Oracle® Communications Policy Management

Policy Wizard Reference

Release 12.1.2

E71643 Revision 01

June 2016

ORACLE

Oracle Communications Policy Management Policy Wizard Reference, Release 12.1.2

Copyright © 2014, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: About this Guide.....13

Introduction.....14
How This Guide is Organized.....14
Scope and Audience.....15
Related Publications.....15
Other Publications.....15
Locate Product Documentation on the Oracle Help Center Site.....17
Customer Training.....17
My Oracle Support (MOS).....17
Emergency Response.....18

Chapter 2: The Oracle Communications Policy Management Solution.....19

Configuration Management Platform System.....20
Specifications for Using the CMP System.....20
Logging In.....20
CMP Interface Overview.....21
CMP Icons.....22
Shortcut Selection Keys.....23
Changing a Password.....23
Understanding Policy Rules.....24
About Creating and Using Policies.....24

Chapter 3: Managing Application Profiles.....27

About Application Profiles.....28
Creating an Application Profile.....28
Modifying an Application Profile.....29
Deleting an Application Profile.....29

Chapter 4: Managing Custom AVPs.....31

About Custom AVPs.....32
Creating an AVP.....33

Modifying an AVP....36
Deleting an AVP....37

Chapter 5: Managing Custom Vendors....38
About Custom Vendors....39
Creating a Custom Vendor....39
Modifying a Custom Vendor....39
Deleting a Custom Vendor....40

Chapter 6: Managing Custom VSAs....41
About Custom VSAs....42
Creating a Custom VSA....42
Modifying a Custom VSA....43
Deleting a Custom VSA....44

Chapter 7: Managing Match Lists....45
About Match Lists....46
Creating a Match List....46
Modifying a Match List....47
Deleting a Match List....47

Chapter 8: Managing Media Profiles....49
About Media Profiles....50
Predefined Media Profiles....50
Creating a Media Profile....52
Modifying a Media Profile....53
Deleting a Media Profile....53

Chapter 9: Managing Monitoring Keys....54
About Monitoring Keys....55
Creating a Monitoring Key....55
Modifying a Monitoring Key....56
Deleting a Monitoring Key....56

Chapter 10: Managing Notification Servers....58
About Notification Servers....59
Creating a Notification Server....59

Enabling Notification on an MPE device....60
Viewing a Notification Server....60
Modifying a Notification Server....61
Associating a Notification Server with an MPE device....61
Associating a Notification Server with a Configuration Template....62
Removing the Notification Server Association with an MPE device....62
Deleting a Notification Server....63

Chapter 11: Managing Policy Counter Identifiers....64

About Policy Counter IDs....65
Creating a Policy Counter ID....65
Modifying a Policy Counter ID....66
Deleting a Policy Counter ID....66
Policy Counter ID Groups....66
Creating a Policy Counter ID Group....67
Adding a Policy Counter ID to a Policy Counter ID Group....67
Modifying a Policy Counter ID Group....67
Deleting a Policy Counter ID from a Policy Counter ID Group....68
Deleting a Policy Counter ID Group....68

Chapter 12: Managing Policy Time Periods....69

About Policy Time Periods....70
Creating a Time Period....70
Modifying a Time Period....72
Deleting a Time Period....72
About Time-of-Day Triggers....72

Chapter 13: Managing Presence Reporting Area Lists....74

About Presence Reporting Area Lists....75
Presence Reporting Area List Case Study....75
Creating a Core Network Pre-Configured Presence Reporting Area List....75
Creating a UE-dedicated Presence Reporting Area List....76
Area List Type-Value Combinations....76
Modifying a Presence Reporting Area List....77
Deleting a Presence Reporting Area List....78

Chapter 14: Managing Quotas....79

About Quotas....80

About Quotas Plans....80
Creating a Plan....80
Modifying a Plan....84
Deleting a Plan....84
Example: Creating and Using a Plan....84
About Quotas Passes....86
Creating a Pass....87
Modifying a Pass....89
Deleting a Pass....90
Creating a Pass Group....90
Adding a Pass to a Pass Group....90
Modifying a Pass Group....91
Removing a Pass from a Pass Group....91
Deleting a Pass Group....92

Chapter 15: Managing Quota Conventions....93
About Quota Conventions....94
Creating a Quota Convention....94
Modifying a Quota Convention....95
Associating a Quota Convention with a Plan....96
Deleting a Quota Convention....96

Chapter 16: Managing RADIUS CoA Templates....97
About RADIUS CoA Templates....98
Creating a RADIUS CoA Template....98
Modifying a RADIUS CoA Template....100
Deleting a RADIUS CoA Template....100
Example of Creating and Using a RADIUS CoA Template....101

Chapter 17: Managing Retry Profiles....103
About Retry Profiles....104
Creating a Retry Profile....104
Modifying a Retry Profile....105
Deleting a Retry Profile....106

Chapter 18: Managing Roaming Profiles....108
About Roaming Profiles....109
Creating a Roaming Profile....109

Modifying a Roaming Profile....111
Deleting a Roaming Profile....112

Chapter 19: Managing Service Classes....113

About Service Classes....114
Creating a Service Class....114
Modifying a Service Class....115
Deleting a Service Class....116

Chapter 20: Managing Services and Rating Groups....117

About Services....118
Creating a Service....118
Modifying a Service....118
Deleting a Service....119
About Rating Groups....119
Creating a Rating Group....119
Adding a Service to a Rating Group....120
Modifying a Rating Group....120
Removing a Service from a Rating Group....120
Deleting a Rating Group....121

Chapter 21: Managing Subscriber Keys....122

About Subscriber Keys....123
Creating a Subscriber Key....123
Modifying a Subscriber Key....125
Deleting a Subscriber Key....125

Chapter 22: Managing Traffic Profiles....126

About Traffic Profiles....127
About Traffic Profile Variables....127
Creating a Wireless Traffic Profile....129
Creating a Cable Traffic Profile....139
Modifying a Traffic Profile....147
Deleting a Traffic Profile....148
About Traffic Profile Groups....148
Creating a Traffic Profile Group....149
Adding a Traffic Profile to a Traffic Profile Group....149
Modifying a Traffic Profile Group....149

