging servers, as specified. To define a charging server, see *Managing Charging Servers*.

Action **set custom AVP name value to the policy context property name**

Parameters set custom AVP *avp-name* value to the policy context property *property-name*

avp-name — An existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

property-name — String that represent the policy context property.

Description Makes the AVP value accessible throughout the policy context so other policies can access this AVP value as a context property. Note that the context property variable will be set only if this AVP exists in the request and its value is not null.

Action **set custom AVP name value to the user property name and save always**

Parameters set custom AVP *avp-name* value to the user property *property-name* and save *always*

avp-name — An existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

property-name — String that represent the user property; maximum of 255 characters can be entered.

always — Select send mode:

- **always**
- **unless rejected**
- send mode from an existing **Policy Table**

Description Sets an AVP value as a User object property to persist between sessions.

Action **set external field to # percent of select type for selected quota**

Parameters set *field* to *value* percent of *type* for *quota-name* quota

field — String name of field in external database.

value — String value of field in external database.

type — One of the following:

- **service-specific**
- **time**
- **total volume**

quota-name — Name(s) of quotas defined in the CMP.

Description Sets a field in an external database to a percentage of the time, total volume, or service-specific quota of one or more selected quotas. This can be an LDAP server or an SPR. The MPE device on which this policy is executed must have write access to the database, and the external field must be defined on the MPE device. For more information, see *Configuring Data Source Interfaces*. See *Managing Quotas* for information on quotas.

Action **set external field to `value`**

Parameters set *field* to `value`

field — String name of field in external database.

value — String value of field in external database. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

Description Sets the value of a field in an external database. This can be an LDAP server or an SPR. The MPE device on which this policy is executed must have write access to the database, and the external field must be defined on the MPE device. For more information, see *Configuring Data Source Interfaces*.

Example

```
set Quota Volume to `{User.Quota.Gold.volume}`
```

```
set Last Session to `{Date(yyyy-MM-DD hh:mm:ss:SSSZ)}`
```

Action **set policy context property name to value**

Parameters set policy context property *property-name* to *value*

property-name — String. May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

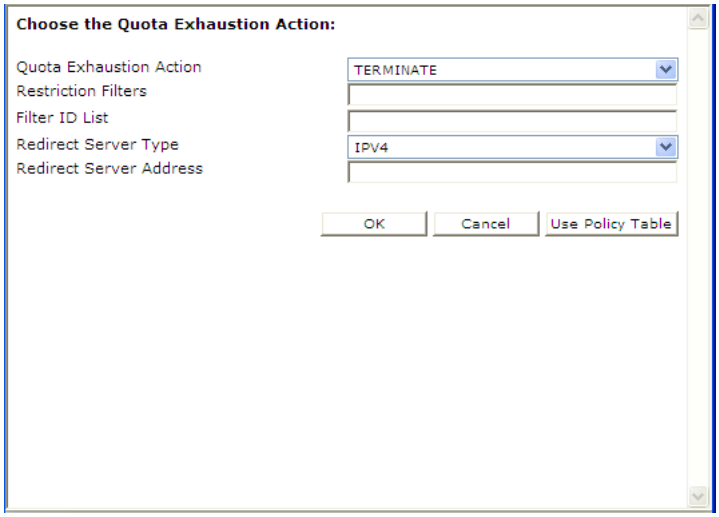
value — String.

Description Sets and saves a subscriber property in the SPR. You can specify that the property is not saved if the policy rejects the message.

Action **set Quota Exhaustion Action to specified**

Parameters set Quota Exhaustion Action to *action*

action — Specifies the action the GGSN takes when a subscriber reaches the quota grant. Selecting this parameter opens a window with the following options:



- **Quota Exhaustion Action** — Select one of the following:
  - **TERMINATE** (the default) — Terminate the subscriber's session. If you select this option, the other options are not applicable.
  - **REDIRECT** — Redirect the session to another server. If you select this option, configure the following additional fields:
    - **Redirect Server Type** — Select **IPV4**, **IPV6**, **URL**, or **SIP URI**
    - **Redirect Server Address** — Type the server address
  - **RESTRICT ACCESS** — If you select this option, additional configuration fields appear:

- **Restriction Filters** — Type a comma-separated list of Diameter IP Filter rules
- **Filter ID List** — Type a comma-separated list of named filters on the GGSN

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

Description Sets the action to take if the subscriber's quota is exhausted. See *Managing Quotas* for information on quotas.

Action **set session revalidation time to # seconds**

Parameters set session revalidation time to *seconds* seconds

seconds — See common parameters.

Description Provisions the session revalidation time to the number of seconds from when the policy executes.

Action **set session revalidation time to time on day using configured local time**

Parameters set session revalidation time to *time* on *day-of-week* using *time-zone*

time — A time, in the format *hh*:*mm* (limited to 15-minute intervals).

day-of-week — One or more of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

time-zone — One of the following:

- **configured local time** (the default) — Calculate the time from the location configured for this MPE device
- **system local time** — Calculate the time from the location of this MPE device
- **user local time** — Calculate the time from the location of the user equipment

Description Sets the session revalidation time (to the quarter hour) after which the enforcement device requests revalidation from the MPE device for the requested user's service. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location.

Action **set the subscriber or pool property name to now + 0 days rounded up with same granularity using configured local time and save always**

Parameters set the *subscriber* property *property-name* to *datetime direction duration granularity* rounded up with *same* granularity using *time-zone* and save *save-mode*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

datetime — Either the local date-time **now** (the default) or a timestamp in the format *yyyy-mm-dd*T*hh*:*mm*:*ss*+*UTCoffset*.

direction — One of the following, indicating future or past:

- **+**
- **-**

duration — Positive integer.

granularity — The calculated date-time is expressed in this granularity:

- **same** (the default)
- **months**
- **days**
- **hours**
- **minutes**

time-zone — One of the following:

- **CONFIGURED LOCAL TIME** (the default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location of the user equipment

save-mode — One of the following:

- **always** (the default)
- **unless rejected**

Description Sets and saves a subscriber or quota pool date-time property in the SPR to either the current date and time or another date-time and an offset. If time-zone information is available from the user equipment, time can be calculated from either the MPE device or the user equipment's location. You can specify that the property is not saved if the policy rejects the message.

Example

```
set the FamilyPlanGold property promotion-end-time to now + 10 days
 rounded up with same granularity using configured local time and
save always
```

Action **set the subscriber or pool property name to now using configured local time and save always**

Parameters set the *subscriber* property *property-name* to *datetime* using *time-zone* and save *save-mode*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

property-name — String.

datetime — Either the local date-time **now** (the default) or a timestamp in the format *yyyy-mm-dd*T*hh*:*mm*+*UTCoffset*.

time-zone — One of the following:

- **CONFIGURED LOCAL TIME** (the default) — Calculate the time from the location configured for this MPE device
- **SYSTEM LOCAL TIME** — Calculate the time from the location of this MPE device
- **USER LOCAL TIME** — Calculate the time from the location of the user equipment

save-mode — One of the following:

- **always** (the default)
- **unless rejected**

Description Sets and saves a subscriber or quota pool timestamp property in the SPR to the current local time or a timestamp. If time-zone information is available from the SPR, time can be calculated from either the MPE device or the SPR device location. You can specify that the property is not saved if the policy rejects the message. For information on quota pools, see *Managing Quotas*.

Example

```
set the FamilyPlanGold property usage-exceeded-time to now using
configured local time and save always
```

Action **set the subscriber or pool property name to user property name + multiple of 0 days rounded up with same granularity and save always**

Parameters set the *subscriber* property *property-name* to user property *property-name direction multiplier duration granularity days* rounded *rounding* with*same* granularity and save *save-mode*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String.

direction — One of the following, indicating future or past:

- **+**
- **-**

multiplier — One of the following:

- **multiple of** (the default): the duration is added repeatedly until the result is in the future
- **exactly**: the duration is added once

duration — Positive integer.

granularity — The offset is expressed in this granularity:

- **days** (the default)
- **months**
- **hours**
- **minutes**

save-mode — One of the following:

- **always** (the default)
- **unless rejected**

Description

Offsets a subscriber or quota pool date-time property, either by the number of time units necessary to move the result into the future or by a specific number of time units. If the value of the first property is in the future, either the exact offset, or one unit of the offset, is added. If the value of the first property is in the past and you specify **+ multiple of**, the duration is repeatedly added until the result is in the future. If the result of the offset is in the past (for example, if you specify **+ exactly 1 day** and the result is still in the past), the action is ignored. You can specify that the property is not saved if the policy rejects the message. If the value of the second property is null then the action is ignored. For information on quota pools, see *Managing Quotas*.

Examples

The following example adds 30 days to the value of the property expiration-date. If the result is in the future, it is saved; if the result is in the past, it is not saved:

```
set the FamilyPlanGold property expiration-date to expiration-date
+ exactly 30 days and save always
```

The following example adds 30 days to the value of the property expiration-date. If the result is in the future, it is saved; if the result is in the past, another offset of 30 days is added, and the result is evaluated again until the result is in the future, at which point the result is saved:

```
set the FamilyPlanGold property expiration-date to expiration-date
+ multiple of 30 days and save always
```

Action

set the subscriber or pool property name to `value` and save always

Parameters

set the *subscriber* property *property-name* to `*value*` and save *save-mode*

subscriber — One of the following:

- **subscriber** (the default) — Individual subscriber
- **pool** — Name of a quota pool defined in the CMP database

property-name — String. May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

value — String. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

save-mode — One of the following:

- **always** (the default)
- **unless rejected**

Description Sets and saves a subscriber or quota pool property in the SPR. You can specify that the property is not saved if the policy rejects the message. For information on quota pools, see *Managing Quotas*.

Example

```
set the FamilyPlanGold property usage-exceeded to `true` and save
always
```

Action **set the user property name to Existing or New custom AVP name and send always**

Parameters set the user property *property-name* to *exists* custom AVP *avp-name* and send *always*

property-name — String. May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

exists — One of the following:

- **Existing or New** (the default)
- **New**

avp-name — Select an existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

always — Select send mode:

- **always**
- **unless rejected**
- **if rejected**
- send mode from an existing **Policy Table**

Description Sets the user property value for an outgoing AVP. If a user property with the corresponding name exists, the AVP will be sent in the reply message.

Action **set threshold to # percent of granted quota for service-specific units**

Parameters set threshold to *extended-percent* percent of *provided-quota* quota for service-specific units

extended-percent — See common parameters.

provided-quota — One of the following:

- **initial**
- **granted** (the default)

Description Sets a threshold, based on a percentage of the volume (in service-specific units) granted to the user, so that the enforcement device (for example, a GGSN) notifies the MPE device when the threshold is reached. This action works on multiple quotas. See *Managing Quotas* for information on quotas.

Action **set threshold to # percent of granted quota for time**

Parameters set threshold to *extended-percent* percent of *provided-quota* for time

extended-percent — See common parameters.

provided-quota — One of the following:

- **initial**
- **granted** (the default)

Description Sets a threshold, based on a percentage of the amount of time (in seconds) retrieved from the SPR, granted to the user, so that the enforcement device (for example, a GGSN) notifies the MPE device when the threshold is reached. This action works on multiple quotas. See *Managing Quotas* for information on quotas.

Action **set threshold to # percent of granted quota for volume**

Parameters set threshold to *extended-percent* percent of *provided-quota* quota for volume

extended-percent — See common parameters.

provided-quota — One of the following:

- **initial**
- **granted** (the default)

Description Sets a threshold, based on a percentage of the volume (in bytes) granted to the user, so that the enforcement device (for example, a GGSN) notifies the MPE device when the threshold is reached. This action works on multiple quotas. See *Managing Quotas* for information on quotas.

Action **set value to Existing or New custom AVP name and send always**

Parameters set *value* to *exists* custom AVP *name* and send *always*

value — Enter string or select string from existing Policy Table that represents third-party non-grouped AVP. Check *Evaluate as expression* to evaluate this value as an expression.

exists — Select type of AVP name:

- **Existing or New** (the default)
- **New**

name — Select an existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

always — Select send mode:

- **always**
- **unless rejected**
- **if rejected**
- or send mode from an existing **Policy Table**

Description Adds the third-party non-grouped AVP to the current Diameter session with the specified value. If a third-party AVP value is set in the current Diameter session, it

	will be sent with the corresponding outgoing message. The value parameter must corresponds to the AVP data type, otherwise this AVP will not be set. If New is selected as the type of AVP name, every time this action is called a new AVP is added to the message, even if the AVP with the same name is already present in the message.
Action	**set volume threshold to # bytes for select quota**
Parameters	set volume threshold to *number* bytes for *quota-name* *number* — See common parameters. *quota-name* — Name of quota defined in the CMP.
Description	Provisions the usage threshold to the specified number of bytes for the selected quota profile. See *Managing Quotas* for information on quotas.

Policy Rule Variables

During policy rule execution within the MPE device, some actions (for example, `send notification`) allow for substitution of policy rule variables with contextual information. Each time the policy rules are evaluated, the unique set of policy rule variables is referred to as the *policy context*. This section summarizes these policy rule variables.

Using Policy Rule Variables

Typically, policy rule variables are used to perform substitution of textual information into a text message that is being used for some type of logging. This is typically done in an action. To use a policy rule variable, insert the variable into the text message when you define the action.

The format of a policy rule variable is as follows:

`“{” name [ “:” default-value ] “}”`

The name can contain the characters A–Z, a–z, 0–9, underscore (_), period (.), and backslash (\).

The following are examples of policy rule variables:

```
{Bandwidth}
{Device.Name}
{Device.Name:UNKNOWN}
```

Basic Policy Rule Variables

Table 8: Basic Policy Rule Variables displays some of the basic policy rule variables that are available.

Under certain circumstances the MPE device can associate additional context information with a request. This information may be used during the policy rule execution. The availability of this information depends on:

- The mode (for example, *Wireless*) in which the MPE device is executing
- Whether the information is provisioned on the MPE device or, if present, a Subscriber Profile Repository (SPR)

- The protocol in use and how much information is available in the request (some protocols have optional information which, if specified, can be used to associate additional information)

There are a number of policy rule variables that can be used to provide information about the device for which a policy rule is being executed. Some of these variables are only available for certain device types, while others are available for all devices.

Table 8: Basic Policy Rule Variables

Variable Name	Description	Modes, Protocols, Device Type
{Policy}	The name of the policy rule that is being executed.	--
{Date}	The date when the policy rule is executed, in the format *MMM*[*M*]/*dd* [/*yyyy*], where *MMM* is "Jan," "Feb," "Mar," ..., or "Dec", and *MM* is "01," "02," "03," ..., or "12."	--
{Time}	The time when the policy rule is executed, in the format *hh*:*mm*:*ss*.*SSS*.	--
{Conditions}	A list of (variable, value) tuples that lists the variables whose values were referenced in the conditions of the policy rule. The list is inserted with one variable per line in the format *variable=value*.	--
{Device}	The name of the device for which the policy rule is being evaluated.	--
{DeviceId}	ID of the device for which the policy rule is being evaluated.	--
{QosDir}	The direction of the flow for which the policy rule is being evaluated, either "Up" or "Down."	--
{Bandwidth}	The DOCSIS type of the flow for which the policy rule is being evaluated: "BES," "NRTP," "RTP," "UGS," or "UGSAD."	--
{Account.AccountId}	The account ID of the account associated with the request.	Wireless
{Account.EndpointId}	The Endpoint ID of the account associated with the request.	Wireless
{Account.Entitlements}		Wireless

Variable Name	Description	Modes, Protocols, Device Type
{Account.UpstreamLimit}	The upstream bandwidth limit of the account associated with the request.	Wireless
{Account.DownstreamLimit}	The downstream bandwidth limit of the account associated with the request.	Wireless
{Account.StaticIpAddresses}		Wireless
{Account.Tier.Name} {AccountTier.Name}	The name of the tier of the account associated with the request.	Wireless
{AccountTier.Entitlements}		Wireless
{Account.Tier.UpstreamLimit} {AccountTier.UpstreamLimit}	The upstream bandwidth limit if the tier of the account associated with the request.	Wireless
{Account.Tier.DownstreamLimit} {AccountTier.DownstreamLimit}	The downstream bandwidth limit if the tier of the account associated with the request.	Wireless
{Application.Name}	The name of the application associated with the request.	Wireless
{Application.LatencySensitivity}		Wireless
{Application.AmIds}		Wireless
{Application.IpAddresses}		Wireless
{Application.Hostnames}		Wireless
{Application.SessionClassIds}		Wireless
{Application.EnforcementPt}		Wireless
{Application.HDThreshold}		Wireless
{Device.Name.}		Wireless
{Element.DownstreamCapacity}		Wireless
{Element.UpstreamCapacity}		Wireless
{Element.BackupHostname}		Wireless
{Element.CapabilitiesSet}		Wireless
{Element.Hostname}		Wireless
{Element.Name}		Wireless
{Element.Subtype}		Wireless
{Element.DiameterIdentities}		Wireless

Variable Name	Description	Modes, Protocols, Device Type
{Element.DiameterRealm}		Wireless
{Element.NasIdentifiers}		Wireless
{Element.OfflineCharging}		Wireless
{Element.OnlineCharging}		Wireless
{Element.PrimaryOfflineChargingServer}		Wireless
{Element.PrimaryOnlineChargingServer}		Wireless
{Element.SecondaryOfflineChargingServer}		Wireless
{Element.SecondaryOnlineChargingServer}		Wireless
{Flow.Usage}		Wireless
{Flow.CurrentOriginalFlowInfo}		Wireless
{Flow.OriginalFlowInfo}		Wireless
{Flow.TranslatedFlowInfo}		Wireless
{Quota.Limit<quota_name>.Volume}		Wireless
{Quota.Limit<quota_name>.Time}		Wireless
{Quota.Limit<quota_name>.ServiceSpecific}		Wireless
{Request.CustomAvpValues}		Wireless
{Request.AdaptorContext}		Wireless
{Request.CreateTimestamp}		Wireless
{Request.EndTimestamp}		Wireless
{Request.EndpointIp}		Wireless
{Request.HandlerKey}		Wireless
{Request.MSTimeZone}		Wireless
{Request.OriginalEvent}		Wireless
{Request.PolicyOutputResourceEvents}		Wireless
{Request.Primary}		Wireless
{Request.ResourceChanges}		Wireless
{Request.SubscriptionsEnabled}		Wireless
{Request.Tasks}		Wireless
{Request.TriggeredByReAuthPolicyAction}		Wireless
{Request.UserIds}		Wireless
{Request.AppId}		Wireless

Variable Name	Description	Modes, Protocols, Device Type
{Request.DestinationHost}		Wireless
{Request.DestinationRealm}		Wireless
{Request.ExplictRoute}		Wireless
{Request.MsgType}		Wireless
{Request.PeerIdentity}		Wireless
{Request.Reason}		Wireless
{Request.ServerAction}		Wireless
{Request.SessionId}		Wireless
{Session.CreatedTimestamp}		Wireless
{Session.EndpointIp}		Wireless
{Session.LastAcceptedTransactionTime}		Wireless
{Session.MSTimeZone}		Wireless
{Session.NextBillingDate}	The next monthly billing date, in the format *MM[M]/dd/yyyy* (for example, MMM/dd/yyyy could result in Oct/24/2011). The date format can be changed by specifying the new format within parentheses; for example, {Session.NextBillingDate (MM/dd} could result in 10/24.	Wireless
{Session.Resources}		Wireless
{Session.Secondary}		Wireless
{Session.ServingMcc}	The serving Mobile Country Code associated with the request.	Wireless
{Session.SessionId}		Wireless
{Session.SubscriberPool}		Wireless
{Session.UsePoolQuota}		Wireless
{User.IMSI}	The IMSI of the subscriber associated with the request.	Wireless
{User.AccountId}	The account ID of the subscriber associated with the request.	Wireless
{User.BillingDay}	The BillingDay value of the subscriber associated with the request.	Wireless

Variable Name	Description	Modes, Protocols, Device Type
{User.BillingType}		Wireless
{User.Custom}		Wireless
{User.*customfield*}	If *customfield* is replaced with the name of a field that is imported from an external data source (such as LDAP), then this is the value of the imported field.	Wireless
{User.DownstreamGuaranteed}		Wireless
{User.DownstreamLimit}		Wireless
{User.E164}	The E164 phone number of the subscriber associated with the request.	Wireless
{User.Entitlements}	The Entitlement value of the subscriber associated with the request.	Wireless
{User.EquipmentIds}		Wireless
{User.IP}	The IP address of the subscriber associated with the request.	Wireless
{User.IsUnknown}		Wireless
{User.MSISDN}	The mobile subscriber ISDN of the subscriber associated with the request.	Wireless
{User.Pool}		Wireless
{User.PoolId}		Wireless
{User.State.*prop*}	The value of a subscriber property, obtained from the SPR, where *prop* is the property name.	Wireless
{User.SIP}	The SIP URI of the subscriber associated with the request.	Wireless
{User.Tier}	The Tier value of the subscriber associated with the request.	Wireless
{User.UpstreamGuaranteed}		Wireless
{User.UpstreamLimit}		Wireless
{User.UserIds}		Wireless
{User.Quota.<quota_name>.Volume}		Wireless
{User.Quota.<quota_name>.Time}		Wireless

Variable Name	Description	Modes, Protocols, Device Type
{User.Quota.<quota_name>ServiceSpecific}		Wireless
{User.State.Deltas}		Wireless
{User.State.EntityStateType}		Wireless
{User.State.New}		Wireless
{User.State.SequenceNumber}		Wireless
{User.State.StateMap}		Wireless
{User.State.UpdateMode}		Wireless
{User.State.Variables}		Wireless
{Device.Name}	The name (as defined in the CMP) of the device.	Any
{Device.UpstreamCapacity}	The upstream bandwidth capacity of the device.	Any
{Device.DownstreamCapacity}	The downstream bandwidth capacity of the device.	Any
{Device.FlowCount}	The number of active flows for the device.	Any
{Element.Name}	The name (as defined in the CMP) of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any
{Element.Hostname}	The hostname (or IP address) of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any
{Element.BackupHostname}	The hostname (or IP address) of the backup network element associated with the current device. If the device is a network element, then	Any

Variable Name	Description	Modes, Protocols, Device Type
	this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	
{Element.UpstreamCapacity}	The upstream bandwidth capacity of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any
{Element.DownstreamCapacity}	The downstream bandwidth capacity of the network element associated with the current device. If the device is a network element, then this is the same as the {Device.Name}. However, if the device is contained within a network element (as is the case with Interfaces, Channels, and so forth), then this will have a different value.	Any
{Session.IMEI}	This variable expands to the IMEI of the subscriber's phone or equipment associated with the request.	Any
{Session.IMEISV}	This variable expands to the IMEISV of the subscriber's phone or equipment associated with the request.	Any

Chapter 21

Managing Policy Rules

Topics:

Policy rules are created and saved within the CMP and then deployed to MPE devices. The CMP lets you create and modify the details within the policies, as well as edit the order in which policy rules are applied to a protocol message.