Removing a Traffic Profile from a Traffic Profile Group....150
Deleting a Traffic Profile Group....150

Chapter 23: Understanding and Creating Policy Rules....151

About Policy Rules....152
Structure and Evaluation of Policy Rules....152
Structure of Policy Rules....152
Evaluating Policy Rules....154
Activating and Deactivating Policy Rules....156
Using Reference Policies....156
Creating a Policy....157
Modes and the Policy Wizard....162
Organizing Policy Rules....162
Parameters Within Policy Rules....162
Conditions for Writing Policy Rules....163
Policy Condition Categories....163
Request Conditions....164
Application Conditions....232
Network Devices Conditions....242
Device Usage Conditions....253
Mobility Conditions....272
User Conditions....284
Policy SDP Properties Conditions....345
State Variables Conditions....352
Policy Context Property Conditions....360
Policy Method Conditions....363
Time-of-Day Conditions....363
Policy Counter Conditions....368
Notification Conditions....376
RADIUS Conditions....379
Actions for Writing Policy Rules....384
Mandatory Policy-Processing Actions....385
Optional Policy-Processing Actions....389
Policy Rule Variables....490
About Policy Rule Variables....490
About Basic Policy Rule Variables....491
Policy Rule Variables for Quotas and Quota Conventions....500
Policy Rule Variables for RADIUS....502

Chapter 24: Managing Policy Rules....505

Displaying a Policy....506
Deploying Policy Rules....506
Modifying and Deleting a Policy....509
Modifying a Policy....509
Deleting a Policy....510
Policy Templates....510
Creating a Policy Template....511
Modifying a Policy Template....511
Deleting a Policy Template....512
Managing a Policy Group....512
Creating a Policy Group....512
Adding a Policy or a Policy Group to a Policy Group....513
Managing Analytics Data Stream Generation for a Policy Group....513
Removing a Policy from a Policy Group....514
Removing a Policy Group....515
Changing the Sequence of Policies or Policy Groups Within a Policy Group....515
Displaying Details of All Policies in a Policy Group....516
Deploying a Policy or Policy Group to MPE Devices....516
Removing a Policy or Policy Group from an MPE Device....517
Changing the Sequence of Deployed Policies or Policy Groups....518
Importing and Exporting Policies, Policy Groups, and Templates....518

Chapter 25: Managing Policy Tables....519

About Policy Tables....520
About Data Matching....521
Policy Matching Operations....521
Example of Data Matching....522
Policy Table Case Study....523
Creating Policy Tables....528
Viewing Policy Tables....530
Associating Policy Tables with a Policy Rule....530
Associating a Parameter with a Policy Table Column....531
Modifying Policy Tables....531
Deleting Policy Tables....532

Chapter 26: Managing Policy Checkpoints....533

About Policy Checkpoints....534
Creating a Policy Checkpoint....534
Viewing and Comparing Policy Checkpoints....535
Restoring a Policy Checkpoint....535

Restoring a Policy Checkpoint to MPE Devices.....536
Deleting a Policy Checkpoint.....537
Glossary.....538

List of Figures

Figure 1: Structure of the CMP Interface....21

Figure 2: Sample AVP Definition....36

Figure 3: Example of Time Slot overlap....71

Figure 4: Example of a Parameter Pop-up....163

Figure 5: Sample Policy Description....506

Figure 6: Policy Deployment....507

Figure 7: Policy Group Deployment....508

Figure 8: Policy Redeployment....509

Figure 9: Policy server selection window....517

Figure 10: Sample Policy Table....530

List of Tables

Table 1: Predefined Media Profiles.....50

Table 2: Example Time Slot definitions.....71

Table 3: Example of a Policy Table.....520

Chapter 1

About this Guide

Topics:

- *Introduction.....14*
- *How This Guide is Organized.....14*
- *Scope and Audience.....15*
- *Related Publications.....15*
- *Locate Product Documentation on the Oracle Help Center Site.....17*
- *Customer Training.....17*
- *My Oracle Support (MOS).....17*
- *Emergency Response.....18*

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

Introduction

This reference contains information about policy rules that you can create, deploy, and manage using the Oracle Communications Policy Management Configuration Management Platform (CMP) system in all operating modes. This reference describes the manageable objects you can include in policy rules, the Policy Wizard you use to create policy rules, and the policy conditions and actions available for your use in writing policy rules.

Conventions

The following conventions are used throughout this guide:

- **Bold text** in procedures indicates icons, buttons, links, or menu items that you can click.
- *Italic text* indicates variables.
- `Monospace text` indicates text displayed on screen or 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 Oracle Communications Policy Management Solution* provides an overview of policies, policy groups, and the Oracle Communications Policy Management Oracle Communications Policy Management Configuration Management Platform (CMP) system, which lets you create, deploy, and manage policy rules and the objects that you can refer to or manipulate within them.
- *Managing Application Profiles* describes how to create and manage application profiles.
- *Managing Custom AVPs* describes how to create and manage custom RADIUS attribute-value pairs (AVPs) in a wireless network.
- *Managing Custom Vendors* describes how to create and manage custom RADIUS vendors in a wireless network.
- *Managing Custom VSAs* describes how to create and manage custom RADIUS vendor-specific attributes (VSAs) in a wireless network.
- *Managing Match Lists* describes how to manage match lists in a wireless network.
- *Managing Media Profiles* describes how to create and manage media profiles in a cable network.
- *Managing Monitoring Keys* describes how to create and manage monitoring keys in a wireless network.
- *Managing Notification Servers* describes how to create and manage notification servers in the CMP system.
- *Managing Policy Counter Identifiers* describes how to create and manage policy counter identifiers in a wireless network.
- *Managing Policy Time Periods* describes how to create and manage policy time periods in a wireless network.
- *Managing Presence Reporting Area Lists* describes how to create and manage Presence Reporting Area lists in a wireless network.
- *Managing Quotas* describes how to create and manage Gx and Gy quotas in a wireless network.