To create policy rules, see *Understanding and Creating Policy Rules*. *Managing Policy Rules* describes how to manage your library of policy rules and policy groups.

Displaying a Policy

To display a policy:

1. From the **Policy Management** section of the Policy Management section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. If a policy references another policy or policy group, a plus sign (+) appears next to the policy name in the content tree. Click on the plus sign to expand the structure of referenced policies and policy groups.
3. From the content tree, select the desired policy.
   The policy is displayed. *Figure 20: Sample Policy Description* shows an example.

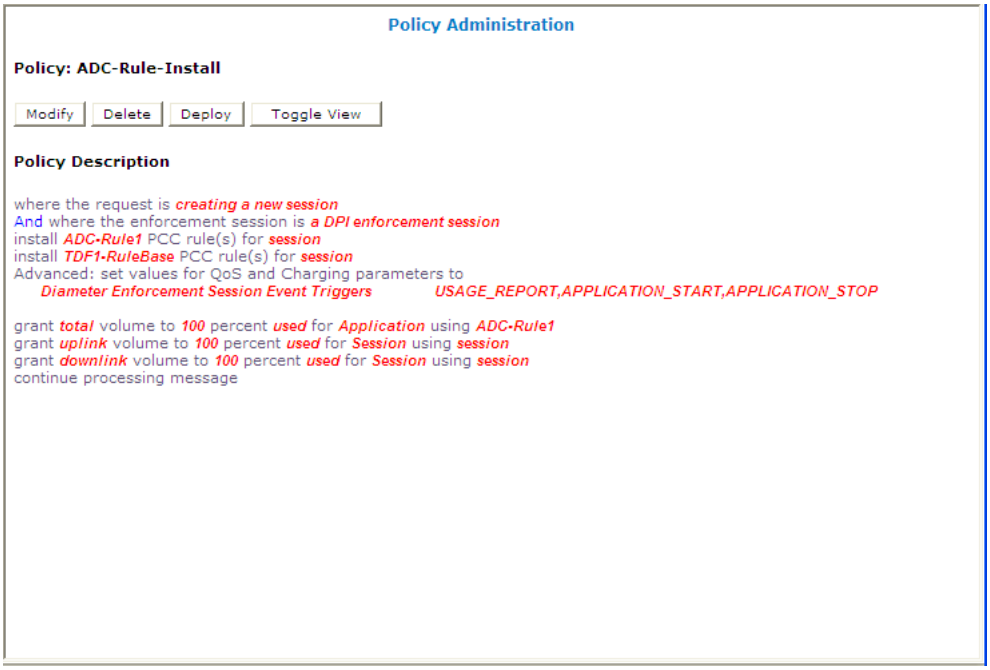


Figure 20: Sample Policy Description

You can choose from two logical views of policy conditions:

- A tree format (the default, shown)
- A Boolean expression format similar to SQL

To switch between one view and the other, click **Toggle View**.

If the policy evaluates a policy group, the policies in the group (which are referenced policies) are displayed. Click on a policy name to see details of that policy. If a referenced policy itself refers to other policies or groups, those policies or groups are also displayed.

Deploying Policy Rules

Deploying a policy (or policy group) is the act of transferring the policy from the CMP to an MPE device. Once deployed, the policy rules defined within the policy or policy group are used as decision-making criteria by the MPE device.

Figure 21: Policy Deployment shows how policies P1 through P7 are created on the CMP and then deployed individually to different MPE devices within the network. Each of the policies is associated individually with the MPE device where it is deployed. In the example, each policy server (MPE device) displays the policies that have been deployed to it and the order in which they are applied to policy requests, from top to bottom.

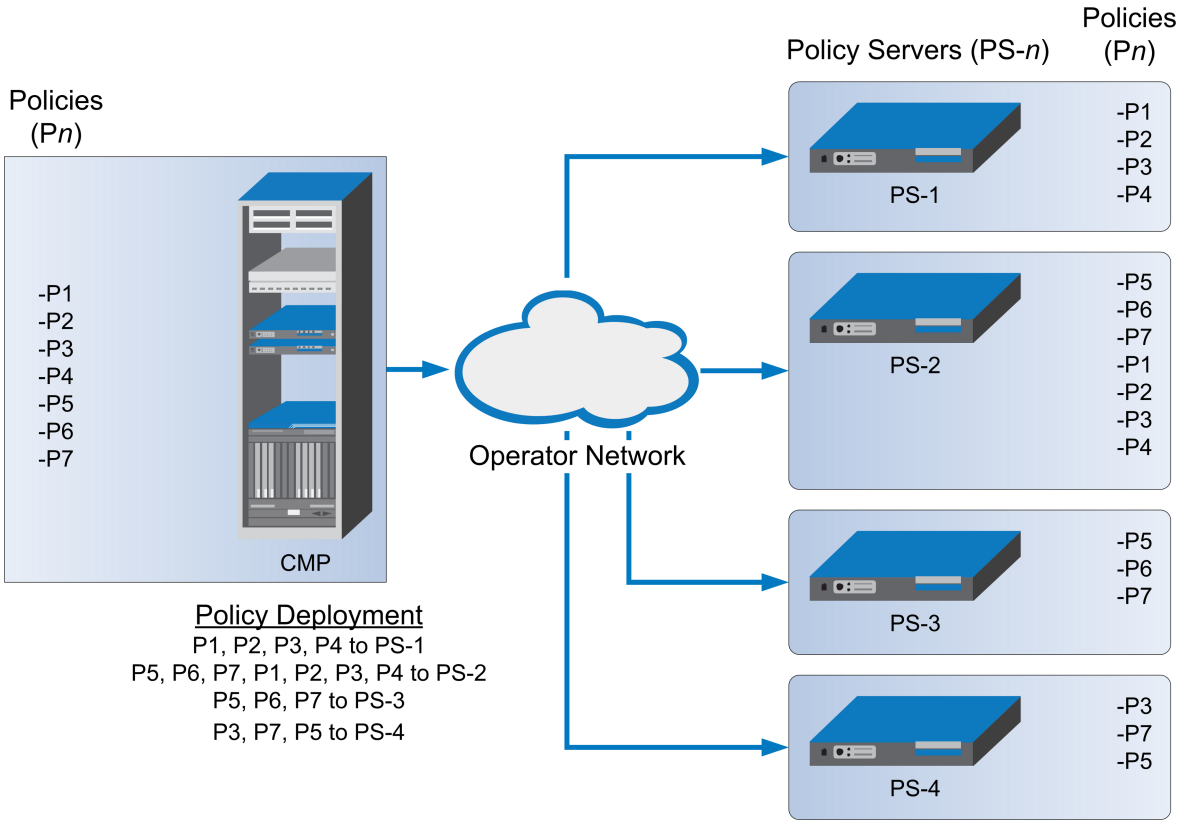


Figure 21: Policy Deployment

Figure 22: Policy Group Deployment shows how the same library of policies can be grouped first and then deployed as policy groups. When a policy group is created, the policies are arranged in the order in which they are to be evaluated. Grouping policies makes deployment of multiple policies easier and helps to ensure consistency in how policies are applied to policy requests on different MPE devices.

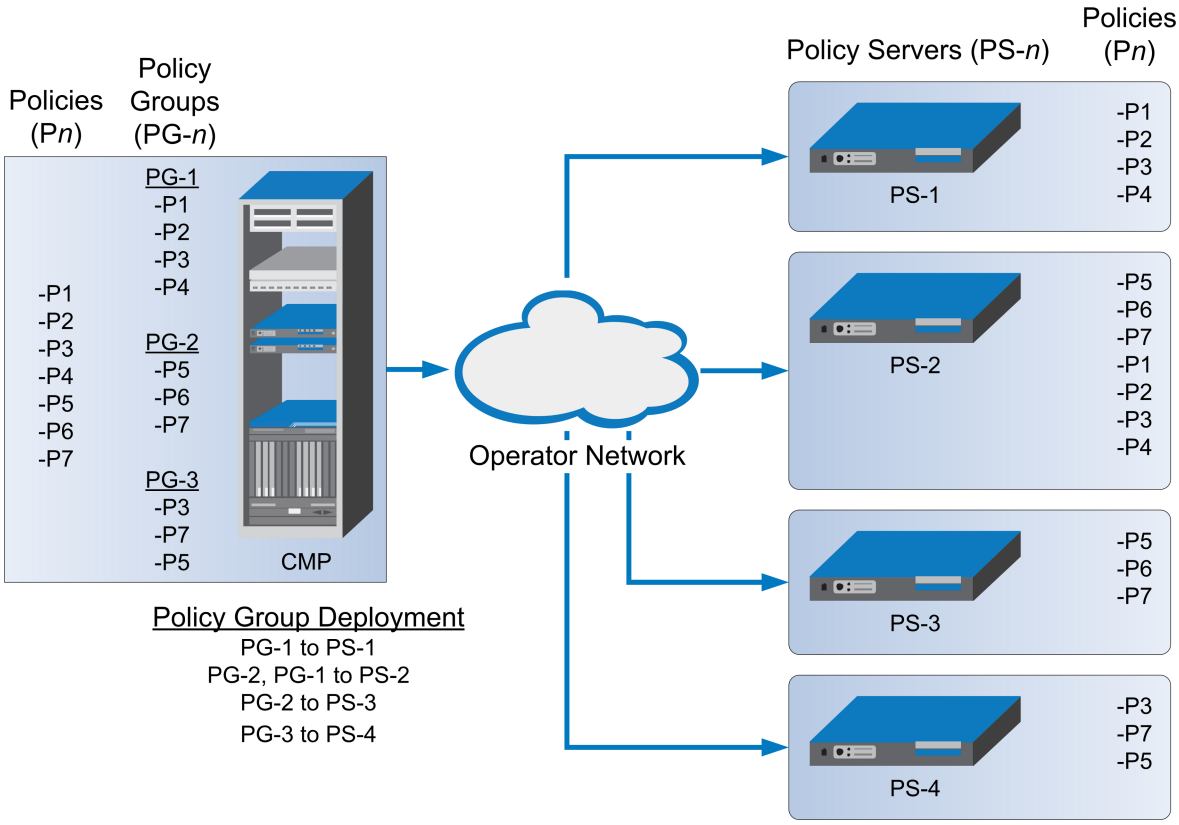


Figure 22: Policy Group Deployment

When you first create a policy rule, that rule exists only within the CMP policy database. Once the policy rule is deployed, any change to the policy rule is automatically redeployed when you complete your changes. Automatic redeployment also applies to policy groups as well: any change to a policy group triggers automatic redeployment. If you add a policy rule that was not previously deployed to a policy group that is deployed to one or more MPE devices, then the rule is deployed automatically to those MPE devices.

Figure 23: Policy Redeployment shows that when a policy (P3) is modified, its associated groups (PG-1 and PG-3) are redeployed automatically.

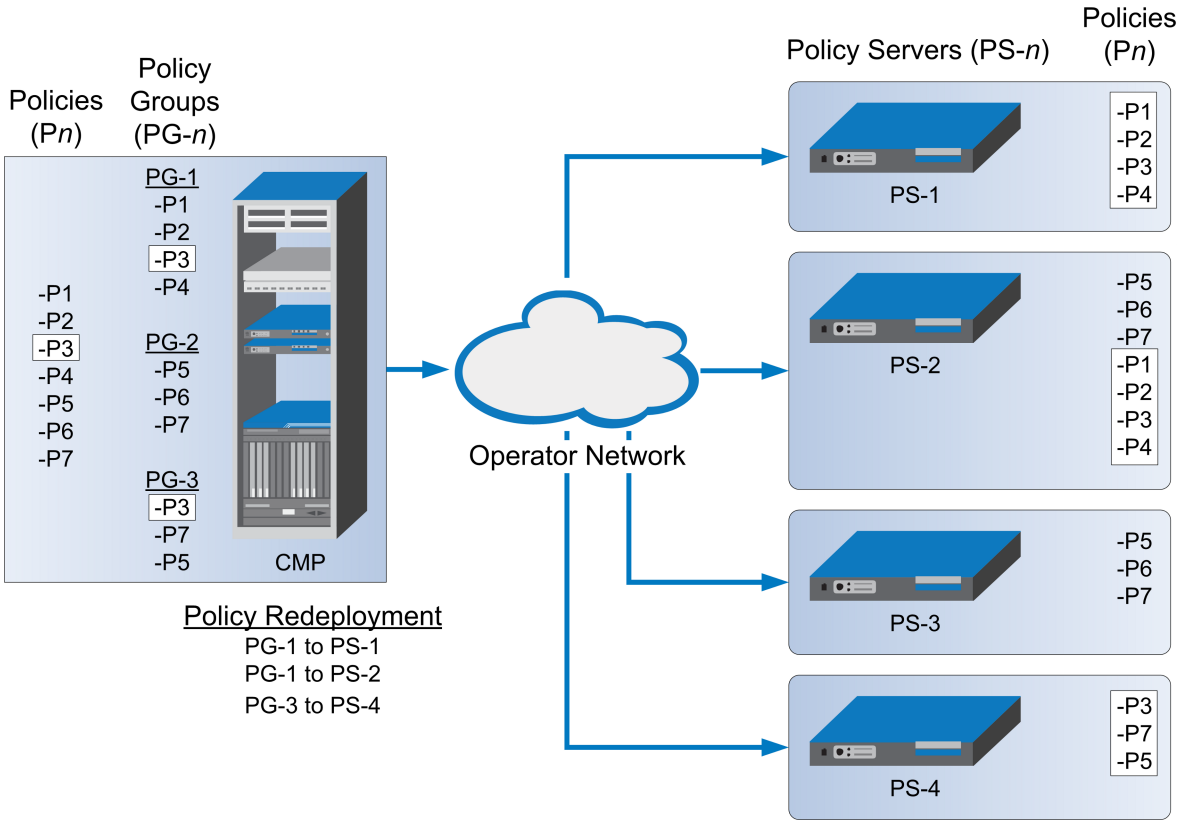


Figure 23: Policy Redeployment

When a policy rule is used as a reference policy, you do not need to deploy it; it is deployed automatically when called by a parent, or top-level, policy.

Modifying and Deleting a Policy

Policies can be modified and then redeployed to MPE devices. When a policy that resides in multiple policy groups is modified, the changes are propagated to the various groups.

Modifying a Policy

To modify an existing policy:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The Policy Administration page opens in the work area, listing the available policies.
3. Select the policy you want to edit.
   The Policy Administration page displays information about the policy.
4. Click **Modify**.
   The policy wizard opens in a Modify Policy tab.

5. Edit the desired policy information.

   See *Creating a New Policy* for details on the fields within the policy wizard.

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

The policy is modified. The modified policy is now ready to be added to a policy group (see *Adding a Policy to a Policy Group*), or deployed to one or more MPE devices (see *Deploying a Policy or Policy Group to MPE Devices*).

Note: Redeployment of a policy is automatically performed to those MPE devices where the policy was initially deployed.

Deleting a Policy

Policies, policies within a policy group, and entire policy groups can be removed from an MPE device when they are no longer needed. Because the policy still resides on the CMP, it can be redeployed at a later date if needed. If a policy is no longer needed, it can be deleted from the CMP as well.

Note: Deleting a policy from the CMP automatically removes the policy from all associated MPE devices.

To delete a policy:

1. From the **Policy Management** section of the navigation pane, select **Policy Library**.
   The content tree displays a list of policy groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The Policy Administration page opens in the work area, displaying all defined policies.
3. Use one of the following methods to select the policy to delete:
   - From the work area, click the **Delete** icon located to the right of the policy you want to delete.
   - From the policy group tree, select the policy; the Policy Administration page opens. Click **Delete**.

   You are prompted: "Are you sure you want to delete this Policy?"
4. Click **OK** to delete the policy (or **Cancel** to cancel the request).

The policy is deleted.

To remove a deployed policy from an MPE device, see *Removing a Policy or Policy Group from an MPE Device*.

Policy Templates

The CMP lets you create policy templates to simplify the creation of multiple policies with similar conditions and actions. A policy template is similar to a policy, except that some (or all) of the parameters in the conditions and actions are not completely defined. Those parameters are defined later, when you use the policy template to create policy rules.

The policy template wizard is used to create or modify a policy template. This wizard is similar to the policy wizard; however, the policy template wizard allows parameters to be only partially defined. For example, a template may only be configured for policy requests requiring bandwidth above a certain value, but not define the exact bandwidth value. You can then specify a specific bandwidth value when you use the template to create the new policy rule.

Creating a Policy Template

To create a new policy template:

1. From the **Policy Management** section of the navigation pane, select **Template Library**.
   The content tree displays the Template Library group.
2. Select the **Template Library** group.
   The Template Administration page opens in the work area.
3. On the Template Administration page, click **Create Template**.
   The Create New Policy Template window opens (*Figure 24: Create New Template Window*).
4. Select the base policy or policy template with which to begin:
   - **Blank** — No policy template attributes are pre-defined.
   - **Use Template** — Select an existing template with pre-defined attributes. Modify the template as needed, then save the template with a new template name.
   - **Copy Existing Policy** — Select an existing policy. Modify the policy as needed, then save the policy as a policy template.
5. Edit the desired policy information from one or more of the policy wizard pages.
   See *Creating a New Policy* for details on the fields within the policy wizard.
6. When you finish, click **Finish** to save the policy template and close the window (or **Cancel** to discard your changes and close the window).
   The window closes.

The policy template is created.

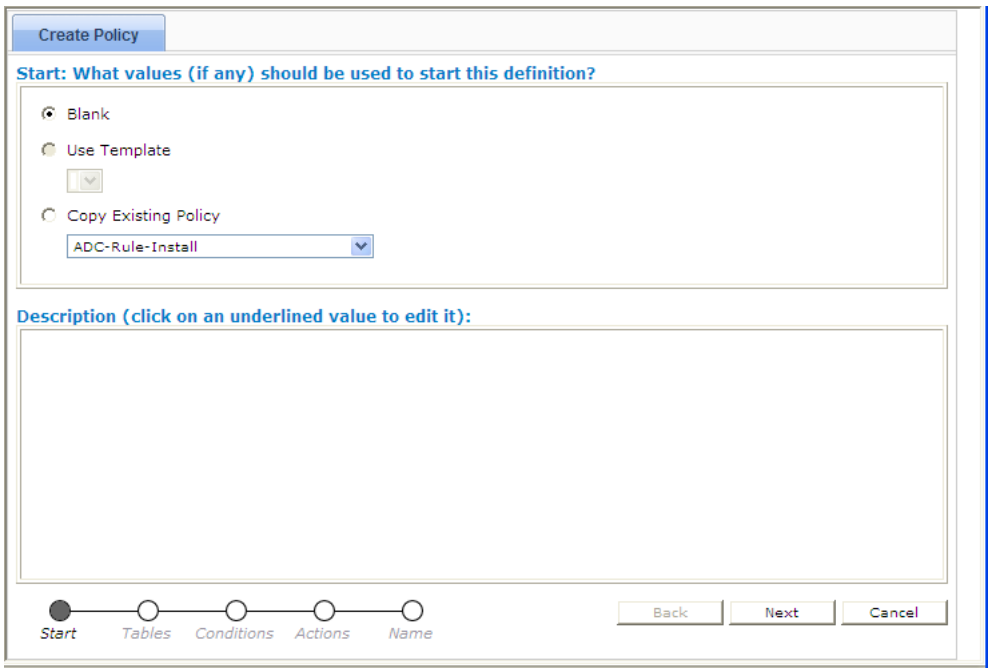


Figure 24: Create New Template Window

Modifying a Policy Template

You can edit a policy template to make changes. Modifying a policy template does not modify previously configured policies.

To modify an existing policy template:

1. From the **Policy Management** section of the navigation pane, select **Template Library**.
   The content tree displays the **Template Library** group.
2. Select the **Template Library** group.
   The Template Administration page opens in the work area.
3. Select the template you want to modify.
   The Template Administration page displays a description of the template.
4. Click **Modify**.
   The Modify Policy tab opens with the last step of the template creation process. *Figure 25: Modify Policy Template Window* shows an example.
5. Click **Back** to return to where you want to edit the template and modify the desired information.
6. When you finish, click **Finish** to save the modified template (or **Cancel** to discard your changes).
   The window closes.

The template is modified.

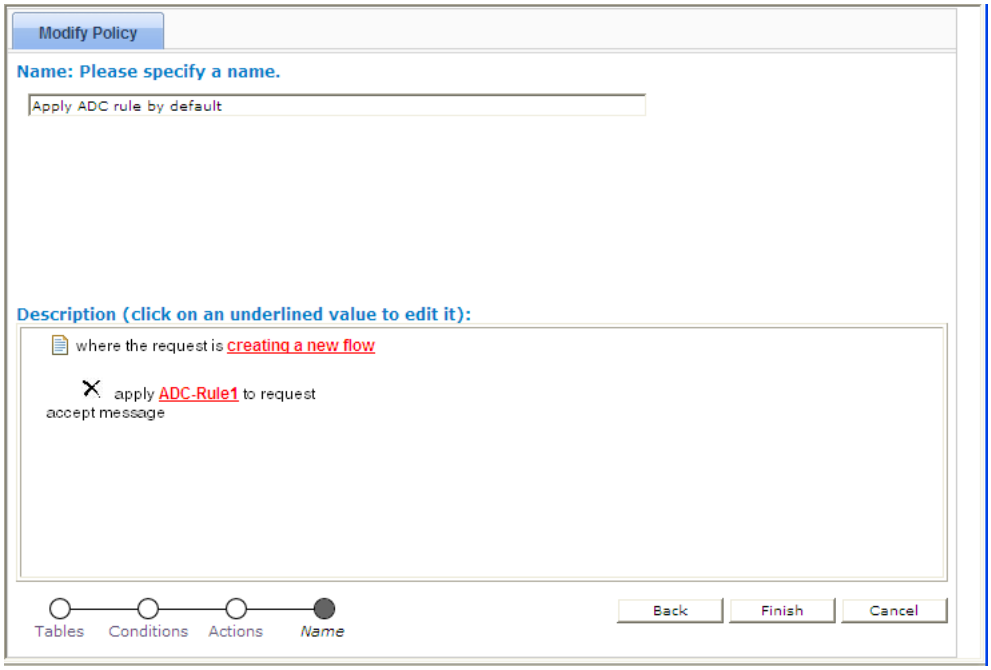


Figure 25: Modify Policy Template Window

Deleting a Policy Template

To delete a policy template:

1. From the **Policy Management** section of the navigation pane, select **Template Library**.

The Template Administration page opens in the work area, displaying all defined policy templates.

2. Use one of the following methods to select the policy template to delete:
   - From the work area, click the **Delete** icon, located to the right of the policy template you want to delete.
   - From the template library, select the template; the Template Administration page displays the template. Click **Delete**.

   You are prompted: "Are you sure you want to delete this template?"
3. Click **OK** to delete the policy template (or **Cancel** to cancel the request).

The policy template is deleted.

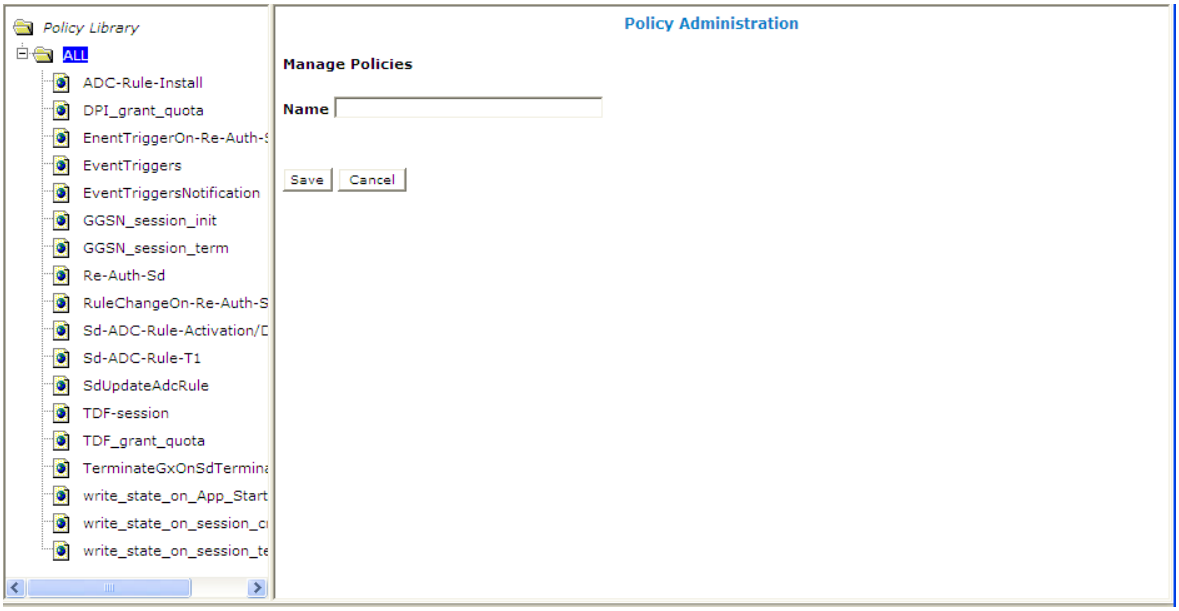
Managing a Policy Group

The CMP lets you create policy groups. Policy groups are an organizational aid that provide for flexible policy management, deployment, and execution. Policies are saved to a group in the order in which the MPE device applies them to a policy request. If needed, you can change that order. You can save a policy to multiple policy groups and add a policy to, or remove it from, a policy group at any time.

Creating a Policy Group

To create a new policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The Policy Administration page opens in the work area, listing available policies.
3. On the Policy Administration page, click **Create Group**.
   The group naming field opens in the work area; for example:



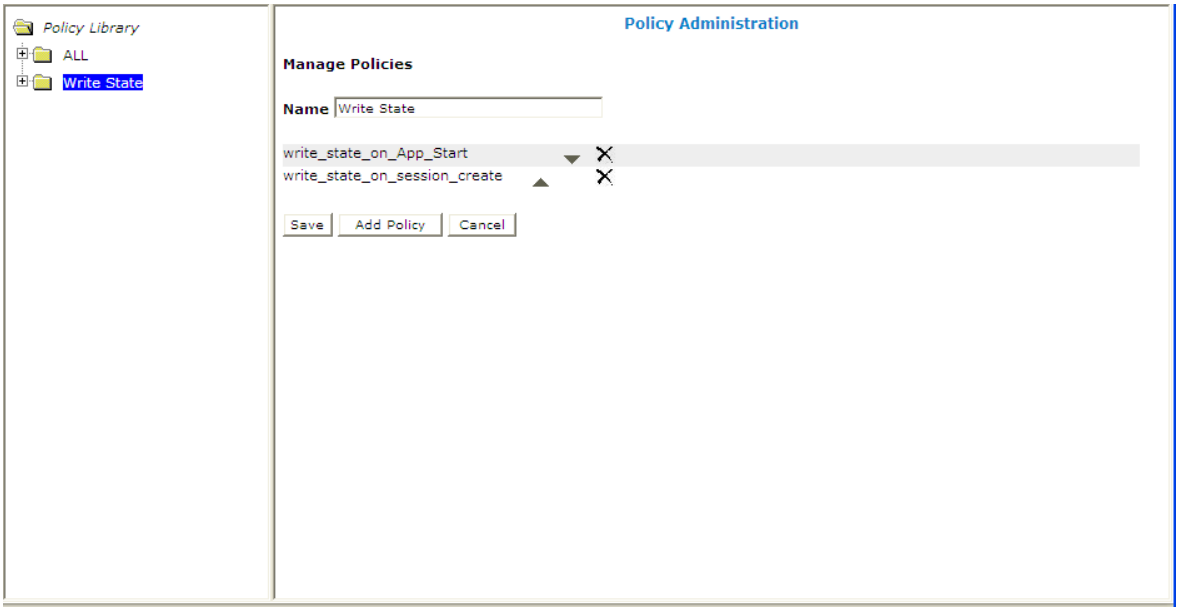
4. Enter the name to assign to the new group, then click **Save** (or **Cancel** to discard your changes).

The new group information is saved to the CMP and displayed in the content tree.

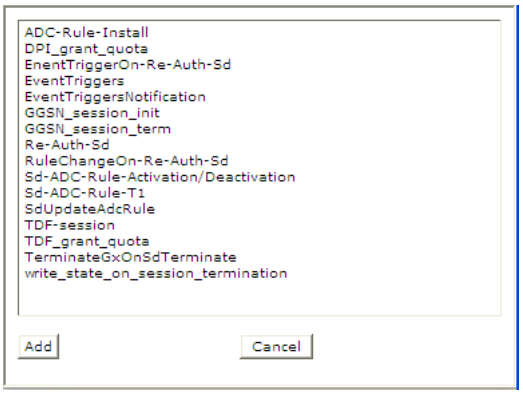
Adding a Policy to a Policy Group

To add one or more policies to a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the policy group to which you want to add the policy.
   The Policy Administration page opens in the work area, listing the policies currently in the group.
3. On the Policy Administration page, click **Modify**.
   The Policy Administration page opens in the work area; for example:



4. Click **Add Policy**.
   A window opens, displaying the policies available; for example:



5. Select the desired policy or policies to add to this group and click **Add** (or **Cancel** to cancel the request).
   The policies are added to the policy group and the window closes.

   Note: Policies are applied to messages in the order in which they appear in the policy group. You can change the sequential order as desired (see *Changing the Sequence of Deployed Policy Groups*).

6. When you finish, click **Save** (or **Cancel** to discard your changes).
   The added policies are displayed in the policy group tree.

Now you can deploy the policy group to the policy servers (see *Deploying a Policy or Policy Group to MPE Devices*).

Note: If this group had been deployed previously, it is automatically redeployed at this time, ensuring the MPE devices are resynchronized with the CMP.

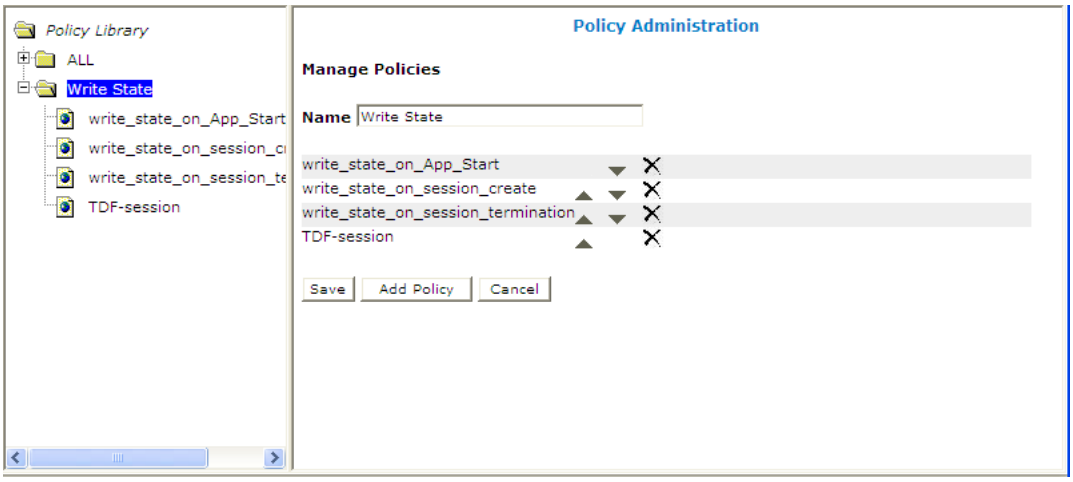
Removing a Policy from a Policy Group

Removing a policy from a policy group that has been saved to the CMP only removes the policy from the selected policy group. The policy itself remains in the **ALL** group, as well as any other group to which it had been added. (To remove a policy from all groups in the Policy Library, see *Removing a Policy or Policy Group from an MPE Device*.)

To remove a policy from a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the desired policy group.
   The Policy Administration page opens in the work area, listing the policies it contains.
3. Remove the desired policy using one of the following methods:
   - From the content tree, select the desired policy within the policy group; its profile information is displayed. Click **Remove**.

   - From the content tree, select the desired policy group and click **Modify**. Select the remove icon, located to the right of the policy you want to remove.



After a policy is removed from a policy group, the modified group is ready to be deployed to MPE devices (see *Deploying a Policy or Policy Group to MPE Devices*).

Note: This modified policy group is redeployed at this time, ensuring that the MPE devices are resynchronized with the CMP system.

Changing the Sequence of Policies Within a Policy Group

The order in which policies appear in a policy group is the order in which they are deployed and applied to policy requests. You can modify the order of policies, both inside and outside of a policy group.

To change the order of the policies within a group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the desired policy group.
   The Policy Administration page opens in the work area, displaying policies in their current sequential order.
3. On the Policy Administration page, click **Modify**.
   The Manage Policies page opens.
4. Use the up and down arrow icons, located to the right of policies, to change the sequence of policies within the group.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The modified group is ready to be deployed to MPE devices (see *Deploying a Policy or Policy Group to MPE Devices*).

Note: This modified group is redeployed at this time, ensuring that the MPE devices are resynchronized with the CMP.

Displaying Policy Details Contained Within a Policy Group

To display the policies within a policy group:

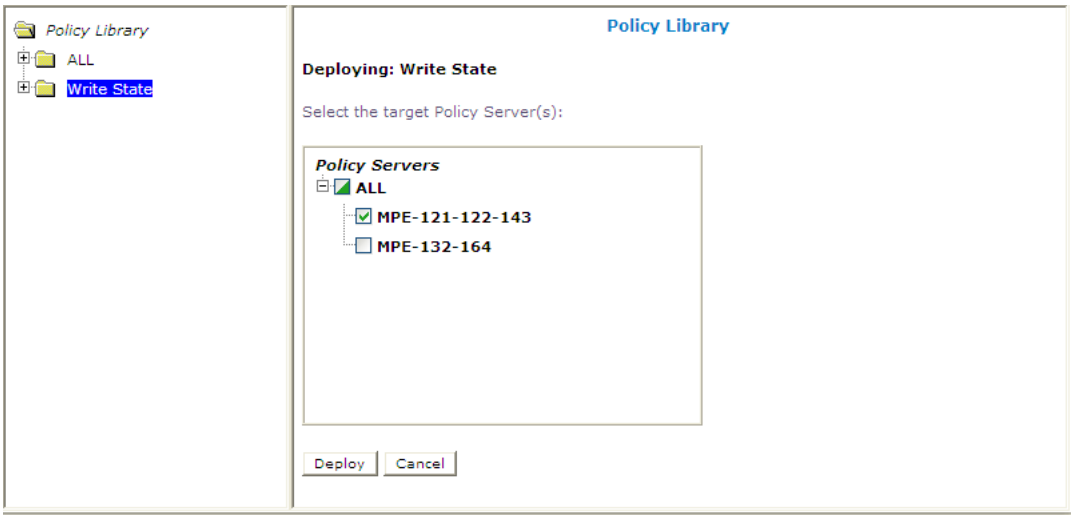
1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the desired policy group.
   The Policy Administration page opens in the work area, listing the policies it contains.
3. Click **Show Details**.
   The configured policies, including the configured parameters for the policies, are displayed. To switch between logical views of policy conditions, click **Toggle View** .
4. When you finish, click **Cancel**.

Deploying a Policy or Policy Group to MPE Devices

The basic procedure for deploying either a policy or a policy group to MPE devices is the same. The following procedure uses the example of deploying a policy group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.

2. From the content tree, select the policy group to deploy.
   The Policy Administration page opens in the work area, listing the policies it contains.
3. On the Policy Administration page, click **Deploy**.
   The policy server tree is displayed, listing all possible target policy servers (MPE devices) and server groups. You can expand the tree view if necessary.
4. Select the desired target MPE devices or server groups.



5. Click **Deploy** (or **Cancel** to cancel the request).

The policy information is saved to each selected MPE device. A message confirms that the deployment process was successful.

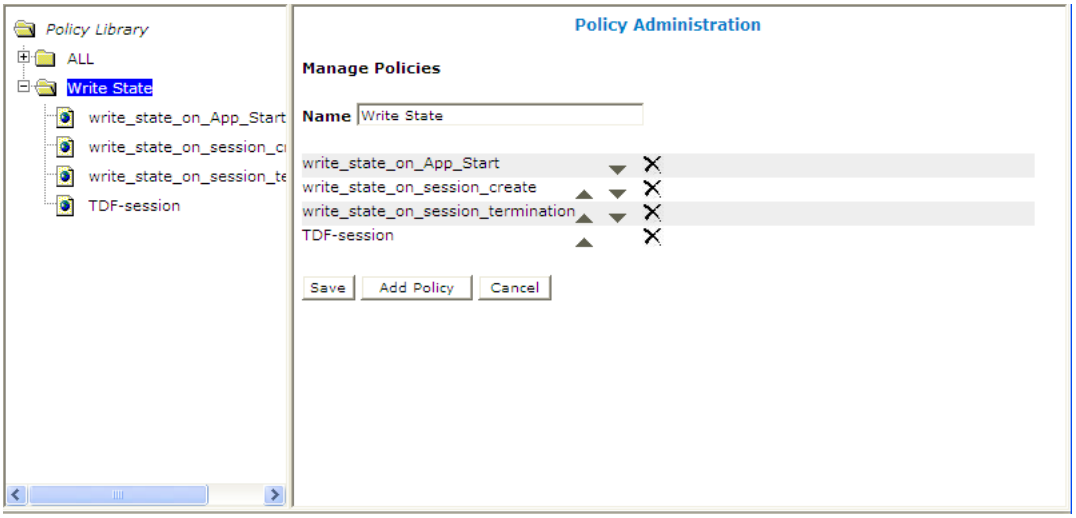
Removing a Policy from a Policy Group on an MPE Device

To remove a policy from within a policy group that was deployed to an MPE device, the policy group is modified on the CMP system, then redeployed. (To remove an entire policy group from an MPE device, see *Removing a Policy or Policy Group from an MPE Device*.)

To remove a policy from a policy group and then redeploy the group:

1. From the **Policy Management** section of the navigation pane, select **Policy Library.**
   The content tree displays a list of policy library groups; the initial group is **ALL**.
2. From the content tree, select the desired policy group.
   The Policy Administration page opens in the work area, listing the policies the group contains.
3. Remove the desired policy using one of the following methods:
   - From the Policy Library tree, select the policy. The Policy Administration page displays the profile information. Click **Remove**.

- On the Policy Administration page, click **Modify** and then select the Remove icon located next to the policy you want to remove.



Removing a Policy or Policy Group from an MPE Device

Removing a deployed policy or policy group from an MPE device is performed from the Policy Server Administration page.

To remove a policy/policy group from 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, displaying information about the MPE device.
3. On the Policy Server Administration page, select the **Policies** tab.

4. Click **Modify**.
   The Manage Policies page opens.
5. Click the Remove icon, located to the right of the policy or policy group that you want to remove.
6. When you finish, click **Save** (or **Cancel** to cancel the request).

The policy or policy group is redeployed to the MPE device, minus the removed policy or policy group.

Changing the Sequence of Deployed Policy Groups

Changing the sequential order of deployed policy groups is performed directly on an MPE device using the Policy Server Administration page.

To change the sequential order of policy groups:

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, displaying information about the MPE device.
3. On the Policy Server Administration page, select the **Policies** tab.
4. Click **Modify**.
   The Manage Policies page opens in the work area.
5. Use the up and down arrow icons, located to the right of each policy group, to change the sequential positioning of the policy groups.
6. When you finish, click **Save** (or **Cancel** to cancel the request).