- *Managing Quota Conventions* describes how to create and manage quota conventions in a wireless network.
- *Managing RADIUS CoA Templates* describes how to create, manage, and use RADIUS Change of Authorization (CoA) templates in a wireless network.
- *Managing Retry Profiles* describes how to create and manage retry profiles in a wireless network.
- *Managing Roaming Profiles* describes how to create and manage roaming profiles.
- *Managing Service Classes* describes how to create and manage service classes in a cable network.
- *Managing Services and Rating Groups* describes how to create and manage Gy services and rating groups in a wireless network.
- *Managing Subscriber Keys* describes how to create and manage RADIUS subscriber keys in a wireless network.
- *Managing Traffic Profiles* describes how to create and manage traffic profiles.
- *Understanding and Creating Policy Rules* describes policy rules and lists the rule elements available in the CMP policy wizard for defining rules.
- *Managing Policy Rules* describes how to manage your library of policy rules and policy groups.
- *Managing Policy Tables* describes how to create and manage your library of policy tables.
- *Managing Policy Checkpoints* describes the method of saving CMP objects and their configuration, as well as their association, to the CMP database at a specific point in time.

Scope and Audience

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

- Policy designers, who use the CMP system to design and create policy rules for a carrier network
- Policy administrators, who use the CMP system to deploy, monitor, and manage policy rules in a Policy Management network

Related Publications

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

Other Publications

The following documents are useful for reference:

- PCMM CableLabs specifications:
  - PKT-SP-MM-I05: PacketCable™ Multimedia Specification
  - PKT-SP-DQOS-I12-050812: PacketCable™ Dynamic Quality-of-Service Specification
- Internet Engineering Task Force (IETF) specifications:
  - RADIUS RFCs:

    - RFC 2865: RADIUS
    - RFC 2866: RADIUS Accounting
    - RFC 3576: Dynamic Authorization Extensions to RADIUS
  - Diameter RFCs:
    - RFC 3539: Authentication, Authorization and Accounting (AAA) Transport Profile
    - RFC 3588: Diameter Base Protocol
  - TACACS+ RFC 1492: An Access Control Protocol, Sometimes Called TACACS
  - RFC 3164: The BSD syslog Protocol
- 3rd Generation Partnership Project (3GPP) technical specifications:
  - 3GPP TS 23.003: Numbering, addressing and identification (Release 12)
  - 3GPP TS 23.203: Policy and charging control architecture (Release 13.2)
  - 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses (Release 13)
  - 3GPP TS 29.208: End-to-end Quality of Service (QoS) signalling flows (Release 6)
  - 3GPP TS 29.209: Policy control over Gq interface (Release 6)
  - 3GPP TS 29.211: Rx Interface and Rx/Gx signalling flows (Release 6)
  - 3GPP TS 29.212: Policy and Charging Control over Gx/Sd reference point (Release 13.0)
  - 3GPP TS 29.213: Policy and Charging Control signalling flows and QoS parameter mapping (Release 12.x6)
  - 3GPP TS 29.214: Policy ad Charging Control over Rx reference point (Release 13.0)
  - 3GPP TS 29.219: Policy and Charging Control: Spending limit reporting over Sy reference point (Release 11.3)
  - 3GPP TS 29.229: Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 8)
  - 3GPP TS 29.273: Evolved Packet System (EPS); 3GPP EPS AAA interfaces (Release 12.6)
  - 3GPP TS 32.240: Charging architecture and principles (Release 8)
  - 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging applications (Release 8)
- 3rd Generation Partnership Project 2 (3GPP2) technical specifications:
  - 3GPP2 X.S0013-012-0: Service Based Bearer Control — Stage 2
  - 3GPP2 X.S0013-013-0: Service Based Bearer Control — Tx Interface Stage 3
  - 3GPP2 X.S0013-014-0: Service Based Bearer Control — Ty Interface Stage 3
- 3rd Generation Partnership Project (3GPP) technical specifications:
  - 3GPP TS 23.203: Policy and charging control architecture (Release 8)"
  - 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows (Release 6)"
  - 3GPP TS 29.212: "Policy and Charging Control over Gx/Sd reference point (Release 11)"
  - 3GPP TS 29.213: "Policy and Charging Control signalling flows and QoS parameter mapping (Release 11.4)"
  - 3GPP TS 29.214: "Policy and Charging Control over Rx reference point (Release 8)"
  - 3GPP TS 29.219: "Policy and Charging Control: Spending limit reporting over Sy reference point (Release 11.3)"
  - 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 8)"
  - 3GPP TS 32.240: "Charging architecture and principles (Release 8)"

- 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications (Release 8)"

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.
3. Under the Oracle Communications subheading, click the **`Oracle Communications documentation`** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **`PDF`** link, select **`Save target as`** (or similar command based on your browser), and save to a local folder.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

1. Select **`2`** for New Service Request
2. Select **`3`** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:

- For Technical issues such as creating a new Service Request (SR), Select **1**
- For Non-technical issues such as registration or assistance with MOS, Select **2**

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

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

Emergency Response

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

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

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

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

Chapter

2

The Oracle Communications Policy Management Solution

Topics:

- *Configuration Management Platform System....20*
- *Understanding Policy Rules.....24*

This chapter provides an overview of policy rules, and the Oracle Communications Policy Management Configuration Management Platform (CMP) system, which includes a policy wizard to aid in creating policy rules and manageable objects to which policy rules can refer.

Configuration Management Platform System

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

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

Specifications for Using the CMP System

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

Web Browsers for Wireless and Cable modes	• Mozilla Firefox® release 10.0 or later • Google Chrome version 20.0 or later
Web Browsers for Wireline mode	• Mozilla Firefox release 23.0.1 or later
Monitor	Resolution of 1024 x 768 or greater

Logging In

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

Note: The CMP system also supports carrier-specific network authentication and authorization environments (SANE Authentication and Radius Authentication and Accounting). For information on setting up an alternate login process, see *CMP User Guide*.