The policy groups are redeployed to the MPE device in their new sequential order. A confirmation message displays in the work area.

Importing and Exporting Policies, Policy Groups, and Templates

Policies, policy groups, and templates can be exported from the CMP for inspection or backup purposes. These items are exported as a whole and cannot be exported individually, as every policy, policy group, and policy template that resides on the CMP is saved to a single file when performing the export function.

For information only, exported policies are marked with policy version numbers as well as the version number of the CMP software under which they were created. This does not affect importation of policies created under different versions of the CMP.

Importing Policies

To import a policy file to the CMP:

1. From the **Policy Management** section of the navigation pane, select **Policy Import / Export**.
   The Import/Export page opens.
2. On the Import/Export page, click **Browse** to locate the policy file to import.

3. Select the desired collision handling option:
   - **Delete all before importing** — All policies, policy groups, and templates currently on the CMP are deleted first; then the imported versions are saved to the MPE device.
   - **Overwrite with imported version** — All items are imported. If the CMP currently contains any policies, policy groups, or templates using the same names as the ones being imported, they are overwritten with the imported versions.
   - **Reject any that already exist** — All items are imported except for imported versions with the same name as any policy, policy group, or template currently on the CMP.
   - **Any collisions prevent all importing** — No items are imported if any of the imported versions has the same name as any policy, policy group, or template currently on the CMP. This is the default.
4. Click **Import**.

The policies are imported.

If you try to import an invalid file you receive a validation error: "You must correct the following error(s) before proceeding: There is a problem with the import file. The name is required, the file must be present, and the file must be in the correct format."

Exporting Policies

To export the policies or policy templates that reside in the policy library:

1. From the **Policy Management** section of the navigation pane, select **Policy Import / Export**.
   The Import/Export page opens.
2. Select the type of export: **Policies** (the default) or **Templates.**
3. Select the policy group to export: **All** (the default) or a named group.
4. Click **Export** to export the policy group in XML format, or **Text** to export the policy group in descriptive format. Policies exported in text format cannot be reimported.
   A standard File Download window opens.
5. Click **Save** (or **Cancel** to close the window and cancel the request).
   A standard Save As window opens.
6. Assign a name to the policy file (the default is PolicyExport.xml), use the browse function to map to the desired location, and click **Save**.
   When the policies are successfully exported, a standard Download Complete window opens.
7. Select **Close** to close the Download Complete window.

The policies or templates are exported to a file.

Managing Policy Checkpoints

A policy checkpoint is a method of saving the records in the CMP at a specific point in time. Records saved are policies, policy groups, policy templates, policy tables, retry profiles, service profiles, traffic profiles, and traffic profile groups. Related profiles are not saved. You can save up to ten checkpoints.

Once a checkpoint is created, you can return to this set of records at any time by restoring the checkpoint.

CAUTION

CAUTION: When you restore a checkpoint, all existing data is permanently removed.

The checkpoint function is different from the export/import function in these ways:

- Checkpoints are saved on the CMP server rather than to a file.
- A checkpoint saves all records mentioned above; the import/export feature allows you to select which records to import or export.
- A checkpoint can only be used on a specific CMP, and cannot be migrated to another CMP system.

To see this feature on the GUI menu and be able to use it, a value other than 0 must be specified for the **Allow policy backup and rollback** field on the *Configuring System Settings* page. This field also controls the maximum number of checkpoints that can be saved.

Viewing and Comparing Policy Checkpoints

Use this procedure to view all checkpoints and/or compare a selected checkpoint's records to the current CMP records. You can also view the records saved for a specific checkpoint.

To view/compare policy checkpoints in the CMP:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**. The Checkpoint/Restore page opens.
2. Click **Diff** to view a report that compares the selected checkpoint's records to the current CMP records.
3. Click **More Info** to view a list of all required profile names for this checkpoint. These profiles must exist in the system before a checkpoint is restored, otherwise the restore will fail.

Creating a Policy Checkpoint

Use this procedure to create a new checkpoint. A checkpoint saves policies, policy groups, policy templates, traffic profiles, and traffic profile groups; related profiles are not saved.

Note that the maximum number of checkpoints that can be created is defined on the System Settings page. If you create more than the number defined, the oldest checkpoint is deleted.

To create a new policy checkpoint in the CMP:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**. The Checkpoint/Restore page opens.
2. Click **Create a new checkpoint**.
   If the maximum number of checkpoints already exists, the message, **X checkpoints already exist, by creating this checkpoint the oldest one will be deleted. Continue?** appears (where X is the maximum number of checkpoints).

   To add the new checkpoint click **OK**, or click **Cancel** to exit the checkpoint creation process.

When the checkpoint is created, the message, **Checkpoint successfully added** appears in green on the screen.

Restoring a Policy Checkpoint

CAUTION

CAUTION: All current records are lost when a restore is performed. It is recommended that you save a checkpoint before restoring a previous checkpoint.

Use this procedure to return to a saved checkpoint. A checkpoint saves policies, policy groups, policy templates, traffic profiles, and traffic profile groups.

Note: Profiles are not saved in checkpoints, so be sure all related profiles exist in the CMP before restoring. If a related profile is not available before you do a restore, the restore process will fail. Use the **More Info** link to view all required profiles for a checkpoint.

To restore to a checkpoint in the CMP without autodeployment to the MPEs:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**. The Checkpoint/Restore page opens.
2. Click the radio button associated with the checkpoint you are restoring.
3. Click **Restore** to restore the selected checkpoint.
   A pop-up dialog box appears with the message, **Caution: You'd better save a checkpoint before any restoration.**
4. Click **Cancel** to exit (if you need to create a checkpoint) or **OK** to continue.
   If you click **OK**, a pop-up dialog box appears with the message, **Are you sure that you want to restore this checkpoint?**
5. Click **OK**.
   The selected checkpoint is restored.

A restored checkpoint message appears, listing which policies and policy groups were restored and which were removed.

Restoring a Policy Checkpoint to MPEs

CAUTION

CAUTION: All current records are lost when a restore is performed. It is recommended that you save a checkpoint before restoring a previous checkpoint.

Note: Profiles are not saved in checkpoints, so be sure all related profiles exist in the CMP before restoring. If a related profile is not available before you do a restore, the restore process will fail. Use the **More Info** link to view all required profiles for a checkpoint.

To restore to a checkpoint in the CMP and autodeploy to all MPEs in the system:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**. The Checkpoint/Restore page opens.
2. Click the radio button associated with the checkpoint you are restoring.
3. Click **Restore & Deploy** to restore records to the selected checkpoint.
   A pop-up dialog box appears with the message, **Caution: You'd better save a checkpoint before any restoration.**
4. Click **Cancel** to exit (if you need to create a checkpoint) or **OK** to continue.

If you click **OK**, a pop-up dialog box appears with the message, **Are you sure that you want to restore this checkpoint and deploy to the MPEs?**

5. Click **OK**.
   The selected checkpoint is restored and deployed to the MPEs.

A restored checkpoint message appears, listing which policies and policy groups were restored, which were removed, and to which MPEs the deployment succeeded.

Deleting a Policy Checkpoint

To delete a saved checkpoint from the CMP:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**.
   The Checkpoint/Restore page opens.
2. Click the radio button associated with the checkpoint you are deleting.
3. Click **Delete the selected checkpoint** to remove the checkpoint from the system.
   A pop-up dialog box appears with the message, **Are you sure you want to delete this Checkpoint?**
4. Click **OK**.
   The message, **Checkpoint deleted successfully** appears in green on the screen.

The selected checkpoint is deleted from the system.

Chapter 22

Managing Policy Tables

Topics:

Managing Policy Tables describes how to create, modify, delete, and view independent objects which are used to capture differences in policy structures.

You can manage multiple policies with small differences by abstracting the policies into tables. The process of modifying the policies then becomes simpler and less prone to error.

About Policy Tables

APNs have a unique charging-rule name which is applicable to home or roaming usage. The rule must be mapped for the flow and session of devices. The following table describes the possible table-driven policy examples.

Table 9: ChargingRuleInstall OnNet

Name	Description
02 - ApnChargingRuleList	CRule Table
02 - Scope	Device Specific flow or session, where the APN matches one of [CRuleTable.CalledStationId]. The serving MCC-MNC matches one of 26207. The device name matches one of [scope.DeviceName]. Install [CRuletable.charging profile on_net] PCC rule(s) for [scope.flowOrsession] continue processing message

Table 10: ChargingRuleInstall OffNet

Name	Description
02 - ApnChargingRuleList	CRule Table
02 - Scope	Device Specific flow or session, where the APN matches one of [CRuleTable.CalledStationId]. The serving MCC-MNC matches one of 26207. The device name matches one of [scope.DeviceName]. Install [CRuletable.charging profile off_net] PCC rule(s) for [scope.flowOrsession] continue processing message

Creating Policy Tables

1. From the **Policy Management** section of the navigation pane, select **Policy Table Library**.
   The content tree displays the Policy Table Library group.
2. Select the **Policy Table Library** group.
   The Policy Table Administration page opens in the work area.
3. On the Policy Table Administration page click **Create Policy Table**.
   The New Policy Table Administration page opens.
4. Enter information as appropriate for the Policy Table:
   a) **Name** (required) — The name you assign to the policy table.
      The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).

b) **Description/Location** (required) — Free-form text that identifies the policy table.

5. Click **Add Row** or **Add Column** — (required) At least one key column must be selected.

   If **Add Column** is selected, you must populate the following definitions in the Policy Table column pop-up:

   - **Column Name** (required) — The name you assign for the column.
   - **Key** (required) — A check box and entry field which indicates that this is a key column.
   - **Column Type** (required) — The folder icon when clicked opens the wizard, which displays the optional actions and conditions. Select your fields of choice from an action or condition.

   Your column name, key, type, actions, and conditions are selected.

6. Click **Operations** — You can perform the following from the pulldown list:

   - **Delete Row** — Deletes the table row.
   - **Move Row Up** — Moves the table row up.
   - **Move Row Down** — Moves the table row down.
   - **Delete Column** — Deletes the column in the table.
   - **Move Column Left** — Moves the column left in the table.
   - **Move Column Right** — Moves the column right in the table.
   - **Sort Column** — Sorts the column in the table.
   - **UnSort Column** — Reverts the column to its original order.

7. Click **Validate**. If selected, the data modified is validated. If invalid, a diagnostic message appears.

   The Policy Table is displayed on the Policy Table Administration page.

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

Modifying Policy Tables

1. From the **Policy Management** section of the navigation pane, select **Policy Table Library**.
   The Policy Table Administration page opens in the work area.
2. On the Policy Table Administration page, select the policy table you want to modify.
   The Policy Table Administration page displays information about the policy table.
3. Click **Validate**. If selected, the data modified is validated. If invalid, a diagnostic message appears.
4. Click **Modify**.
   The table fields become editable. See *Creating Policy Tables* for information about the table fields.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

The policy table content is modified.

Deleting Policy Tables

1. From the **Policy Management** section of the navigation pane, select **Policy Table Library**.
   The Policy Table Administration page opens in the work area.

2. Delete the Policy Table using one of the following methods:
   - From the work area, click the **Delete** icon located to the left of the Policy Table name you wish to delete..
   - Open the policy and click **Delete**.

   You are prompted: "Are you sure you want to delete this policy table?"
3. Click **OK** (or **Cancel** to cancel the request).

The policy table is deleted.

Viewing Policy Tables

From the **Policy Management** section of the navigation pane, select **Policy Table Library**.
A tree frame view of all existing policy tables. You will see all of the existing policy tables in the main frame when you click **ALL**.

Note: The policy table details are viewed by clicking the actual policy table name in the tree frame.

Chapter 23

Managing Subscribers

Topics:

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

Note: For information about the Subscriber Profile Repository (SPR), see the *Tekelec Subscriber Data Management* documentation.

Creating a Tier

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

To create a subscriber tier:

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

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

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

      Enter up to 250 characters.

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

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

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

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

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

The tier is created and applied to MPE devices controlled by this CMP, and the message “Tier created successfully” is displayed.

Deleting a Tier

To delete a tier:

1. From the **Subscriber** section of the navigation pane, select **Tiers**.
   The **Tiers** folder appears in the content tree.
2. Delete the tier using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the tier you wish to delete.
   - From the content tree, select the tier and click **Delete**. You are prompted, “Are you sure you want to delete this Tier?”
3. Click **OK** (or **Cancel** to cancel the request).

The tier is deleted, and the message “Tier deleted successfully” is displayed.

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. 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 26: 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.

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 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.

Policy Server Administration

Policy Server: MPE1

System | Reports | Logs | Policy Server | Diameter Routing | Policies | Data Sources | Session Viewer

Session Viewer:

Identifier type: IMSI Identifier name: 310410000000017 Search

Subscriber Session Data:

1 session(s) has been found.

SessionId: pgw1.test.com;1336073844;13 Delete Session

AppId: 16777238
AppName: Gx []
PeerId: mra1.test.com
DestinationHost: pgw1.test.com
DestinationRealm: test.com
Type: Server
UserAddress: 2001:0DB8:85A3:9837:0000:0000:0000:0000/64
UserIds: NAI:0310410000000017@nai.epc.mnc410.mcc310.3gppnetwork.org, IMSI:310410000000017
Persistant User: User: NAI:0310410000000017@nai.epc.mnc410.mcc310.3gppnetwork.org key: 13422
Account ID:null

User IDs:
IP:2001:0DB8:85A3:9837:0000:0000:0000:0000
NAI:0310410000000017@nai.epc.mnc410.mcc310.3gppnetwork.org
IMSI:310410000000017
IP:10.3.3.33
Pool ID:null
Entitlements:
Tier CID:0
Upstream Limit:0
Upstream Guaranteed:0
Downstream Limit:0
Downstream Guaranteed:0
Equipment IDs:
Custom Fields:
Billing Type:0
Billing Day:0
Associated session count:1
Subcribed for notifications:false
Unknown:true

Figure 26: Session Viewer Page

Chapter 24

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.

Viewing Active Alarms

The Active Alarms report 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.

To view the Active Alarms report, from the **System Wide Reports** section of the navigation pane, select **Active Alarms**.

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

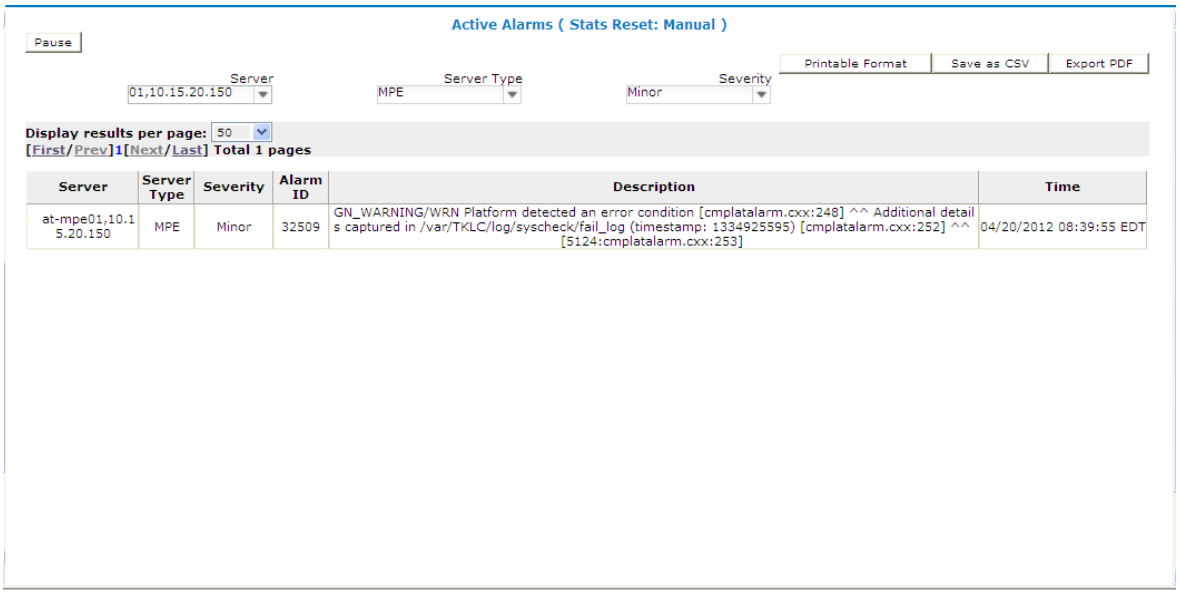


Figure 27: Sample Active Alarms Report

The alarm levels are as follows:

- **Critical** — Service is being interrupted.
- **Major** — Service may be interrupted if the issue is not corrected.
- **Minor** — Non-service affecting fault.

Notification with a severity of Info are not displayed in the Active Alarms report, but are written to the trace log. For more information, see *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.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To select alarms from an individual Policy Management cluster, select it from the **Server** list.
- To select alarms from a class of Policy Management cluster, select **All** (the default), **CMP**, **MRA**, or **MPE** from the **Server Type** list.
- To pause the display of alarms, click **Pause**. To resume the display, click **Refresh**.

- To filter results by severity, from the **Severity** list select **All** (the default) to display alarms of all severities, **Major** to display alarms of severity Major, or **Minor** to display alarms of severity Minor.
- To reformat the report for printing, click **Printable Format**.
- To save the report in comma-separated-value (spreadsheet) format, click **Save as CSV**.
- To save the report as a Portable Document Format (PDF) file, click **Export PDF**.

Viewing the Alarm History Report

The Alarm History Report displays historical alarm information.

To view the alarm history report, from the **System Wide Reports** section of the navigation pane, select **Alarm History Report**.

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.

After entering filtering information, click **Filter** to refresh the display with the filtering applied.

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

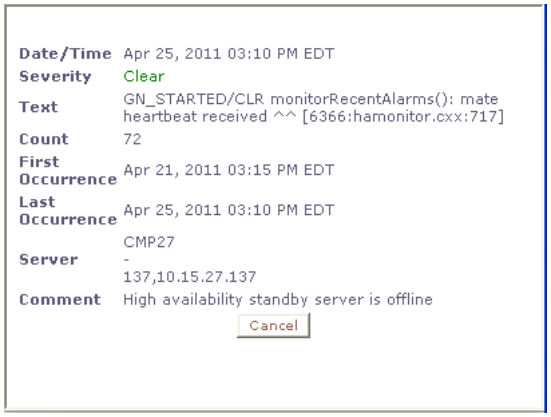
Alarms contain the following information:

- **Occurrence** — The most recent time this alert was triggered.
- **Severity** — The severity of the alert:
  - **Critical** — Service is being interrupted.
  - **Major** — Service may be interrupted if the issue is not corrected.
  - **Minor** — Non service affecting fault.
  - **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.

- **Text** — User-readable text of the alert.
- **OAM VIP** — OAM IP address or IPv4 address
- **Server** — IP address, in IPv4 or IPv6 format, or FQDN of the device from which this alarm was generated.
- **Alarm ID**— When clicked, the alarm ID provides online help information.

To view alert details, click the binoculars icon, located to the right of the alert. A window displays additional information; for example:



Click **Cancel** to close the window.

KPI Dashboard

The KPI Dashboard provides a multi-site system-level summary of performance and operational health indicators in the CMP's web-based GUI. 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's KPIs in a separate table when MRAs are managed by the CMP or with all MPE's KPIs in one table when MRAs are not managed by the CMP (e.g. 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 28: Example of KPI Dashboard with MRAs Managed by the CMP illustrates the dashboard's contents when MRAs are managed by the CMP.

mra21-189	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra21-189(Server-A)	Active	20 (0%)	3435 (0%)	3438 (0%)	42	34	4 of 4	2 of 2	1 of 4	0	0	0	22862	5280
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
mpe21-187(Server-A)	Active	4 (0%)	1500 (0%)		4	36	2 of 2	0 of 0		0	0	0	0	2350
mpe21-188(Server-A)	Active	9 (0%)	1500 (0%)		3	36	2 of 2	0 of 0		0	0	0	0	3030

mra21-34	Performance						Connections			Alarms			Protocol Errors	
MRA	State	TPS	PDN	Active Subscribers	CPU %	Memory %	MPE	MRA	Network Elements	Critical	Major	Minor	Sent	Received
mra21-34(Server-A)	Active	19 (0%)	4590 (0%)	4590 (0%)	33	34	4 of 4	2 of 2	1 of 4	0	0	0	23165	17502
mra21-34(Server-B)	Standby				1	34								
mra21-34(Server-C)	Spare				43	34								
MPE	State	TPS	PDN		CPU %	Memory %	MRA	HSS		Critical	Major	Minor	Sent	Received
mpe21-186(Server-A)	Active	9 (0%)	1500 (0%)		51	36	2 of 2	0 of 0		0	0	0	690	9679
mpe21-32(Server-A)	Active	7 (0%)	1999 (0%)		20	33	2 of 2	0 of 0		0	0	0	1	1588
mpe21-32(Server-B)	Standby				54	34								
mpe21-32(Server-C)	Spare				60	34								

Figure 28: Example of KPI Dashboard with MRAs Managed by the CMP

When MRAs are not managed by the CMP, the displayed headings are:

- Name/MPE
- Performance:
  - State
  - TPS
  - Sessions
  - CPU %
  - Memory %
- Connections
  - SPR
  - 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 (discussed below). When MRAs are managed by the CMP, a button on the top left corner lists each of the MRAs with a checkbox that allows the user to enable/disable the table for that MRA.

Each MRA or MPE system has three rows in the table. The first row displays information for the active server, Server A, in the cluster. The second row displays information for the standby server, Server

B, in the cluster, if present. And the third row displays information for the spare server, Server C, if present. If any of these are set to Reverse Site Preference, then an "R" will appear by the server's State. Several of the KPI columns are not populated for the standby or spare server (since the server is 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 on the name of an MPE or MRA device to display detailed statistics. For more information on detailed device statistics, see the description of 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 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 11: KPI Definitions for MRA* shows the mappings for MRAs; *Table 12: KPI Definitions for MPE when MRAs are Managed by CMP* shows the mappings for MPEs when the MRAs are managed by the CMP; and *Table 13: KPI Definitions for MPE when MRAs are not Managed by CMP* shows the mappings for MPEs when the MRAs are not managed by the CMP.

Table 11: KPI Definitions for MRA

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby and spare server (spare only shows Status, CPU % and Memory%)**
Name	Not derived from statistics.	Not derived from statistics.
State	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus

KPI Dashboard Column	Mapping to Statistics	
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN Connections	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	None
Active Subscribers	CurrentMRABindingCount and CurrentMRABindingPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
MPE Connections	A value in the form "X of Y", where: X is CurrentMPEConnectionCount Y is ConfiguredMPEConnectionCount	None
MRA Connections	A value in the form "X of Y", where: X is CurrentMRAConnectionCount Y is ConfiguredMRAConnectionCount	None
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 12: KPI Definitions for MPE when MRAs are Managed by CMP

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
Name	Not derived from statistics.	Not derived from statistics.
Status	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
PDN Connections	CurrentPDNConnectionCount and CurrentPDNConnectionPercentageOf Capacity	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
HSS Connections	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 13: KPI Definitions for MPE when MRAs are not Managed by CMP

KPI Dashboard Column	Mapping to Statistics	
	Active server	**Standby server**
Name	Not derived from statistics.	Not derived from statistics.
Status	Label representation of the PrimaryServerStatus	Label representation of the SecondaryServerStatus
TPS	CurrentTransactionsPerSecond and CurrentTPSPercentageOfCapacity	None
Sessions	CurrentSessionCount and CurrentSessionPercentageOfCapacity	None
CPU %	PrimaryCPUUtilizationPercentage	SecondaryCPUUtilizationPercentage
Memory %	PrimaryMemoryUtilizationPercentage	SecondaryMemoryUtilizationPercentage
SPR Connections	A value in the form "X of Y", where: X is CurrentSPRConnectionCount Y is ConfiguredSPRConnectionCount	None
Network Element Connections	A value in the form "X of Y", where: X is CurrentConnectedNECount	None
Critical Alarms	Not derived from statistics	Not derived from statistics
Major Alarms	Not derived from statistics	Not derived from statistics
Minor Alarms	Not derived from statistics	Not derived from statistics
Protocol Errors Sent	CurrentProtocolErrorSentCount	None
Protocol Errors Received	CurrentProtocolErrorReceivedCount	None

Clicking on an MRA or MPE opens the Reports tab. See the Reports section of the *CMP Wireless User's Guide* for details on reports.

Mapping Reports Display to KPIs

From the KPI Dashboard, you can click on any MPE or MRA 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 the name as it appears in OSSI XML output.

Table 14: Diameter Application Function (AF) Stats

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 sent/received	Y	Y	AAR Recv Count\AAR Send Count
AAR initial messages recd /sent	Y	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR modification messages recd/sent	Y	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages recd/sent	Y	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages recd/sent	Y	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	Y	Y	AAR Timeout Count
ASR messages recd/sent	Y	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	Y	Y	ASR Timeout Count
ASA success messages recd/sent	Y	Y	ASA Recv Success Count\ASA Send Success Count
ASA failure messages recd/sent	Y	Y	ASA Recv Failure Count\ASA Send Failure Count
RAR messages recd/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages recd/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd /sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages recd/sent	Y	Y	STR Recv Count\STR Send Count
STR messages timeout	Y	Y	STR Timeout Count
STA success messages recd /sent	Y	Y	STA Recv Success Count\STA Send Success Count
STA failure messages recd/sent	Y	Y	STA Recv Failure Count\STA Send Failure Count
Currently active sessions	Y	N	Active Session Count

Display	MPE	MRA	Name
Max active sessions	Y	N	Max Active Session Count
Diameter AF Peer Stats (in Diameter AF Stats window)	N	Y	
Connect Time	N	Y	Connect Time
Disconnect Time	N	Y	Disconnect Time
Connection Type			
IP Address: Port			
Total messages in/out	N	Y	Msg In Count\Msg Out Count
Total error messages in/out			
AAR messages sent/received	N	Y	AAR Recv Count\AAR Send Count
AAR initial messages recd/sent	N	Y	AAR Initial Recv Count\AAR Initial Send Count
AAR modification messages recd/sent	N	Y	AAR Modification Recv Count\AAR Modification Send Count
AAA success messages recd/sent	N	Y	AAA Recv Success Count\AAA Send Success Count
AAA failure messages recd/sent	N	Y	AAA Recv Failure Count\AAA Send Failure Count
AAR messages timeout	N	Y	AAR Timeout Count
ASR messages recd/sent	N	Y	ASR Recv Count\ASR Sent Count
ASR messages timeout	N	Y	ASR Timeout 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
RAR messages recd/sent	N	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	N	Y	RAR Timeout Count
RAA success messages recd/sent	N	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages rec/sent	N	Y	RAA Recv Failure Count\RAA Send Failure Count
STR messages recd/sent	N	Y	STR Recv Count\STR Send Count
STR messages timeout	N	Y	STR Timeout Count

Display	MPE	MRA	Name
STA success messages rec/sent	N	Y	STA Recv Success Count\STA Send Success Count
STA failure messages recd/sent	N	Y	STA Recv Failure Count\STA Send Failure Count

Table 15: 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/reopned 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 recd/sent	Y	Y	CCR Recv Count\CCR Send Count
CCR messages timeout	Y	Y	CCR-Timeout Count
CCA success messages recd/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages recd/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 recd/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages recd/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 recd/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages recd/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 recd/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages recd/sent	Y	Y	RAR Recv Count\RAR Send Count
RAR messages timeout	Y	Y	RAR Timeout Count
RAA success messages recd/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Currently active sessions	Y	N	Active Session Count
Max active sessions	Y	N	Max Active Session Count

Table 16: Diameter Charging Function (CTF) Statistics

Display	MPE	MRA	Name
Connections	N	Y	Conn Count
Currently OK peers	N	Y	Peer Okay Count
Currently down/suspect/reopened peers	N	Y	Peer Down Count\Peer Suspect Count\Peer Reopen Count
Total messages in/out	N	Y	Msg In Count\Msg Out Count
CCR messages sent/received	N	Y	CCR Recv Count\CCR Send Count
CCA success messages recd/sent	N	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	N	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages sent/received	N	Y	CCR-I Recv Count\CCR-I Send Count
CCA-I success messages recd/sent	N	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	N	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages sent/received	N	Y	CCR-U Recv Count\CCR-U Send Count
CCA-U success messages recd/sent	N	Y	CCA-U Recv Success Count\CCA-U Send Success Count

Display	MPE	MRA	Name
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 17: 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 sent/received	Y	Y	CCR Recv Count\CCR Send Count
CCR messages Timeout	Y	Y	CCR-Timeout Count
CCA success messages recd/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-I messages sent/received	Y	Y	CCR-I Recv Count\CCR-I Send Count

Display	MPE	MRA	Name
CCR-I messages Timeout	Y	Y	CCR-I Timeout Count
CCA-I success messages recd/sent	Y	Y	CCA-I Recv Success Count\CCA-I Send Success Count
CCA-I failure messages recd/sent	Y	Y	CCA-I Recv Failure Count\CCA-I Send Failure Count
CCR-U messages sent/received	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages Timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages recd/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages sent/received	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages Timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages recd/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages sent/received	Y	Y	RAR Recv Count\RAR Send Count
RAR messages Timeout	Y	Y	RAR Timeout Count
RAA success messages recd/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
Diameter BBERF connections	Y	Y	
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count

Table 18: 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 sent/received	Y	Y	CCR Recv Count\CCR Send Count
CCR messages Timeout	Y	Y	CCR-Timeout Count
CCA success messages recd/sent	Y	Y	CCA Recv Success Count\CCA Send Success Count
CCA failure messages recd/sent	Y	Y	CCA Recv Failure Count\CCA Send Failure Count
CCR-U messages sent/received	Y	Y	CCR-U Recv Count\CCR-U Send Count
CCR-U messages Timeout	Y	Y	CCR-U Timeout Count
CCA-U success messages recd/sent	Y	Y	CCA-U Recv Success Count\CCA-U Send Success Count
CCA-U failure messages recd/sent	Y	Y	CCA-U Recv Failure Count\CCA-U Send Failure Count
CCR-T messages sent/received	Y	Y	CCR-T Recv Count\CCR-T Send Count
CCR-T messages Timeout	Y	Y	CCR-T Timeout Count
CCA-T success messages recd/sent	Y	Y	CCA-T Recv Success Count\CCA-T Send Success Count
CCA-T failure messages recd/sent	Y	Y	CCA-T Recv Failure Count\CCA-T Send Failure Count
RAR messages sent/received	Y	Y	RAR Recv Count\RAR Send Count
RAR messages Timeout	Y	Y	RAR Timeout Count
RAA success messages recd/sent	Y	Y	RAA Recv Success Count\RAA Send Success Count
RAA failure messages recd/sent	Y	Y	RAA Recv Failure Count\RAA Send Failure Count
TSR messages sent/received	Y	Y	
TSA success messages recd/sent	Y	Y	
TSA failure messages recd/sent	Y	Y	
Diameter TDF connections	Y	Y	
Currently active sessions	Y	N	Curr Session Count
Max active sessions	Y	N	Max Active Session Count

Table 19: Diameter Distributed Routing and Management Application (DRMA) 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
DBR messages recd/sent	Y	Y	DBRRecv Count\DBRSend Count
DBR messages timeout	Y	Y	DBRTimeout Count
DBA success messages recd/sent	Y	Y	DBARecv Success Count\DBASend Success Count
DBA failure messages recd/sent	Y	Y	DBARecv Failure Count\DBASend Failure Count
DBA messages recd/sent – binding found	Y	Y	Binding Found Recv Count\Binding Found Send Count
DBA messages recd/sent – binding not found	Y	Y	Binding Not Found Recv Count\Binding Not Found Send Count
DBA messages recd/sent – PCRF down	Y	Y	Binding Found Pcrf Down Recd Count\ Binding Found Pcrf Down Send Count
DBA messages recd/sent – all PCRFs down	Y	Y	All Pcrfs Down Recv Count\ All Pcrfs Down Send Count
RUR messages recd/sent	Y	Y	RURRecv Count\ RURSend Count
RUR messages timeout	Y	Y	RURTimeout Count
RUA success messages recd/sent	Y	Y	RUARecv Success Count\ RUASend Success Count
RUA failure messages recd/sent	Y	Y	RUARecv Failure Count\ RUASend Failure Count
LNR messages recd/sent	Y	Y	LNRRecv Count\ LNRSend Count
LNR messages timeout	Y	Y	LNRTimeout Count
LNA success messages recd/sent	Y	Y	LNARecv Success Count\ LNASend Success Count
LNA failure messages recd/sent	Y	Y	LNARecv Failure Count\ LNASend Failure Count
LSR messages recd/sent	Y	Y	LSRRecv Count\ LSRSend Count

Display	MPE	MRA	Name
LSR messages timeout	Y	Y	LSRTimeout Count
LSA success messages recd/sent	Y	Y	LSARecv Success Count\ LSASend Success Count
LSA failure messages recd/send	Y	Y	LSARecv Failure Count\ LSASend Failure Count

Table 20: Diameter DRA Statistics

Display	MPE	MRA	Name
Currently active bindings	N	Y	DRABinding Count
Max active bindings	N	Y	Max DRABinding Count
Total bindings	N	Y	DRATotal Binding Count
Suspect bindings	N	Y	Suspect Binding Count
Detected duplicate bindings	N	Y	Detected Duplicate Binding Count
Released duplicate bindings	N	Y	Released Duplicate Binding Count
Diameter Release Task Statistics	N	Y	
Bindings Processed	N	Y	Release Bindings Processed
Bindings Released	N	Y	Release Bindings Removed
RAR messages sent	N	Y	Release RARs Sent
RAR messages timed out	N	Y	Release RARs Timed Out
RAA success messages recd	N	Y	Release RAAs Received Success
RAA failure messages recd	N	Y	Release RAAs Received Failure
CCR-T messages processed	N	Y	Release CCRTs Received

Table 21: 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)

Table 21: 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 22: Diameter Event Trigger Statistics

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

Table 23: Diameter Protocol Error Statistics

Display	MPE	MRA	Name
Total errors recd	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count

Display	MPE	MRA	Name
Last time for total error recd	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 24: Diameter Connection Error Statistics

Display	MPE	MRA	Name
Total errors recd	Y	Y	In Error Count
Total errors sent	Y	Y	Out Error Count
Last time for total error recd	Y	Y	Last Error In Time
Last time for total error sent	Y	Y	Last Error Out Time
Diameter Protocol Errors on each error codes	Y	Y	(see specific errors listed in GUI)

Table 25: KPI Interval Statistics

Display	MPE	MRA	Name
Interval Start Time	Y	Y	Interval Start Time
Configured Length (seconds)	Y	Y	Configured Length (Seconds)
Actual Length (Seconds)	Y	Y	Actual Length (Seconds)
Is Complete	Y	Y	Is Complete
Interval MaxTransactions Per Second	Y	Y	Interval Max Transactions Per Second
Interval MaxMRABinding Count	Y	Y	Interval Max MRABinding Count
Interval MaxSessionCount	Y	Y	Interval Max Session Count
Interval MaxPDNConnectionCount	Y	Y	Interval Max PDNConnection Count

Table 26: Policy Statistics

Display	MPE	MRA	Name
Peg Count	Y	N	
Evaluated	Y	N	
Executed	Y	N	

Display	MPE	MRA	Name
Ignored	Y	N	
Policy Details Stats:			
Policy TDF session	Y	N	
Name	Y	N	
Evaluated	Y	N	Eval Count
Executed	Y	N	Trigger Count
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	
Policy ADC-Rule-Install	Y	N	
Name	Y	N	
Evaluated	Y	N	
Executed	Y	N	
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	
Policy write state on session create	Y	N	
Name	Y	N	

Display	MPE	MRA	Name
Evaluated	Y	N	
Executed	Y	N	
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	
Policy write state on session termination	Y	N	
Name	Y	N	
Evaluated	Y	N	
Executed	Y	N	
Ignored	Y	N	
Total Execution Time (ms)	Y	N	
Max Execution Time (ms)	Y	N	
Avg Execution Time (ms)	Y	N	
Processing Time Stats	Y	N	

Table 27: Quota Profile Statistics Details

Display	MPE	MRA	Name
Peg Count	Y	N	
Application	Y	N	
Session	Y	N	
Total	Y	N	

Table 28: Diameter Sh Statistics

Display	MPE	MRA	Name
UDR messages recd/sent	Y	N	UDR Recv Count\UDR Send Count
UDR messages timeout	Y	N	UDR Timeout Count
UDA success messages recd/sent	Y	N	UDA Recv Success Count\UDA Send Success Count
UDA failure messages recd/sent	Y	N	UDA Recv Failure Count\UDA Send Failure Count
PNR messages recd/sent	Y	N	PNR Recv Count\PNR Send Count
PNA success messages recd/sent	Y	N	PNA Recv Success Count\PNA Send Success Count
PNA failure messages recd/sent	Y	N	PNA Recv Failure Count\PNA Send Failure Count
PUR messages recd/sent	Y	N	PUR Recv Count\PUR Send Count
PUR messages timeout	Y	N	PUR Timeout Count
PUA success messages recd/sent	Y	N	PUA Recv Success Count\PUA Send Success Count
PUA failure messages recd/sent	Y	N	PUA Recv Failure Count\PUA Send Failure Count
SNR messages recd/sent	Y	N	SNR Recv Count\SNR Send Count
SNR messages timeout	Y	N	SNR Timeout Count
SNA success messages recd/sent	Y	N	SNA Recv Success Count\SNA Send Success Count
SNA failure messages recd/sent	Y	N	SNA Recv Failure Count\SNA Send Failure Count
Currently active sessions Y N Active Session Count			
Max active sessions	Y	N	Max Active Session Count
Diameter Sh connections	Y	N	Connect Count

Table 29: Sh Data Source Stats

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

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

Display	MPE	MRA	Name
Max Time spent on unsuccessful subscriptions (ms)	Y	N	Subscription Max Miss Time
Avg Time spent on successful subscriptions (ms)	Y	N	Subscription Avg Hit Time
Avg 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
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 unsubscriptions (ms)	Y	N	Unsubscription Max Hit Time
Max Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Max Miss Time
Avg Time spent on successful unsubscriptions (ms)	Y	N	Unsubscription Avg Hit Time
Avg Time spent on unsuccessful unsubscriptions (ms)	Y	N	Unsubscription Avg Miss Time

Color Threshold Configuration

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

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

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

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

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:

- **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.
- **MRA Binding Count** — The number of bindings (for example, UE or Policy rules and charge function MPE pairs) which are maintained in the MRA.

  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.

- **Transaction Per Second** — The number of diameter requests and answer pairs processed in a second.

Viewing the PDN Connection Count

To view the Packet data network (PDN) connection count report, from the **System Wide Reports** section of the navigation pane, select **PDN Connection Count**.

The **PDN connection count** page is displayed with MRA and Policy server graph tables.

The PDN connection count displays the following:

- **View Raw Data** — The interval data statistics display in the table.
- **Export CSV** — The interval data statistics are exported and displayed in the graph table.
- **View Summary** — The distribution data of the interval statistics are viewed in the graph table.
- **Start Date & Time** — The start date and time for the event of interest. For example, you must select the year, month, and day. The established time must be entered manually and will start after the set duration of 24 hours, 7 days, or 30 days.
- **Duration** — Displays the time duration of the data in a pulldown list. You are provided with the following options:
  - 24 hours
  - 2 days
  - 3 days
  - 4 days
  - 5 days
  - 6 days
  - 7 days

  Note: The default is 24 hours.

- **Show Aggregation** — If the box is checked, the aggregated data of all selected Multimedia Policy Engine (MPEs) or MRAs are displayed in the graph table.

  Note: If a MRA or MPE is not selected, then the chart graph does not display.

- **Refresh** — You are provided with the most recently updated graph table.

Viewing the Session Count

The session counts determine the number of Gx or Gy sessions maintained in the MPE. To view the session count report, from the **System Wide Reports** section of the navigation pane, select **Session Count**.

The **Session Count** page is displayed with interval data statistics.

The session count columns display the following:

- **View Raw Data** — The interval data statistics displayed in the table.
- **Export CSV** — The interval data statistics are exported and displayed in the table.
- **View Summary** — The distribution data of the interval data statistics are viewed in the table.
- **Start Date & Time** — The start date and time for the event of interest. For example, you must select the year, month, and day. The established time must be entered manually and will start after the set duration of 24 hours, or 2, 3, 4, 5, 6, or 7 days.
- **Duration** — Displays the time duration of the data in a pulldown list. You are provided with the following options:
  - 24 hours
  - 2 days
  - 3 days
  - 4 days
  - 5 days
  - 6 days
  - 7 days

  Note: The default is 24 hours.

- **Show Aggregation**— If the box is checked, the aggregated data of all selected MPE or MRA content is displayed in the table.

  Note: If a MRA or MPE is not selected, then the chart graph does not display.

- **Refresh**— You are provided with the most recently updated graph table.

Viewing MRA Binding Count

The MRA binding count determines the number of MRA bindings UE or PCRF pairs maintained in the MRA. To view the MRA binding count report from the **System Wide Reports** section of the navigation pane, select **MRA Binding Count**.

The **MRA Binding Count** page displays with binding count numbers and dates.

The MRA binding count columns display the following:

- **View Raw Data** — The interval data statistics displayed in the graph table.
- **Export CSV** — The interval data statistics are exported and displayed in the graph table.