Before logging in, you need to know the following:

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

Note: The profile **`admin`** has full access privileges and is the assumed profile used in all procedures described in this document. The default password for the **`admin`** profile is **`policies`**. You cannot delete this user profile, but you should immediately change the password. See *CMP User Guide*.

To log in:

1. Open a Web browser and enter the IP address of the CMP system.
   The login page opens.

   Note: The title and text on the login page are configurable. See *CMP User Guide* for details.

2. Enter your **Username**.
3. Enter your **Password**.
4. Click **Login**.
   The main page opens.

You are logged in.

CMP Interface Overview

You interact with the CMP system through an intuitive and highly portable graphical user interface (GUI) supporting industry-standard Web technologies (for example, SSL, HTTP, HTTPS, IPv4, IPv6, and XML). *Figure 1: Structure of the CMP Interface* shows the structure of the CMP interface.

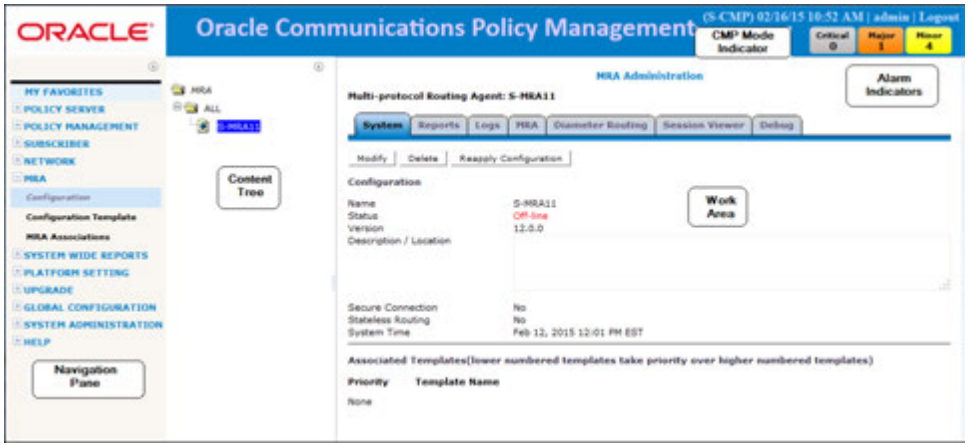


Figure 1: Structure of the CMP Interface

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

You can bookmark options in the Navigation pane by right-clicking the option and selecting **Add to Favorite**. Bookmarked options can be accessed from the **My Favorites** folder at the top of the Navigation pane. Within the My Favorites folder, you can arrange or delete options by right-clicking the option and selecting **Move Up**, **Move Down**, or **Delete from Favorite**.

You can collapse the navigation pane to make more room by clicking the button in the top right corner of the pane. Click the button again to expand the pane.

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

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

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

Work Area	Contains information that relates to choices in both the navigation pane and the content tree. This is the area in which you perform all work.
Alarm Indicators	Provides visual indicators that show the number of active alarms.
CMP Mode Indicator	If you are in a tiered CMP system, this area indicates if you are on a Network Configuration Management Platform (NW-CMP) or a System Configuration Management Platform (S-CMP) server.

CMP Icons

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

Add	Use this icon to add an item to a list.
Calendar	Use this icon to select a date and, in some cases, time.
Clone	Use this icon to duplicate a selection in a list.
Critical error	Displays in reports to indicate a critical error during the blade replication process.
or Delete	When visible in the work area, selecting the Delete icon deletes an item, removing it from the device. **Note:** Deleting an item from the **ALL** folder also deletes the item from any associated group. A delete verification window opens when this icon is selected.
Details	The binoculars icon displays when there is more details for an item.
Edit	Use this icon to modify a selection in a list.
External Connection	When visible in the work area, indicates which server currently has the external connection (the active server).
Gear	The gear icon displays when a policy references another policy or policy group.
Hide	When visible in the work area, selecting the hide icon removes the item from the current view but does not delete the item. **Note:** The item is only hidden during the current session. The item will be visible the next time a user logs into the CMP system.
Manual	Displays when a field is configured by the user. Hover over this icon to see the name of the device.
Major error	Displays in reports to indicate a major error during the blade replication process.
Minor error	Displays in reports to indicate a minor error during the blade replication process.
or Up/Down	The up and down arrow icons are displayed when you can change the sequential order of items in a list.

<-- --> **Left/Right**	The left and right arrow icons are displayed when it is possible to move an item from one list to another.
OK status	Displays in reports to indicate a that the blade replication process completed without error.
Remove	Removes an item from the group. The item is still listed in the **ALL** group and any other group that has an association with the item. For example, if you remove MPE device PS_1 from policy server group PS_Group2, PS_1 still displays in the **ALL** group.
Selection	This icon occurs in the Policy Wizard. The icon is used to select conditions and actions to add to a policy rule.
Synch broken	When visible in the Upgrade Manager, indicates that the CMP system does not have current information on a server.
Template	Displays when a field is configured by template. Hover over this icon to see the name of the template. Click the icon to view the template.
Virtual Machine	Displays when a Policy Management application is running on a virtual machine (VM).
View Cart	Displays the list of configurable objects selected for the **Export** action.

Shortcut Selection Keys

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

Shift + click	Selects two or more consecutive items. To select consecutive items, select the first item, then press Shift and click the last item to select both items and all items in between.
Control + click	Selects two or more non-consecutive items. To select multiple non-consecutive items, press the Ctrl key as you click 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 the password for any user.

If the system administrator has configured your account for password expiration, you will receive a warning when you log in that you must change your password.

Note: To reset the administrator password, contact *My Oracle Support (MOS)*.

To change a password:

1. From the **System Administration** section of the navigation pane, select **Change Password**.
   The **Change Password** page opens. If your account is set up with a password expiration period, the expiration date is displayed.

2. Enter your **Current Password**.
3. Enter your **New Password**.
4. Re-enter your new password to **Confirm Password**.

   Note: If your new password does not conform to the password strength rules, a validation error message appears that includes valid password criteria. Enter and confirm another password that conforms to the criteria.

5. Click **Change Password**.

Your password is changed.

Understanding Policy Rules

A policy rule is an `If-Then` statement that has a set of conditions and actions. If the conditions are met, the actions are performed. You create policy rules within the CMP system, using a policy wizard that organizes a large number of conditions and actions to assist you in the construction of policy rules. After you create policy rules, you manually deploy the rules 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 activity, so the order of evaluation is also configurable through the CMP system. 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. For example, some cable modems have limits on the number of dynamic flows that they can support. Using policy rules, you can ensure that a cable modem does not exceed this limit.
- Some protocols allow for the provisioning of default Quality of Service (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.
- In many protocols, the policy server acts as an intermediary between the Application Managers and the QoS enforcement devices. Many of these QoS enforcement devices implement proprietary features that are activated through the use of standard (or non-standard) fields in protocol messages. Using policy rules, you can activate these proprietary features on behalf of the Application Managers, thus allowing them to use these features without modification.

About Creating and Using Policies

To create and use policies you must:

1. Create manageable objects – see *About Creating Manageable Objects*
2. Create policy rules that use the objects – see *About Creating and Deploying Policies*

3. Deploy and manage the policy rules – see *About Creating and Deploying Policies*

About Creating Manageable Objects

Wireless Mode Objects

The manageable objects for Wireless mode of the CMP system are:

- Create application profiles, which specify protocol information to associate each request with an application. This task is described in *Managing Application Profiles*.
- Create custom attribute-value pairs (AVPs), which are used to encapsulate protocol-specific information with usage monitoring supported by MPE devices in a wireless network. This task is described in *Managing Custom AVPs*.
- Create match lists, which create whitelists and blacklists in a wireless network. This task is described in *Managing Match Lists*.
- Create monitoring keys, which associate quota profiles with policy and charging control (PCC) and application detection control (ADC) rules for usage tracking in a wireless network. This task is described in *Managing Monitoring Keys*.
- Create policy counter identifiers, which define the name, optional description, and default online charging server (OCS) value for which status can be received from the OCS server in a wireless network. This task is described in *Managing Policy Counter Identifiers*.
- Create policy time periods, which are used in policy time-of-day conditions in a wireless network. This task is described in *Managing Policy Time Periods*.
- Create Presence Reporting Area (PRA) lists, which specify areas that can be used in location-specific policies in a wireless network. This task is described in *Managing Presence Reporting Area Lists*.
- Create quotas, which set a limit on a subscriber's usage in a wireless network. This task is described in *Managing Quotas*.
- Create quota passes, which comprise rollovers and top-ups, in a wireless network. This task is described in *Managing Quota Conventions*.
- Create retry profiles, which specify the circumstances under which installation of a PCC rule is retried if the rule is reported to have failed in a wireless network. This task is described in *Managing Retry Profiles*.
- Create Gy services, which identify a class of traffic, and rating groups, which are collections of services, in a wireless network. This task is described in *Managing Services and Rating Groups*.
- Create custom vendors, which are used to support new vendors in a RADIUS Change of Authorization (CoA) message. This task is described in *Managing Custom Vendors*.
- Create custom vendor-specific attributes (VSAs), which are used to encapsulate data specific to a non-standard vendor device. This task is described in *Managing Custom VSAs*.
- Create RADIUS Change of Authorization (CoA) templates, which are used by MPE devices to respond to RADIUS CoA messages. This task is described in *Managing RADIUS CoA Templates*.
- Create subscriber keys, which are used to identify subscribers based on information received in RADIUS messages. This task is described in *Managing Subscriber Keys*.
- Create traffic profiles, which define default settings for protocol messages. This task is described in *Managing Traffic Profiles*.

Cable Mode Objects

The manageable objects for Cable mode of the CMP system are:

- Create application profiles, which specify protocol information to associate each request with an application. This task is described in *Managing Application Profiles*.

- Create media profiles, which describe audio and video CODECs supported for Rx-to-PCMM translation in a cable network. This task is described in *Managing Media Profiles*.
- Create service classes, which correspond to Data-Over-Cable Service Interface Specification (DOCSIS) traffic descriptions defined in cable modem termination systems (CMTSs) in a cable network. This task is described in *Managing Service Classes*.
- Create custom vendors, which are used to support new vendors in a RADIUS Change of Authorization (CoA) message. This task is described in *Managing Custom Vendors*.
- Create custom vendor-specific attributes (VSAs), which are used to encapsulate data specific to a non-standard vendor device. This task is described in *Managing Custom VSAs*.
- Create RADIUS Change of Authorization (CoA) templates, which are used by MPE devices to respond to RADIUS CoA messages. This task is described in *Managing RADIUS CoA Templates*.
- Create subscriber keys, which are used to identify subscribers based on information received in RADIUS messages. This task is described in *Managing Subscriber Keys*.
- Create traffic profiles, which define default settings for protocol messages. This task is described in *Managing Traffic Profiles*.

Wireline Mode Object

The manageable object for Wireline mode of the CMP system is:

- Create application profiles, which specify protocol information to associate each request with an application. This task is described in *Managing Application Profiles*.

About Creating and Deploying Policies

1. Create policy rules on the CMP system. This step is described in *Understanding and Creating Policy Rules*.
2. Deploy the policy rules from the CMP system to MPE devices, and thereafter manage any changes to the set of deployed rules. This step is described in *Managing Policy Rules*.

Optionally, you can consolidate policy rules with similar structures using policy tables. See *Managing Policy Tables*.

Chapter 3

Managing Application Profiles

Topics:

- *About Application Profiles.....28*
- *Creating an Application Profile.....28*
- *Modifying an Application Profile.....29*
- *Deleting an Application Profile.....29*

This chapter describes how to create and manage application profiles within the CMP system.