- **View Summary** — The distribution data of the interval statistics viewed in the graph table.
- **Start Date & Time** — The start date and time for the event of interest. For example, you must select the year, month, and day. The established time must be entered manually and will start after the set duration of 24 hours, or 2, 3, 4, 5, 6, or 7 days.
- **Duration** — Displays the time duration of the data in a pulldown list. You are provided with the following options:
  - 24 hours
  - 2 days
  - 3 days
  - 4 days
  - 5 days
  - 6 days
  - 7 days

  Note: The default is 24 hours.
- **Show Aggregation** — If the box is checked, the aggregated data of all selected MPE or MRA content is displayed in the graph table.
- **Refresh** — You are provided with the most recently updated graph table.

Viewing Transactions Per Second

The transactions per second determines the number of diameter request or diameter answer pairs processed in a second. To view the Transactions per second report from the **System Wide Reports** section of the navigation pane, select **Transactions Per Second**.

The **Transactions Per Second** page displays the Transaction per second MRA and policy server graph tables.

The Transactions per second report columns display the following:

- **View Raw Data** — The interval data statistics displayed in the graph table.
- **Export CSV** — The interval data statistics are exported and displayed in the graph table.
- **View Summary** — The distribution data of the interval statistics viewed in the graph table.
- **Start Date & Time** — The start date and time for the event of interest. For example, you must select the year, month, and day. The established time must be entered manually and will start after the set duration of 24 hours, or 2, 3, 4, 5, 6, or 7 days.
- **Duration** — Displays the time duration of the data in a pulldown list. You are provided with the following options:
  - 24 hours
  - 2 days
  - 3 days
  - 4 days
  - 5 days
  - 6 days
  - 7 days

  Note: The default is 24 hours.

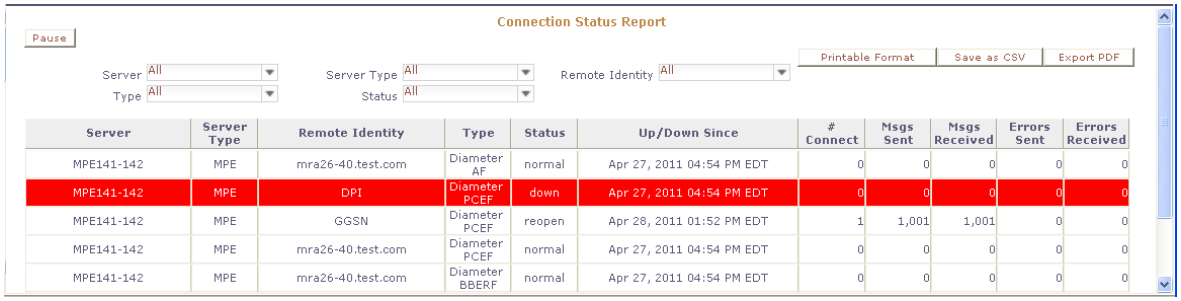
- **Show Aggregation** — If the box is checked, the aggregated data of all selected MPE or MRA content is displayed in the graph table.
- **Refresh** — You are provided with the most recently updated graph table.

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 **Connection Status**.

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



Server	Server Type	Remote Identity	Type	Status	Up/Down Since	# Connect	Msgs Sent	Msgs Received	Errors Sent	Errors Received
MPE141-142	MPE	mra26-40.test.com	Diameter AF	normal	Apr 27, 2011 04:54 PM EDT	0	0	0	0	0
MPE141-142	MPE	DPI	Diameter PCEF	down	Apr 27, 2011 04:54 PM EDT	0	0	0	0	0
MPE141-142	MPE	GGSN	Diameter PCEF	reopen	Apr 28, 2011 01:52 PM EDT	1	1,001	1,001	0	0
MPE141-142	MPE	mra26-40.test.com	Diameter PCEF	normal	Apr 27, 2011 04:54 PM EDT	0	0	0	0	0
MPE141-142	MPE	mra26-40.test.com	Diameter BBERF	normal	Apr 27, 2011 04:54 PM EDT	0	0	0	0	0

Figure 29: Sample Connection Status Report

The report columns display the following data:

- **Server** — name of the associated system
- **Server Type** — **MPE** (Multimedia Policy Engine) or **MRA** (Multi-Protocol Routing Agent)
- **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 bever been established)
- **# Connect** — the number of times that the connection has been re-established

  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.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To select connections from an individual Policy Management cluster, select it from the **Server** list.
- To select connections from a class of Policy Management cluster, select **All** (the default), **MRA**, or **MPE** from the **Server Type** list.
- To select connections from a specific remote identity, select it from the **Remote Identity** list.
- To select connections by connection type, select it from the **Type** list.
- To select connections by connection status, select it from the **Status** list.
- To pause the display of connections, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click on the page number.
- To reformat the report for printing, click **Printable Format**.
- To save the report in comma-separated-value (spreadsheet) format, click **Save as CSV**.
- To save the report as a Portable Document Format file, click **Export PDF**.

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 **Protocol Errors**.

The report columns display the following data:

- **Server** — name of the associated system
- **Server Type** — **MPE** (Multimedia Policy Engine) or **MRA** (Multi-Protocol Routing Agent)
- **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

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.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To select errors from an individual Policy Management cluster, select it from the **Server** list.
- To select errors from a class of Policy Management cluster, select **All** (the default), **MRA**, or **MPE** from the **Server Type** list.
- To select errors from a specific remote identity, select it from the **Remote Identity** list.
- To select errors by error type, select it from the **Error** list.
- To pause the display of errors, click **Pause**. To resume the display, click **Refresh**.
- To display another page of the report, click on the page number.
- To reformat the report for printing, click **Printable Format**.
- To save the report in comma-separated-value (spreadsheet) format, click **Save as CSV**.
- To save the report as a Portable Document Format file, click **Export PDF**.

Viewing the Policy Statistics Report

The policy statistics report provides an aggregate view of policy statistics, with one row for each policy, allowing an administrator to gauge the performance of individual policies. The display is refreshed every ten seconds.

To view the policy statistics report, from the System Wide Reports section of the navigation pane, select **Policy Statistics Report**.

The report columns display the following data:

- **Server Name** — name of the associated system
- **Server Type** — **MPE** (Multimedia Policy Engine) or **MRA** (Multi-Protocol Routing Agent)
- **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

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.

From the report page you can do the following:

- To sort the report on any column, click the column title.
- To display policy statistics for an individual server, select the server's name from the **Server Name** list.
- To display statistics for a specific policy, select that policy's name from the **Policy Name** list.
- To pause the display of errors, click **Pause**. To resume the display, click **Refresh**.
- To change the number of results that appear on the page, click the down arrow for the **Display results per page** list and select the desired number.
- To display another page of the report, click on the page number.
- To reformat the report for printing, click **Printable Format**.
- To save the report in comma-separated-value (spreadsheet) format, click **Save as CSV**.
- To save the report as a Portable Document Format file, click **Export PDF**.

Chapter 25

Upgrade Manager

Topics:

The Upgrade Manager allows you to perform a software upgrade from the GUI. The upgrade process allows a georedundant site to be upgraded in serial order, so no data is lost and there is no down time. During the upgrade process, the Upgrade Manager screen displays the upgrade status. Note that access to this GUI option can be affected by settings on the role setting page.

For specific steps on performing an upgrade, contact the Tekelec *Customer Care Center*.

Upgrade Manager Elements

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

There are three types of elements that appear on the **Upgrade Manager** GUI page: Pulldown menus to filter the servers that appear, the table of filtered servers, and an **Operations** button. The following list of elements describes all of these elements.

Table 30: Upgrade Manager Elements

Element	Description
Name	The table displays the server names of all filtered servers.
Appl Type	Use the **Appl Type** pulldown menu to filter using the application type of server(s) to be upgraded: CMP, MPE, MRA, or All. The table displays all servers in the selected application type.
Site	The table displays the georedundant site name, if any, that is associated with each server.
IP	Use the **IP** pulldown menu to filter by specifying the IP address of a server. The table displays the server with the specified IP address(es).
Server State	Select state of server(s) to be upgraded: Active, Standby, Out-Of-Service, Force Standby, or All. The table displays all servers in the selected state. Server state can appear in different colors, depending on the state displayed.
Prev Release	The table displays the previous release of the server, if known.
Running Release	The table displays the current release of the server.
Replication	Use the **Replication** pulldown menu to filter using the replication status of server(s) to be upgraded: On, Off, or All. The table displays if replication is turned on or off for each server. Replication can appear in different colors, depending on the replication state displayed.
Legacy Replication	Use the **Legacy Replication** pulldown menu to filter using the legacy replication status of server(s) to be upgraded: On, Off, or All. The table displays if legacy replication is turned on or off for each server. Legacy replication can appear in

	different colors, depending on the legacy replication state displayed.
Upgrade Status	The table displays details of last upgrade performed on each server.
<Radio button>	Allows one or more servers to be selected. Used in conjunction with the **Operations** button.
Operations	Click to view more server upgrade options for the server selected using the radio button (last column in table). Options are Push Script, Force Standby (or Cancel Force Standby), Turn Off Replication, and Turn On Legacy Replication. 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 (OK or Cancel). When OK is clicked, a progress bar displays the status of the command completion in a pop-up window.

Chapter 26

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. However, the Change Password option is available to all users (viewer, operator, and administrator).

Configuring System Settings

Within the CMP 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. On the System Settings page, 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.
   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 255 characters.
   l) **Allow policy checkpoint and restore (copies; 0=disallow)** — The number of checkpoints allowed in the system. Valid value range is 0 to 10. If set to 0, the Policy Checkpoint/Restore option is turned off and is no longer visible under the Policy Management heading on the GUI menu. Default value is 0.

4. In the **Invalid Login Threshold** settings section, define the following:
   a) **Enable** — Enables login threshold control.

      By default, this feature is enabled; clear the check box to disable this feature.

   b) **Invalid Login Threshold Value (number of failed logins)** — 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 event log message** — If a user account reaches the threshold, an incident is written to the trace log, including the username and the IP address (in IPv4 or IPv6 format) from which the login attempts were made. The default level is **Warning**; to change the event level, select a different level from the list.

5. The **Password Strength Settings** section lists four character categories: lowercase letters, uppercase letters, numerals, and non-alphabetic characters. You can specify a password strength policy that requires users to create passwords by drawing from these categories:

   - **Require at least categories below** — By default, this setting is 0 (disabled). Select it to require users to include password characters from between one to four of the categories.
   - **Require at least lower-case letter(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 lowercase letters in their passwords.
   - **Require at least upper-case letter(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 uppercase letters in their passwords.
   - **Require at least numeral(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 numerals in their passwords.
   - **Require at least non-alphabetic character(s) (1-64)** — By default, this setting is 0 (disabled). Select it to require users to include from 1 to 64 nonalphabetic characters in their passwords.
   - **Force users with weak password to change password at their next login** — By default, this setting is 0 (disabled). Select it to require users to conform to a new password policy effective the next time they log in.

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

The system settings are configured.

Figure 30: 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@ssword1024.) Users whose passwords do not meet these requirements will be forced to change their passwords the next time they log in.

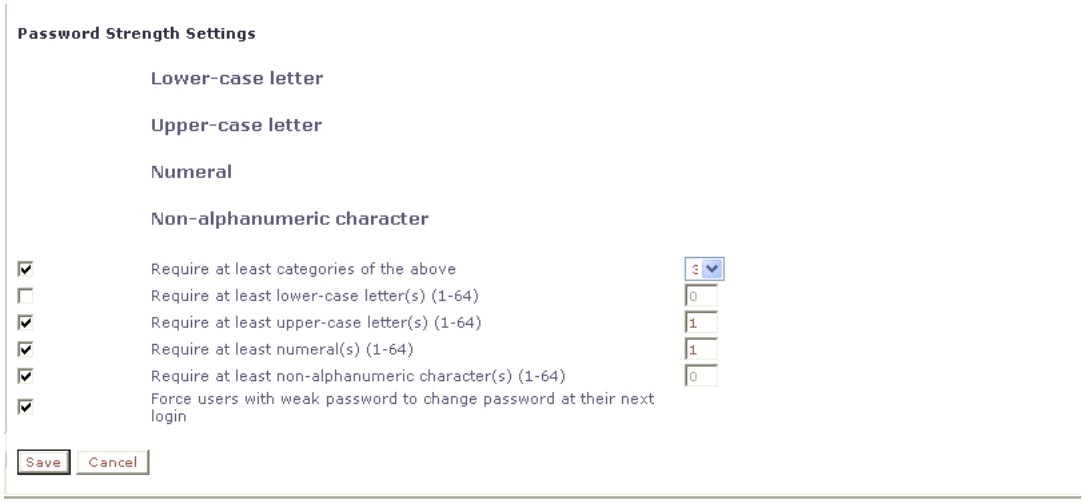


Figure 30: Sample Password Strength Policy

Importing to and Exporting from the CMP Database

In addition to defining manageable objects manually, you can add them to the CMP database using the OSSI XML Interface or by importing them from an XML file. You can also export a list of objects of various types to an XML output file. Additionally, Custom AVP Definitions can be imported as well as exported. 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 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 3rd 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 Definition*.

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).

Tekelec 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 an XML File*).

To use an XML file to input defined objects:

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

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

2. On the Import/Export page, enter the file name of the XML import file, or click **Browse** and, from the standard file open window that appears, locate it.
3. Select the type of import: * (specifies import all types), **Network Elements**, **Tiers**, **Serving Gateway/MCC-MNC Mapping**, **Traffic Profiles**, **Retry Profiles**, **Quotas**, **Match Lists**, **Services**, **Charging Servers**, **Time Periods**, **Applications**, **Monitoring key**, **Custom AVP Definition**, **Policy Table**, **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. Tekelec 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, 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**; that is a different function.

2. Select the type of export: **Network Elements** (the default),**Tiers**, **Serving Gateway/MCC-MNC Mapping**, **Traffic Profiles**, **Retry Profiles**, **Quotas**, **Match Lists**, **Charging Servers**, **Time Periods**, **Applications**, **Monitoring key**, **Custom AVP Definition**, **Policy Table**, **Roles**, **Scopes**, or **Users**.
   If you select **Network Elements**, additional filtering fields are available to help you manage the volume of data being exported. 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.

3. Click **Export**.
   A standard file download window opens, and you are prompted, “Do you want to open or save this file?”
4. Click **Save** to save the file (or **Cancel** to cancel the request).
   Data exported to an XML file. If the operation takes more than five seconds, a progress bar appears.

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

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 role LIadmin cannot be 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.

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), CPU, and memory.

The **Actions** buttons let you restart the CMP software on the server or restart the server itself.

The Trace Log

The Trace Log is part of system administration records notifications for management activity on the CMP system. You can configure the severity level of messages written to the Trace Log; for information, see *Configuring Log Settings*.

To view log information using the Trace Log Viewer:

1. From the **System Administration** section of the navigation pane, select **Trace Log**.
   The Trace Log page opens in the work area.
2. Click **View Trace Log**.
   The Trace Log Viewer window opens. While data is being retrieved, the in-progress message "Scanning Trace Logs" appears.

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. On the Trace Log page, 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** (or **Cancel** to discard your changes).
   The Modify Trace Log Setting page closes.

The trace log configuration is modified.

Viewing the Audit Log

The CMP lets you track and view configuration changes within the system. Using the audit log, you can track and monitor each configuration event, 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 31: 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 31: Audit Log

For a detailed description of an item, click the underlined description. The details of the event display. (*Figure 32: 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 32: 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. On the Audit Log page, 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 an item to audit for display (depending on the CMP mode): **Policy Server**, **Network Element**, **Network Element Group**, **Network Element Link**, **Application**, **MRA**, **Policy**, **Policy Group**, **Account**, **Tier**, **Path**, **Entitlement**, **Alert**, **User**, **Audit**, **OM Statistics**, **Quota**, **Charging Server**, **Service**, **Rating Group**, **Time Period**, **MPE Manager**, **Upgrade Manager**, **Topology Setting**, or **Global Configuration Settings**. By default you can specify three items; click **More Lines** to add an additional item.
   - **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, 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 Data

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. On the Audit Log page, 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** — Enter a date in the format *mm/dd/yyyy*, or click the calendar icon, located to the right of the field, to select a date from the pop-up window.
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 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. On the Audit Log page, click **Export/Purge**.
   The Export and Purge Audit Log Items page opens.
3. In the **Items to Purge** section, enter a date in the format *mm/dd/yyyy*, or click the calendar icon, located to the right of the field, to select a date from the pop-up window.
4. When you finish, click **Purge**.
   You are prompted: "Click 'OK' to purge all audit log items through: *mm/dd/yyyy*."
5. Click **OK** (or **Cancel** to cancel the request).

The data is purged from the audit log.

Managing Scheduled Tasks

The CMP 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: Tekelec strongly recommends that you perform these tasks in the order in which they are listed, or serious system problems can occur. Consult Tekelec Technical Support before changing any task's order.

The tasks include:

- **Stats Files Synchronization #1, 2, 3, 4** — Synchronizes stats files to defined remote server. Up to four synchronization tasks can be defined, and they are scheduled independently. Statistics files are generated and synchronized to external systems only from the active CMP server. 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: 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. 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 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 in order to provide any data through the OM XML interface. The *OSSI XML Interface Definition* document describes the OM Interface and the OM Statistics in detail.

- **Stats File Generator** — Generates stats files by pulling the data from CMP database using OSSI API. This task is also responsible for cleaning up the statistics files. If no external system is configured in any of the Stats File Synchronization tasks, no stats files are generated. Available settings for this task are: Root directory of the local repository, with the default as /var/camiant/stats_export; Stats file retention period, with a default of 72 hours; Stats Type - any stats type can be selected to generate stats, and there is no default value.

- **OSSI Distributor Task** (optional) — Reads from the database topology and subscriber data that has entered the CMP using the OSSI Interface.
- **Subscriber Distributor** — Reads subscriber data from the CMP local database and then distributes it to the appropriate Policy Management devices within the system.
- **Wireless License Tracking Collector** (optional) — Collects wireless Gx sessions for license tracking. This task, disabled by default, is required for license tracking.
- **Wireless License Tracking Session Stats Aggregator** — Collects wireless Gx session statistics for license tracking.
- **Wireless License Tracking Session and Subscriber Stats Aging** — Removes old data from the base and rolled-up session and subscriber statistics tables for wireless license tracking.

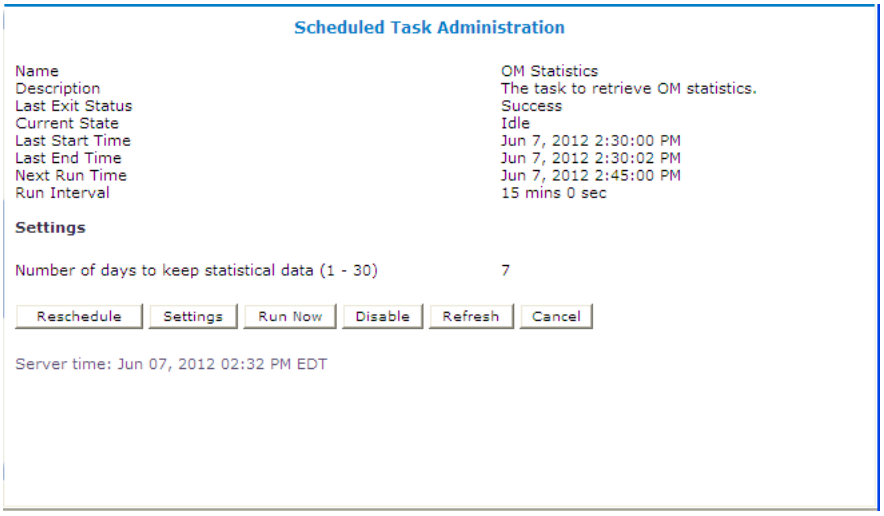
Configuring a Task

To configure an individual task:

1. From the **System Administration** section of the navigation pane, select **Scheduled Tasks**.

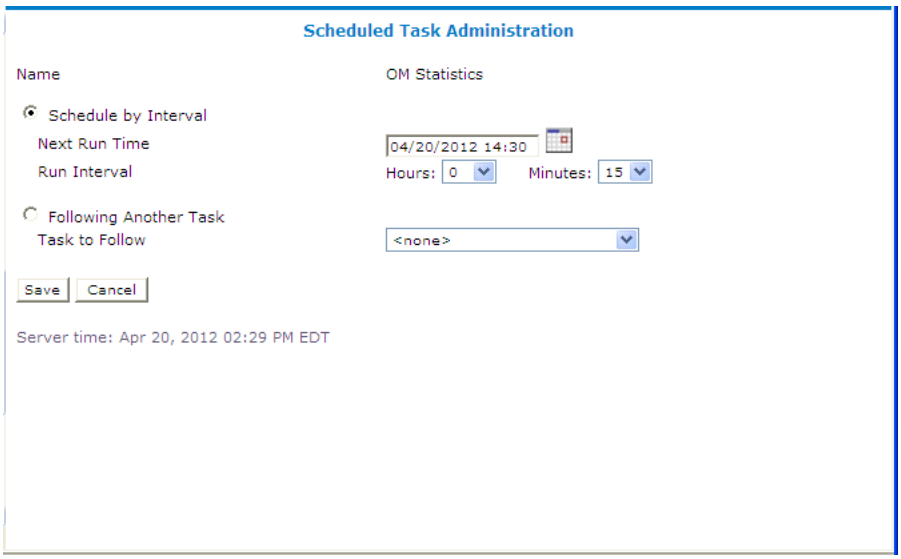
   The Scheduled Task Administration page opens in the work area.