An application is a service provided to network subscribers for which you want to manage Quality of Service (QoS).

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. After 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 typically many servers in 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 a policy charging and rules function (PCRF). The MPE device provides PCRF for the CMP server.

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. 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 250 characters long and must not contain quotation marks (") or commas (,).
      - **Description/Location** (optional) — Free-form text.
      - **Connection IP Addresss** — Enter the IP addresses, 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) **Policy Servers associated with this Application**: select a policy server (MPE device) to associate with this network element.
   c) **PCMM**:
      - **Application Manager IDs** — Enter the PCMM AMIDs that are used by Application Managers for this application. Click **Add** to define multiple values. To delete an existing value, select it from the list and click **Delete**.

- **Session Class IDs** — Enter the Session Class IDs that are used by each Application Manager for this application. Click **Add** to define multiple values. To delete an existing value, select it from the list and click **Delete**.

d) **Diameter**:

- **Diameter Identity** — Enter the Diameter identity (typically an FQDN) 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**.
- **AF Application ID** — Enter the **ID** for any application functions associated with the application, (for example, **`af-application-id1`**).
- **APN Match Lists** — Click **Manage...** to open the **Select Match Lists for APNs**. Select one or more APNs from the **Available** field and move them to the **Selected** field by clicking --> (right arrow). To move selected APNs to the available field, click <-- (left arrow).

5. Click **Save**.

The application profile is created. The profile is stored in the **Applications** group and is available for use in a policy.

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. Select the application profile.
   The profile is displayed.
4. Click **Modify**.
   The **Modify Application** page opens.
5. Modify the application profile information.
   See *Creating an Application Profile* for a description of the fields on this page.
6. Click **Save**.

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 (trash can icon), located to the right of the profile.
   - From the content tree, select the application and click **Delete**. A confirmation message displays.
4. Click **OK**.

The application profile is deleted from the CMP database and all MPE devices.

Chapter 4

Managing Custom AVPs

Topics:

- *About Custom AVPs.....32*
- *Creating an AVP.....33*
- *Modifying an AVP.....36*
- *Deleting an AVP 37*

This chapter describes how to create, modify, and delete custom third-party attribute-value pairs (AVPs) in the CMP system.

In a wireless network, custom AVPs are used to encapsulate protocol-specific data for routing, authentication, authorization, and accounting information.

About Custom AVPs

An attribute-value pair (AVP) is used to encapsulate protocol-specific information with usage monitoring supported by the MPE device. Diameter messages such as RAA, CCA, CCR, and RAR are supported by third-party AVP policy conditions. The supported outgoing Diameter messages set or remove third-party AVPs.

Note: The Diameter messages listed are examples only. There are many messages associated with Diameter.

You can create policy conditions to evaluate the presence of both standard (base) and third-party AVPs in Diameter messages or group AVPs during policy execution. A policy condition can check for the presence of both standard and third-party AVPs in incoming Diameter messages and evaluate their values. A policy action can use standard and third-party AVPs for routing, authentication, authorization, and accounting.

Standard AVPs can be included in third-party AVP conditions and actions. To include a standard (base) AVP in a nonstandard application message, or to use a pre-standard AVP as a standard AVP, define it as a custom AVP.

When defined, custom AVPs are located at the end of a parent Diameter message or group AVP. If the parent AVP is null, the custom AVP is inserted at the root level of the message. For example, a custom AVP definition appears at the end of this Charging-Rule-Install 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 ]
*[ customAVP ]
```

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.

A third-party AVP is identified by a unique identifier in the following format:

```
name:vendorId
```

For example:

Condition	`where the request AVP NEW_AVP3:555 value is numerically equal to 2012`
Parameters	The AVP name and vendor ID. In the example, the vendor ID is 555.
Description	A well-defined AVP custom name is referred to if the vendor ID is not specified.

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

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

To create 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. Click **Create AVP Definition**.
   The **New AVP Definition** page opens.
4. Enter information as appropriate:
   a) **AVP Name** (required) — The name you assign to the AVP.
      The name can be up to 255 characters long and must not contain the following characters: `"` `,` `:` `;` `>` `<` `.` (period)
   b) **Description** — Free-form text that identifies the AVP.
      Enter up to 250 characters.
   c) **AVP Code** (required) — A unique numeric value assigned to the new AVP.
   d) **Vendor Id** — Select a vendor from the vendor list.
      To add a vendor to the list, see *Managing Custom Vendors*.
   e) **Protect Flag** (optional) — 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** (required) — Select the data type from the list:
      - **address**
      - **enumerated**
      - **float32**
      - **float64**
      - **grouped**
      - **id**
      - **int32**
      - **int64**
      - **ipFilterRule**
      - **octetString**

- **time**
- **uint32**
- **uint64**
- **uri**
- **utf8String**

i) **Parent AVP** — If the AVP is a member of a grouped AVP, then the parent AVP must be specified. Select one of the following from the list:

- **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**
- **Packet-Filter-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**
- **Vzw-Trigger:12951**

5. Click **Save**.
6. If the AVP name matches the name of a standard AVP, a confirmation message displays. Click **OK** to overwrite the existing AVP.

The AVP is created.

Figure 2: Sample AVP Definition shows an example of a base AVP definition defined as a custom AVP for use in a non-standard application message.

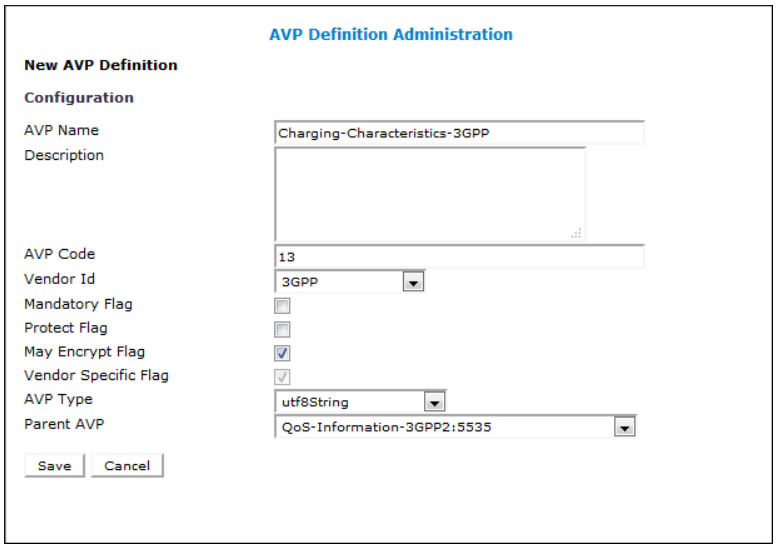


Figure 2: Sample AVP Definition

Modifying an AVP

To modify 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. Select the AVP to modify.
   The **AVP Definition Administration** page opens, displaying 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. Click **Save**.

The AVP is modified.

Deleting an AVP

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

   A confirmation message displays.
3. Click **OK**.

The AVP is deleted.

Chapter 5

Managing Custom Vendors

Topics:

- *About Custom Vendors.....39*
- *Creating a Custom Vendor.....39*
- *Modifying a Custom Vendor.....39*
- *Deleting a Custom Vendor.....40*

This chapter describes how to create, modify, and delete custom vendor definitions in the CMP system.

Custom vendors are used in RADIUS Change of Authorization (CoA) messages.

About Custom Vendors

A custom vendor is used to define a vendor not stored in a RADIUS dictionary that is part of the CMP database. This dictionary includes vendor IDs and text descriptions, and includes standard vendor-specific attributes (VSAs). You can define custom vendors, define VSAs for them, and add them to the dictionary.

Custom VSAs are typically used in a RADIUS Change of Authorization (CoA) message. You can create policy conditions to evaluate the presence of VSAs in RADIUS messages, and to include custom VSAs in RADIUS response messages.

For information on how to create a VSA, see *Managing Custom VSAs*. For information on how to use a VSA in a RADIUS CoA message, see *Managing RADIUS CoA Templates*.

Creating a Custom Vendor

To create a custom vendor:

1. From the **Policy Server** section of the navigation pane, select **Custom Vendors**.
   The content tree displays the Custom Vendors group.
2. Select the **Custom Vendors** group.
   The **Custom Vendor Administration** page opens in the work area.
3. Click **Create Custom Vendor**.
   The **Create Custom Vendor** page opens.
4. Enter information as appropriate:
   a) **Name** (required) — The name you assign to the vendor.
      Enter a string.
   b) **Description** — Free-form text that identifies the vendor.
      Enter up to 250 characters.
   c) **Vendor Id** — Enter the vendor ID.
      Enter a positive integer.
5. Click **Save**.

The custom vendor is defined in the RADIUS dictionary and can now be assigned a vendor-specific attribute (VSA) and used in a policy. See *Managing Custom VSAs* for more information about VSAs.

Modifying a Custom Vendor

To modify a custom vendor definition:

1. From the **Policy Server** section of the navigation pane, select **Custom Vendors**.
   The **Custom Vendor Administration** page opens in the work area, listing the defined custom vendors.

2. Select the custom vendor definition you want to modify.
   The **Custom Vendor Administration** page displays information about the vendor.
3. Click **Modify.**
   The **Modify Custom Vendor** page opens.
4. Modify vendor information.
   For a description of the fields contained on this page, see *Creating a Custom Vendor*.
5. Click **Save**.

The custom vendor definition is modified.

Deleting a Custom Vendor

You cannot delete a custom vendor definition that is used in a CoA template.

To delete a custom vendor definition:

1. From the **Policy Server** section of the navigation pane, select **Custom Vendors**.
   The **Custom Vendor Administration** page opens in the work area, listing the defined custom vendors.
2. Delete the custom vendor using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the vendor.
   - From the content tree, select the vendor and click **Delete**.

   A confirmation message displays.
3. Click **OK**.
   The vendor is removed from the list.

The custom vendor definition is deleted.

Chapter 6

Managing Custom VSAs

Topics:

- *About Custom VSAs.....42*
- *Creating a Custom VSA.....42*
- *Modifying a Custom VSA.....43*
- *Deleting a Custom VSA.....44*

This chapter describes how to create, modify, and delete custom vendor-specific attributes (VSAs) in the CMP system.

In a wireless network, custom VSAs are used to carry vendor-specific data.

Note: Managing custom VSAs is a function that is applicable to Radius CoA mode only.

About Custom VSAs

A vendor-specific attribute (VSA) is used to encapsulate data specific to a vendor device. A VSA consists of a vendor ID and the attribute value. VSAs are stored in a RADIUS dictionary that is part of the CMP database. The dictionary includes a text description of the VSA and type information, and includes standard VSAs. You can define VSAs and add them to the dictionary.

Custom VSAs are typically used in a RADIUS Change of Authorization (CoA) message. You can create policy conditions to evaluate the presence of VSAs in RADIUS messages, and to include custom VSAs in RADIUS response messages.

For information on how to assign values to VSAs, and then send them in a RADIUS CoA message, see *Managing RADIUS CoA Templates*.

Note: Custom VSAs is a function that is applicable to Radius CoA mode only.

Creating a Custom VSA

Note: Custom VSAs is a function that is applicable to Radius CoA mode only.

To create a custom VSA:

1. From the **Policy Server** section of the navigation pane, select **Custom VSA Definitions**.