2. To display details about a task, click on its name; the current settings and status are displayed; for example:



3. The options for this task are as follows:

- **Reschedule** — Click to reschedule the time that this task is performed on the Policy Management device:



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

  Valid run intervals are from 0 to 24 hours in 5-minute increments.
- **Following Another Task** — Defines the run time as following the completion of another scheduled task that you select from the list.
- **Settings** — Number of days to keep data; the default is seven days.
- **Run Now** — Runs the process immediately.

  You are prompted: "Click 'OK' to run this task now." Click **OK** to run the task (or **Cancel** to cancel the request).
- **Disable** or **Enable** — Disables or enables the next scheduled execution of this process.

If you click **Disable**, you are prompted: "Click 'OK' to disable this task." Click **OK** (or **Cancel** to cancel the request); the task is disabled and will not run at its next scheduled time, and the button changes to **Enable**.

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

User Management

The CMP lets you configure the following user attributes:

- **Roles** — What a user can do within the CMP.
- **Scopes** — Network element groups and Policy Management device groups that provide a context for a role.
- **Users** — Once you define roles and scopes, you can apply them to user profiles.
- **RADIUS Authentication** — Lets the CMP authenticate users using RADIUS Authentication. These users must match the RADIUS Server account information before access is permitted.

Configuring Roles

Assigning roles to the various users that access the CMP lets you control who can configure and access what within the CMP. The default roles are:

- **Viewer** — Permits read-only access to functions associated with Policy Management device management and configuration. Access is also permitted to limited system administration functions, such as Change Password.
- **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.
- **Administrator** — Permits full read/write access to all functions. You cannot delete the Administrator 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 are set to **Hide** (that is, the functions do not appear to users of the role, so access must be explicitly granted) or **Read-Only**.
4. Enter the following information:
   a) **Name** — The desired name for the new role
   b) **Description/Location** (optional) — Free-form text

c) **Policy Server Privileges** — Defines access to the following MPE device management functions (assigning each the privilege **Hide**, **Read-Only**, or **Read-Write**):

Configuration

Application

Match Lists

Quotas

Services & Rating Groups

Traffic Profiles

Retry Profiles

Charging Server

Time Period

Monitoring Key

AVP Definition

Global Configuration Settings

d) **Subscriber Privileges** — Defines access to the subscriber functions (assigning the privilege **Hide**, **Read-Only**, or **Read-Write**):

Entitlement

Subscriber Tier

Quota Usage

e) **SPR Privileges** — Defines access to the SPR functions (assigning the privilege **Hide**, **Read-Only**, or **Read-Write**):

Subscriber Data

f) **Network Privileges** — Defines access to the network management Paths function, (assigning the privilege **Hide**,**Read-Only**, or **Read-Write**):

Network Element

g) **MRA Privileges** — Defines access to the MRA Configuration function, (assigning the privilege **Hide**, **Read-Only**, or **Read-Write**):

Configuration

h) **Policy Management Privileges** — Defines access to the policy management functions:

Policy Library (with the privileges **Hide**, **Read-Only**, **Read and Deploy**, or **Read, Deploy, and Write**),

Template Library (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Policy Table Library (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Policy Import/Export (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

i) **Platform Setting Privileges** — Defines access to the platform setting functions:

Topology Configuration (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Server Operation (with the privileges **Hide** or **Read-Write**)

j) **Upgrade Manager Privileges** — Defines access to software upgrade functions:

System Maintenance (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

k) **System Administration Privileges** — Defines access to system administration functions:

XML Import/Export (with the privileges **Hide** or **Show**)

Operational Measurements (with the privileges **Hide** or **Read-Only**)

User Management (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Scheduled Tasks (with the privileges **Hide** or **Read-Write**)

Event Log, Audit Log, & Alerts of Policy Server (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Event Log (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Audit Log (with the privileges **Hide**, **Read-Only**, or **Read-Write**)

Audit Log User Info (with the privileges **Hide** or **Show**)

Push Method for Statistics (with the privileges **Read-Only** or **Read-Write**)

Note: This privilege is mainly used for KPI Push in the Scheduled Tasks Administration.

If set to **Read-Only**, the following fields are displayed for the Stats File Generator setting:

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

Task Settings

- **Local Repository**— Root directory of the local repository.
- **Maximum age to keep files (hours)**— Stats file retention period. Defaults to 72 hours.
- **File Format**— Any format can be selected. Defaults to XML.
- **Stats Type**— Any stats type can be selected to generate stats. Defaults to No one. If you do not select a stats type, the task will not run normally.

New tasks are created to synchronize stats files. These tasks will retry if a remote server is unreachable. The following fields are displayed for the Stats Files Synchronization setting:

Remove Server Information

1. Host Name/IP Address
2. Password
3. Path of Remote Repository

- **Retry Limit**— You have a limit of 3 tries in 1 minute intervals.

Note: There are a total of 4 synchronized tasks which are supported but cannot be edited.

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

Privileges are assigned to the role.

Modifying a Role

To modify a role:

1. From the **System Administration** section of the navigation pane, select **User Management**. The content tree displays the User Management group.

2. From the content tree, select the **Roles** group.
   The Role Administration page opens in the work area, displaying existing roles.
3. Select the role to modify.
   The Role page opens.
4. On the Role page, click **Modify**.
   The Modify Role page opens.
5. Modify role information as necessary.
   See *Creating a New Role* for a description of the fields contained within this page.
6. When you finish, click **Save** (or **Cancel** to discard your changes).

The role is modified.

Deleting a Role

You can delete any role except the Administrator role. You cannot delete a role that is in use.

To delete a role:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
2. From the content tree, select the **Roles** group.
   The Role Administration page opens in the work area, displaying existing roles.
3. Delete the role using one of the following methods:
   - From the work area, click the Delete icon located next to the role to delete.
   - From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

   You are prompted: "Are you sure you want to delete this Role?"
4. Click **OK** (or **Cancel** to cancel the request).

The role's information is deleted from the CMP.

Creating a New Scope

The CMP lets you 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. Once you define a scope you can apply it to a user.

To configure a new scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
2. In the content tree, click **Scopes**.
   The Scope Administration page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. On the Scope Administration page, click **Create Scope**.
   The New Scope page opens.
4. Enter the following information:
   a) **Name** — The desired name for the new scope.

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

5. Select the policy server groups included in this scope.
6. Select the network element groups included in this scope.
7. Select the MRA groups included in this scope.
8. When you finish, click **Save** to create the scope (or **Cancel** to discard your changes).

The scope is created.

Modifying a Scope

To modify a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
2. In the content tree, click **Scopes**.
   The Scope Administration page opens in the work area, displaying existing scopes. The default scope is **Global**.
3. On the Scope Administration page, select the scope you want to modify.
   The scope description opens.
4. Click **Modify**.
   The Modify Scope page opens. *Creating a New Scope* describes the fields on this page.
5. Modify scope information as necessary.
6. When you finish, click **Save** (or **Cancel** to discard the request).

The scope is modified.

Deleting a Scope

You can delete any scope except **Global**. To delete a scope:

1. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
2. From the content tree, click **Scopes**.
   The Scope Administration page opens in the work area, displaying existing scopes. (*Figure 33: Deleting a Scope* shows an example.)
3. Delete the role using one of the following methods:
   - From the work area, click the Delete icon, located to the right of the role to delete.
   - From the content tree, select the role to delete (role information displays in the work area), then click **Delete**.

   You are prompted: "Are you sure you want to delete this Scope?"
4. Click **OK** (or **Cancel** to cancel the request).

The scope is deleted.

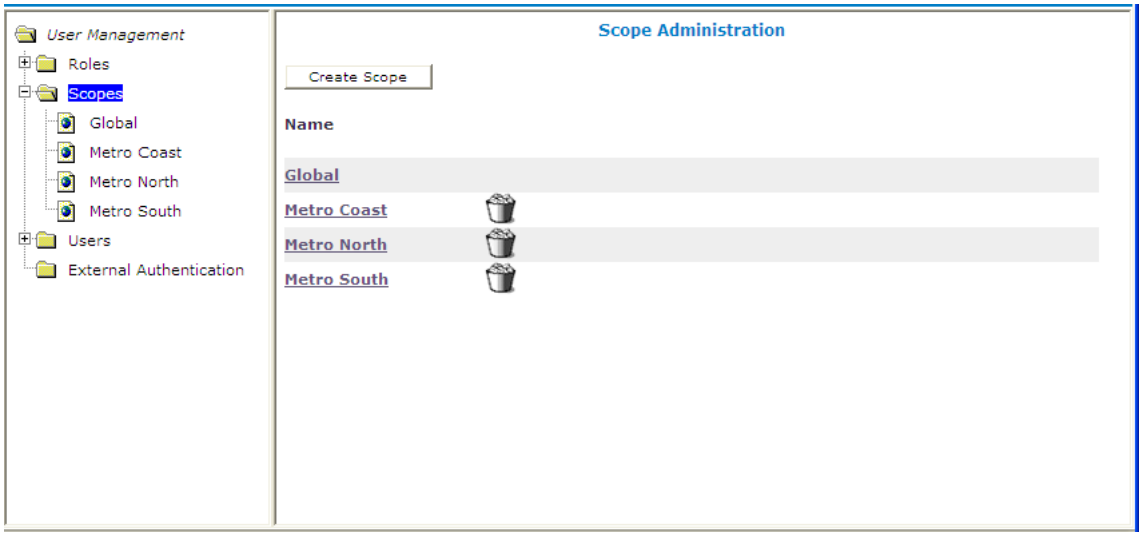


Figure 33: Deleting a Scope

Creating a User Profile

The User Management functions include the tools necessary to create, modify, or delete system user profiles.

The CMP 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, Tekelec recommends changing this value from its 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 in to the CMP 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 attributes:
   a) **Username** — Assign a name to the user profile (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).
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, the user must change passwords on next login.
g) **Role** — Select a role from the pulldown list to assign to the user profile.
h) **Scopes** — Select one or more scopes to assign to the user profile.

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

The user profile is created and stored in the **Users** group.

Modifying a User Profile

To modify a user profile:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
The content tree displays the User Management group.
3. In the content tree, click **Users**.
The User Administration page opens in the work area, displaying existing users.
4. Select the desired user profile from the content tree.
The profile information page opens.
5. Click **Modify**.
The Modify User page opens. (*Figure 34: Modify User Page* shows an example.)
6. Modify the user profile as desired.
(For field descriptions, see *Creating a User Profile*.)
7. When you finish, click **Save** (or **Cancel** to discard your changes).

The user profile is modified.

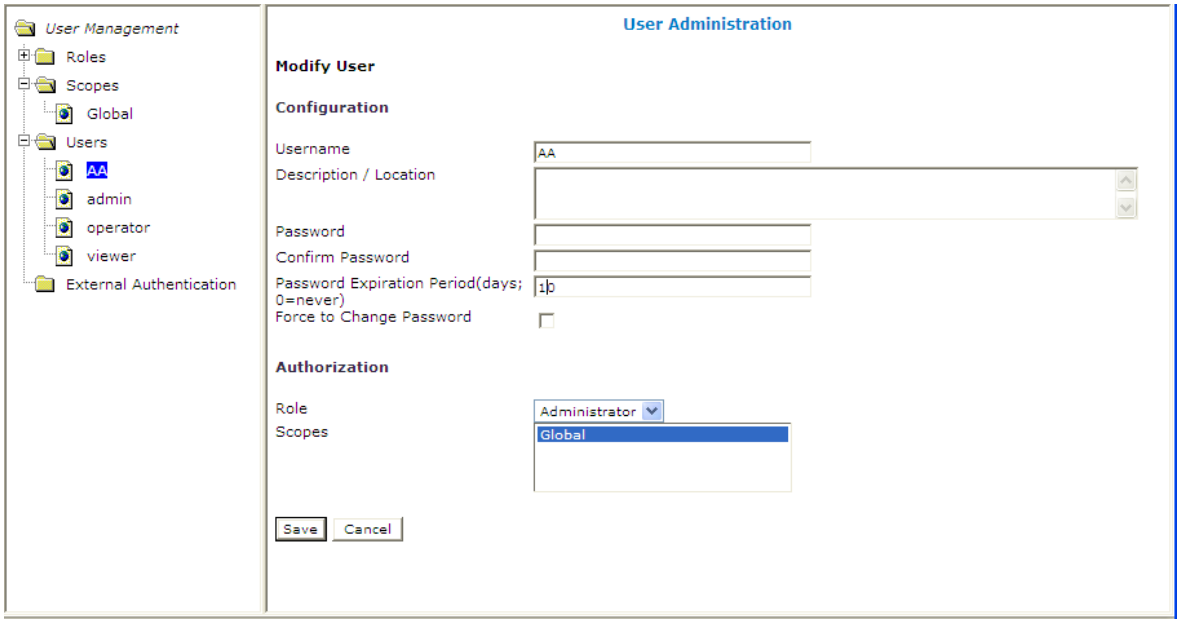
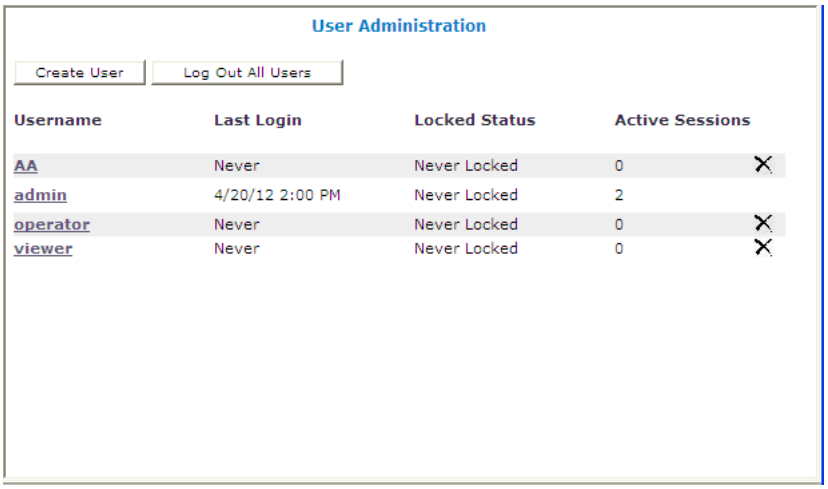


Figure 34: Modify User Page

Deleting a User Profile

You can delete any user profile except **admin**. To delete a user profile:

1. Log in to the CMP as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
3. In the content tree, click **Users**.
   The User Administration page opens in the work area, displaying existing users; for example:



4. Delete the desired user profile using one of the following methods:
   - From the work area, select the delete icon, located to the right of the profile you want to delete.

- From the content tree, select the user profile that you want to delete (profile information displays in the work area), then click **Delete**.

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

5. Click **OK** to delete the user profile (or **Cancel** to abandon the request).

The user profile is deleted.

Locking and Unlocking User Accounts

A user is locked out after exceeding the login failure threshold, or if the **admin** user locks the user out. A locked-out user sees the following message on the login page when attempting to log in: "Your account is locked. Please contact the Administrator."

Note: The **admin** account cannot lock itself.

Locking an Account

To lock a user account:

1. Log in to the CMP 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 desired user profile from the content tree.
   The User Administration page opens.
5. Click **Lock**.
   You are prompted: "Are you sure you want to lock out this user?"
6. Click **OK** (or **Cancel** to cancel the request).
   The account is locked. The page displays: "User account locked successfully." The **Lock** button becomes an **Unlock** button. On the User Administration page, the user's Locked Status changes to "Locked."

Unlocking an Account

To unlock a user account:

1. Log in to the CMP 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 desired user profile from the content tree.
   The User Administration page opens.
4. Click **Unlock**.
   You are prompted: "Are you sure you want to unlock this user?"
5. Click **OK** (or **Cancel** to cancel the request).
   The account is unlocked. The page displays: "User account unlocked successfully." The **Unlock** button becomes a **Lock** button. On the User Administration page, the user's Locked Status changes to "Unlocked by Admin."

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.
3. When you finish, click **Change Password**.

Your password is changed.

RADIUS Authentication and Accounting

The CMP supports RADIUS authentication and accounting. You can configure the CMP 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 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 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 authenticates against its local database (if enabled).
4. If local authentication is not enabled, authentication fails.
5. The user **admin** is always authenticated locally, regardless of configuration settings.

This process provides a fail-safe mechanism for accessing the CMP system even in the face of misconfiguration or network problems that cause the RADIUS servers to become inaccessible.

RADIUS configuration involves three steps:

1. Configuring the RADIUS server to accept authentication (and accounting, if used)

2. Associating user roles and scopes on the CMP system
3. Configuring the CMP system to work with RADIUS

Configuring the RADIUS Server

The RADIUS server must be configured to authenticate clients and users on the CMP system. Some of the configuration values must be consistent with configuration parameters on the CMP. (The RADIUS administrator will be aware of the names and locations of the configuration files.)

Defining the CMP 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 = camiant
        shortname = MPE5
}
client 10.0.10.23 {
        secret = camiant
        shortname = CMP56
}
```

The best practice is to define IP addresses rather than FQDNs. If no netmask is given, the default is /32. The shared secret (in this example, "`camiant`") must be both defined on the RADIUS server and entered into the CMP configuration (see *Enabling RADIUS on the CMP System*). The shortname is used as an alias.

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 to define what attributes to send back to the client. Tekelec provides a VSA dictionary file, dictionary.camiant, in the directory `/opt/camiant/install/radius`. *Figure 35: Tekelec VSA Dictionary For RADIUS* shows the contents of this file. The local RADIUS administrator is responsible for incorporating the Tekelec VSA dictionary into the RADIUS server.

```
========== dictionary.camiant ====================
# Camiant Inc VSA's, from RFC 2548
# The filename given here should be an absolute path.
#
# Place additional attributes or $INCLUDEs here.

VENDOR Camiant 21274
BEGIN-VENDOR Camiant
ATTRIBUTE Camiant-MI-role 1 string
ATTRIBUTE Camiant-SUI-role 2 integer
ATTRIBUTE Camiant-MI-scope 3 string
VALUE Camiant-SUI-role camiantView 101
```

```
VALUE Camiant-SUI-role camiantUser 102
VALUE Camiant-SUI-role camiantService 104
END-VENDOR Camiant
======================
```

Figure 35: Tekelec VSA Dictionary For RADIUS

The Tekelec VSA dictionary specifies three attributes. The attributes **Camiant-SUI-role** is for access to the SUI. The valid values for the SUI role, in ascending order of capability, are **camiantView**, **camiantUser**, and **camiantService**. RADIUS authentication for the SUI will not work unless the dictionary.camiant has been included into RADIUS.

The attributes **Camiant-MI-role** and **Camiant-MI-scope** are for access to the GUI. The GUI has both a scope and a role associated with a user. The responses sent back from the RADIUS server should match what is configured in the CMP. The defaults for the GUI 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 GUI scope is **Global**, and the administrator can create other scopes within the GUI.

Associating Roles and Scopes

The GUI of the CMP 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 Tekelec VSA dictionary, by defining the attributes **Camiant-MI-role** and **Camiant-MI-scope**. The flexibility of roles and scopes can be supported by RADIUS if the Tekelec dictionary is integrated.

The following example defines users who have access at different role levels:

```
Jeff      Password == "garbage"
          Camiant-MI-role = "Administrator",
          Camiant-MI-scope = "Global"

view      Password == "camiant"
          Class = "Viewer",
          Camiant-MI-role = "Viewer",
          Camiant-MI-scope = "Global"
```

However, if Tekelec 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 GUI can use the Class attribute for RADIUS authentication.

To accept the Class attribute for GUI login, define a scope and a role that matches what the RADIUS server returns as the Class attribute. The GUI uses the Class atttribute for both required credentials. For example, consider this user defined in RADIUS:

```
Dawn      Password == "camiant"
          Class = "Viewer"
```

Dawn can get access to the GUI if you have defined both a role named Viewer and a scope named Viewer; the GUI matches the one returned value to both of the required credentials.

Enabling RADIUS on the CMP System

By default, RADIUS Authentication is disabled in the CMP system. Enabling authentication requires admin privileges. The user **admin** is always authenticated against the local database account; thus, the admin user is best suited to setting up RADIUS authentication (see *Creating a User Profile*).

Two configuration parameters must match with the configuration that was put on the RADIUS server:

- **Source of User Credentials** must match up with the user configuration in the RADIUS server, but this will also depend on what is configured in the next parameter.
- If **Action if missing credentials** is set to **Use following defaults** then a user will be authenticated as long as the password is correct. This user could log in even though the class is not valid:

```
test      Password == "tekelec"
          Class = "noone"
```

If **Action if missing credentials** is set to **reject** then the configuration of the user will depend on the configuration of **Source of user credentials**.

To enable RADIUS authentication and accounting:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
3. From the content tree, select **External Authentication**.
   The External Authentication page opens, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**.
   The modify page opens.
5. In the **Configuration** section, select **Enable RADIUS Authentication**.
   Additional fields appear (*Figure 36: External Authentication Configuration Page*).
6. Edit the following fields:
   a) **Enable RADIUS Accounting** — Enables RADIUS accounting on the CMP system.
   This feature is disabled by default. When enabled, the CMP system sends an Accounting-Start message to the accounting server when a user logs in, and an Accounting-Stop message when the user logs out. These messages contain a session ID attribute that uniquely identifies the user session so that it can be matched between Start and Stop.
   b) **Destination for Accounting Messages** — Choose the following from the list:
      - **Both Primary and Secondary** (the default) — Specifies that accounting messages generated for each user session are sent to both the primary and (when configured) secondary RADIUS servers.
      - **Primary (Secondary on error)** — Accounting messages are sent only to the primary server, as long as it is reachable. If the primary accounting server is unreachable, messages are sent to the secondary accounting server.
   c) **NAS IP Address** (required) — IP address, in IPv4 or IPv6 format, of the network access server.
   By default, this is the local host address.
   d) **Use local authentication** — Choose when to use local authentication:
      - **When RADIUS servers timeout**

- **When both RADIUS servers timeout or reject**
- **Never** — Fallback to local authentication is never used (however, the user **admin** is always authenticated locally)

e) **Source of User Credentials** — Choose the following from the list:

- **RADIUS Class** — The value of the Class attribute returned by the server determines both the role and scope.
- **Camiant VSAs —** The value of Camiant VSAs returned by the server determines the role and scope.

f) **Action if Missing Credentials:**

- **Reject** — If you select this option, a user whose login credentials are missing is not logged in.
- **Use following defaults**:

  1. **Default Role** — Role assigned if the user credentials are missing or mismatched. The default is **Viewer**.
  2. **Default Scope** — Scope assigned if the user credentials are missing or mismatched. The default is **Global**.

7. In the **RADIUS Servers** section, edit the following fields:

a) **Primary RADIUS Authentication Server**

- **Server** — FQDN or IP address (in IPv4 or IPv6 format) assigned to the primary authentication server.

  Note: To disable the primary server, delete its IP address.

- **Port** — IP port number of the primary server. The default is port 1812.
- **Timeout (seconds)** — How long the CMP system waits for a response from the server. The default is 3 seconds.
- **Retries** — How many times the CMP system tries to send a message to the server. The default is 3.
- **Shared Secret** — A password-like string that must match between the CMP system and the 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.
- **Shared Secret** — A password-like string that must match between the CMP system and the server. If it does not match, the server ignores all messages from the CMP system.

d) **Secondary RADIUS Accounting Server**

If configured, the secondary accounting server uses the same fields as the primary server.

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

RADIUS Authentication and Accounting is configured.

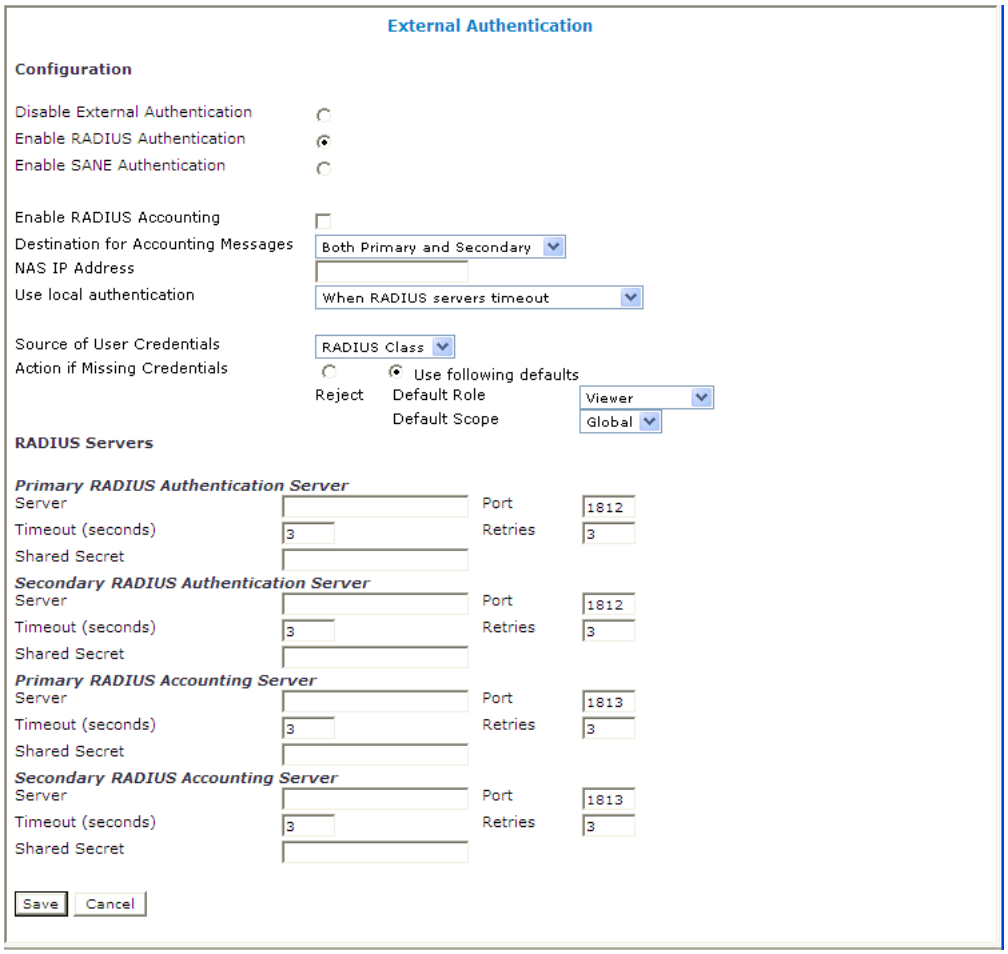


Figure 36: External Authentication Configuration Page

SANE Authentication

The CMP system supports Secure Access to Network Elements (SANE) authentication and authorization. You can configure the CMP system to operate in a SANE network environment such that a user elsewhere in the network can gain single-signon access. When the CMP system is configured to authenticate using SANE, users can log in using a SANE client. (Usage of a SANE client is outside the scope of this document.)

The **admin** account is treated separately. An admin user enters the CMP URL in any supported browser to log in.

The authentication process is as follows:

1. From a SANE client GUI, the user selects the CMP system. A web browser session is launched. An encrypted SANE authentication artifact is sent to the CMP system through the browser.
2. The CMP system forwards the artifact to a SANE server (the SANE responder).
3. If the SANE server verifies the artifact, it returns an assigned role and scope for the user, and the CMP system allows the user to log in accordingly. Otherwise, the CMP system rejects the login request.
4. The user **admin** is always authenticated locally, regardless of configuration settings. (That user clicks on the **Login** link.)

Enabling SANE Authentication on the CMP System

By default, SANE Authentication is disabled in the CMP system. Enabling authentication requires admin privileges. The user **admin** is always authenticated against the local database account; thus, the admin user is best suited to setting up SANE authentication (see *Creating a User Profile*).

To enable SANE authentication:

1. Log in to the CMP system as **admin**.
2. From the **System Administration** section of the navigation pane, select **User Management**.
   The content tree displays the User Management group.
3. From the content tree, select **External Authentication**.
   The External Authentication page opens, displaying the current configuration information. By default, external authentication is disabled.
4. Click **Modify**.
   The modify page opens.
5. In the **Configuration** section, select **Enable SANE Authentication**.
   Additional fields appear.
6. Edit the following fields:
   a) **Artifact Parameter Name** — Name of the artifact parameter. Enter an alphanumeric string. The default is **artifact**.
   b) **Verification for Account** — Choose the following from the list:
      - **On login only** (the default) — The CMP system authenticates the user once, on login. The user is considered authenticated until logout.
      - **On each request** — The CMP system authenticates the user on login, and then again for each HTTP or HTTPS request. If any request is not authenticated, the user is immediately logged out.
   c) **Action if Missing Credentials:**
      - **Reject** — If you select this option, a user login is rejected even if the authentication is successful.
      - **Use following defaults** — If you select this option, a user with missing credentials is allowed to log in, but the system assigns a default role and scope:
        1. **Default Role** — Default role assigned to the user. The default role is **Viewer**.

2. **Default Scope** — Default scope assigned to the user. The default scope is **Global**.

7. In the **SANE Servers** section, edit the following fields:
   a) **SAML Service Name** — Name of the Security Assertion Markup Language service registered with the UDDI server. Enter an alphanumeric string.
   b) **UDDI Inquiry URL** — Universal Description, Discovery and Integration URL, in HTTP or HTTPS format, for the inquiry.
8. When you finish, click **Save** (or **Cancel** to discard your changes).
   The window closes.

SANE authentication is configured on the CMP.

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*.

Appendix A

CMP Modes

Topics:

The functions available in the CMP 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, Tekelec pre-configures servers delivered to customers. 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. For information on setting modes as part of installation, see the *Software Installation Guide*.

CAUTION

CAUTION: CMP modes should only be set in consultation with Tekelec Technical Support. Setting modes inappropriately could result in the loss of network element connectivity, policy function, OM 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 37: Mode Settings Page*). Select modes, sub-modes, and management options, and then click **OK**. The browser page closes and you are automatically logged out. When you next log in, the CMP system reopens in the selected mode.

Table 31: CMP Modes and Sub-Modes briefly describes each mode and sub-mode.

The management options are as follows:

- **Manage Policy Servers** — Manage MPE devices
- **Manage SIP-AM Servers** — Manage Session Initiation Protocol Application Manager (SIP-AM) servers
- **Manage CD-AM Servers** — Manage Content Distribution Network 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 Geo-redundant MPE/MRA** — Manage georedundant MPE or MRA servers
- **Manager is HA (clustered)** — Enable High Availability features

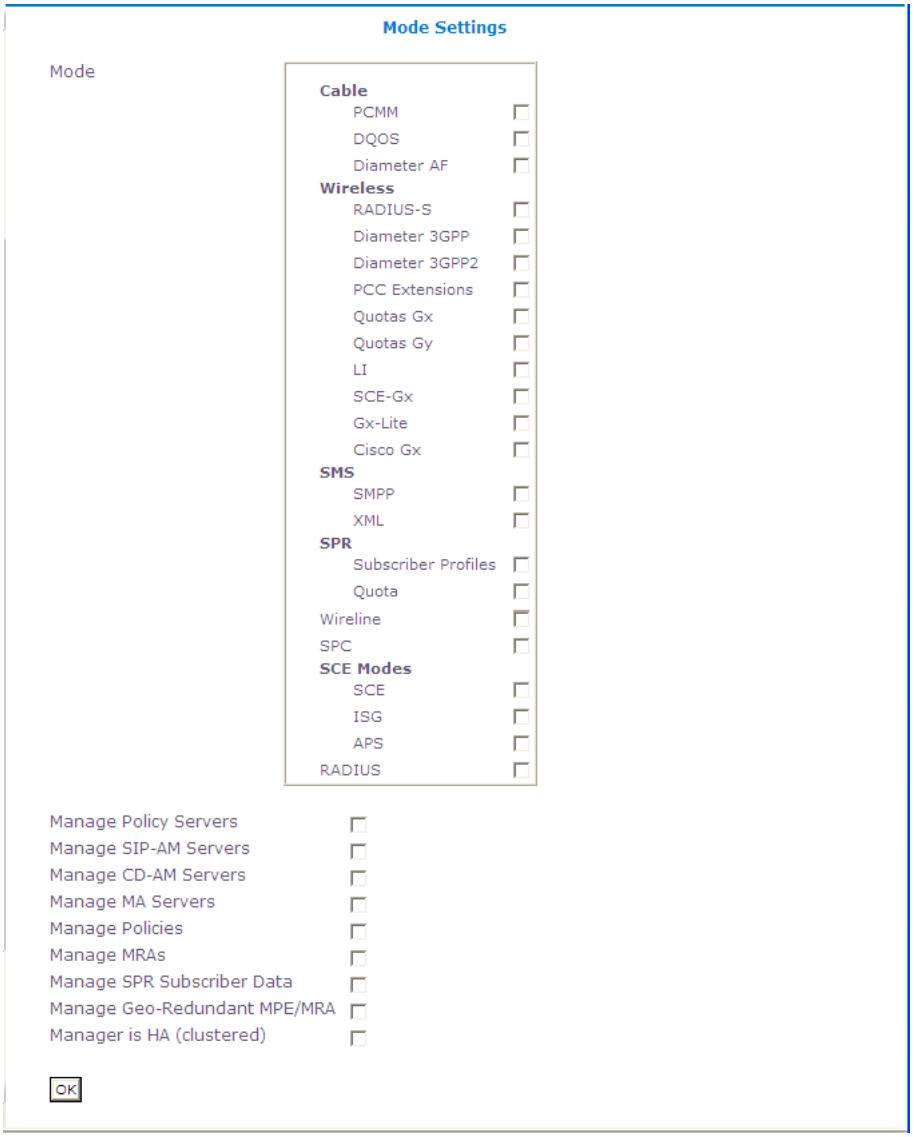


Figure 37: Mode Settings Page

Table 31: CMP Modes and Sub-Modes

Mode	Sub-Mode	Description
Cable Mode	Enables support of a cable carrier environment. Functions are described in the *Configuration Management Platform Cable User's Guide*.	
	PCMM	Supports PacketCable MultiMedia functions.
	DQOS	Supports Dynamic Quality of Service functions.
	Diameter AF	Supports Diameter AF functions.

Mode	Sub-Mode	Description
Wireless Mode	Enables support of a wireless carrier environment. Functions are described in the *Configuration Management Platform Wireless User's Guide*.	
	RADIUS-S	Supports RADIUS-S protocol.
	Diameter 3GPP	Supports Diameter 3GPP protocol.
	Diameter 3GPP2	Supports Diameter 3GPP2 protocol.
	PCC Extensions	Supports Policy and Charging Control functions.
	Quotas Gx	Supports a subscriber quota environment using the Diameter Gx protocol. The Gx protocol supports deep packet inspection (DPI) devices.
	Quotas Gy	Supports a subscriber quota environment using the Diameter Gy protocol
	LI	Supports Lawful Intercept functions. Described in the *Configuring Lawful Intercept Application Note*.
	SCE-Gx	Supports the Cisco Service Control Engine Gx protocol. If this mode is selected, Diameter 3GPP and RADIUS must also be selected, and other Gx sub-modes must not be selected.
	Gx-Lite	Supports the Gx-Lite protocol, a simplified version of 3GPP Gx for use by non-GGSN PCEF vendors that do not have access to network-level information.
	Cisco Gx	Supports the Cisco Gx protocol.
SMS Mode	Enables support of SMS servers. Functions are described in the *Configuration Management Platform Wireless User's Guide*.	
	SMPP	Supports SMS using SMPP protocol.
	XML	Supports SMS using XML.

Mode	Sub-Mode	Description
SPR Mode	Enables support of subscriber database management. Select only one sub-mode. Functions are described in the Subscriber Data Management documentation.	
	Subscriber Profiles	Supports subscriber profile functions.
	Quota	Supports subscriber quotas.
Wireline Mode	Enables support of a wireline carrier environment. Functions are described in the *Configuration Management Platform Wireline User's Guide*.	
SPC Mode	Enables the COPS Application Manager product, which accepts service provisioning requests from a Session Border Controller over the Common Open Policy Service (COPS) protocol. Functions are described in the *Service Provisioning over COPS Application Manager User's Guide*.	
SCE Modes	Enables support of a Cisco Systems environment.	
	SCE	Supports a network containing Service Control Engine (SCE) devices.
	ISG	Supports a network containing Intelligent Services Gateway (ISG) devices.
	APS	Supports router automatic protection switching (APS) functions.
RADIUS Mode	Enables support of RADIUS AAA.	

Glossary

#

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2

A

AAA	Authentication, Authorization, and Accounting
APN	Access Point Name The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.
application	The telecommunications software that is hosted on the platform. A service provided to subscribers to a network; for example, voice over IP (VoIP), video on demand (VoD), video conferencing, or gaming.
AVP	Attribute-Value Pair The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.

B

bps	Bits per second

C

C

CCA	Credit Control Answer The Diameter message that is received from the prepaid rating engine to acknowledge a CCR command.
CCR	Credit Control Request A Diameter message to be sent to a prepaid rating engine to request credit authorization for an SMS.
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.
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. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of

D

	Diameter interfaces, including Rx, Gx, Gy, and Ty.
DNS	Domain Name System A system for converting Internet host and domain names into IP addresses.
DPI	deep packet inspection A form of packet filtering that examines the data and/or header part of a packet as it passes an inspection point. The MPE device uses DPI to recognize the application for establishing QoS or managing quota. See also packet inspection.
DQoS	Dynamic Quality of Service A COPS-based protocol that is part of the Packet Cable standards used to communicate between a CMS and a CMTS for setting up voice calls. An MPE device can be inserted between these two entities to apply additional policy rules as sessions are established.

E

E.164	The international public telecommunication numbering plan developed by the International Telecommunication Union.
ESN	Electronic Serial Number
event	A notification of a state change to a FRU. An event can be an alarm or an informational notification. Events can indicate the assertion or clearing of an alarm. In addition, events can indicate a basic state

E

change that is informational and not related to an alarm condition (for example, card inserted).

F

FQDN

Fully qualified domain name

The complete domain name for a specific computer on the Internet (for example, www.tekelec.com).

G

GGSN

Gateway GPRS Support Node

An edge router that acts as a gateway between a GPRS wireless data network and other networks. The MPE supports GGSN nodes as network elements. See also GPRS, PGW, and SGW.

GPRS

General Packet Radio Service

A mobile data service for users of GSM mobile phones.

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

Gx

The diameter credit control based interface between a PCRF and 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.

I

I

IMS	IP Multimedia Subsystem These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication
IP	Internet Protocol IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
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.

L

LDAP	Lightweight Directory Access Protocol A protocol for providing and receiving directory information in a TCP/IP network.

L

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.
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 device	A physical piece of equipment or a logical (software) entity connected to a network; for example, CMTS, video distribution router, gateway router, or a link. This may also include sub-components of network elements (such as an interface) or lower-level devices such as cable modems or CPEs.
network topology	A map of physical equipment or logical entities in a network.

O

OSSI	Operation Support System Interface An interface to a “back-end” (office) system. The Configuration Management Platform includes an OSSI XML interface.

P

packet inspection	Packet inspection (or shallow packet inspection) is a form of packet filtering that checks the header portion of a packet. See also deep packet inspection.
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function

P

	The ability to dynamically control access, services, network capacity, and charges in a network.
PDN	Packet Data Network A digital network technology that divides a message into packets for transmission.
PLMN	Public Land Mobile Network
policy and charging rules function	See PCRF.
policy group	An ordered group of policies, organized for ease of administration or deployment.

Q

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

R

RADIUS	Remote Authentication Dial-In User Service A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.
RAT	Radio Access Technology
RR	Resource Record

R

	An entry into the DNS database. Depending on their type (e.g. A, SRV, etc.), RRs provide a different set of parameters that characterize a certain DNS name.
RTCP	Real-time Transport Control Protocol Provides out-of-band control information for an RTP flow.

S

SCE	Service Control Engine A deep-packet inspection product.
SDM	Subscriber Data Management
server	Any computer that runs TPD. Could be a Rack Mount Server or a Blade Server.
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

S

SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SPR	Subscriber Profile Repository A logical entity that may be a standalone database or integrated into an existing subscriber database such as a Home Subscriber Server (HSS). It includes information such as entitlements, rate plans, etc. The PCRF and SPR functionality is provided through an ecosystem of partnerships
SSL	Secure Socket Layer
Subscriber Profile Repository	See SPR.

U

UE	User Equipment

V

VoIP	Voice Over Internet Protocol Voice communication based on the IP protocol competes with legacy voice networks, but also with Voice over Frame Relay and Voice and Telephonie over ATM. Realtime response, which is characterized by minimizing frame loss and latency, is vital to voice

V

communication. Users are only prepared to accept minimal delays in voice transmissions.

W

whitelist

Provisioning whitelist.

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.