   The content tree displays the **Custom VSA Definitions** group.
2. Select the **Custom VSA Definitions** group.
   The **VSA Definition Administration** page opens in the work area.
3. Click **Create VSA Definition**.
   The **New VSA Definition** page opens.
4. Enter information as appropriate:
   a) **Name** (required) — The name you assign to the VSA.
      Enter a string.
   b) **Description** — Free-form text that identifies the VSA.
      Enter up to 250 characters.
   c) **VSA Code** (required) — Enter an integer representing the VSA. The default is 0.
   d) **Vendor Id** — Select the available vendor from the pulldown list (the vendor is stored and displayed by a vendor ID):
      - **IETF** (default)
      - **3GPP**
      - **3GPP2**
      - **Camiant**
      - **Cisco**
      - **Cisco-BBSM**
      - **Cisco-VPN3000**
      - **Cisco-VPN5000**
      - **Juniper**

- **Juniper-M-Series**
- (Any custom vendors appear at the end of the list. For information about custom vendors, see *Managing Custom Vendors*.

e) **VSA Type** (required) — Select the attribute data type from the pulldown list:

- **octets**
- **ipv6prefix**
- **text**
- **ipaddr**
- **abinary**
- **integer**
- **evs**
- **string**
- **ifid**
- **enum**
- **ipv6addr**
- **date**
- **tlv**

f) **Compound Type** (required) — Select the description of the attribute structure from the pulldown list:

- **Map**
- **Pair**
- **Single-Value**
- **List**

g) **Field Separator** — If the attribute value has multiple fields, enter the field separator.

h) **Sub-Field Separator** — If the attribute value has sub-fields, enter the sub-field separator.

5. Click **Save**.

The custom VSA is created. The VSA definition displays on the **VSA Definition Administration** page and is defined in the RADIUS dictionary. The custom VSA can be assigned a value. For more information, see *Managing RADIUS CoA Templates*.

Modifying a Custom VSA

To modify a VSA:

1. From the **Policy Server** section of the navigation pane, select **Custom VSA Definitions**.
   The **VSA Definition Administration** page opens in the work area, listing the defined VSAs.
2. Select the VSA to modify.
   The **VSA Definition Administration** page displays information about the VSA.
3. Click **Modify.**
   The **Modify VSA Definition** page opens.
4. Modify VSA information.
   For a description of the fields contained on this page, see *Creating a Custom VSA*.

5. Click **Save**.

The VSA definition is modified.

Deleting a Custom VSA

You cannot delete a VSA that is used in a CoA template.

To delete a VSA:

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

   A confirmation message displays.
3. Click **OK**.

The VSA is deleted.

Chapter 7

Managing Match Lists

Topics:

- *About Match Lists.....46*
- *Creating a Match List.....46*
- *Modifying a Match List.....47*
- *Deleting a Match List.....47*

This chapter describes how to create and manage match lists in the CMP system.

In a wireless network, a match list is a set of defined values that can represent, for example, IDs or Internet addresses. Match lists provide whitelist and blacklist functions in policy rules. Match lists support wildcard matching.

About Match Lists

A match list is a set of values in various categories, including access point names (APNs), subscriber IMSIs, location area codes (LACs), service area codes (SACs), Internet addresses, and user equipment identities. A match list can function as a whitelist (listing items to be included) or a blacklist (listing items to be excluded). By using a match list, you can, for example, apply a policy to all subscribers in a set of LACs, or block access to a list of Internet addresses known to be high risk.

Match lists support wildcards. Using wildcards, a range of values can be specified compactly.

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. 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 40 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
   c) **Type** — Select from the following:
      - **string** (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.
      - **MCC-MNC** — The list consists of Mobile Country Code-Mobile Network Code pairs.
      - **Location Info** — The list consists of locations (formatted as string, wildcard string, or numeric range) and time periods selected from the time periods list. Time period is optional and the default value is none. For information about creating and managing time periods, see *Managing Policy Time Periods*.
   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** (access point name)
      - **User Equipment Identity**
      - **USER IMSI**
      - **USER E.164**
      - **USER SIP URI**

- **USER NAI**
- **Serving MCC-MNC**
- **Cell Identifier**
- **Location Area Code**
- **Service Area Code**
- **Routing Area 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. Click **Save**.

The match list is defined in the CMP database and can now be used in a policy.

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. Click **Save**.

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 Definitions Reference Guide*.

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 (trash can icon), located to the right of the match list.
   - From the content tree, select the match list and click **Delete**.

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

The match list is deleted.

Chapter 8

Managing Media Profiles

Topics:

- *About Media Profiles.....50*
- *Creating a Media Profile.....52*
- *Modifying a Media Profile.....53*
- *Deleting a Media Profile.....53*

This chapter defines how to manage media profiles in the CMP system.

In a cable network, a media profile describes a CODEC supported for Rx-to-PCMM translation.

Note: Media Profiles is a function that is applicable to Cable mode only.

About Media Profiles

Note: Media Profiles is a function that is applicable to Cable mode only.

A media profile describes a CODEC supported for Rx-to-PCMM translation. The MPE device includes a predefined set of media profiles, and you can create new RTP (real-time transport protocol) profiles. After you have defined a media profile in the CMP system, it is automatically deployed to MPE devices.

Media profiles are named *codec_name-transport_type-sample_rate*. Media profiles are mapped to CODECs based on the information received in a session description protocol (SDP) message.

In defining a media profile in the CMP system, you specify its name, transport type, sample rate, frame size (in both milliseconds and bytes), and packetization time.

Note: You cannot create media profiles for the UDPTL or UDP transport types.

Predefined Media Profiles describes the predefined media profiles.

Predefined Media Profiles

The CMP installs a set of Media Profiles. The following tables lists the Predefined media files available.

Table 1: Predefined Media Profiles

CODEC Name	AVT Profile	Frame Length (ms)	Frame Size (bytes)	Bit Rate (kbps)	Sample Rate (kHz)
PCMU	0	0.125	1	64	8
G721	2	0.125	1	64	8
GSM	3	20	33	13.2	8
G723	4	30	24	5.3, 6.3	8
PCMA	8	0.125	1	64	8
G722	9	0.125	1	64	8
G722-48	dynamic	1	6	48	8
G722-56	dynamic	1	7	56	8
G722-64	dynamic	1	8	64	8
G728	15	2.5	5	16	8
G729	18	10	10	8	8
G726-16	dynamic	0.5	1	16	8
G726-24	dynamic	1	3	24	8
G726-32	dynamic	0.25	1	32	8
G726-40	dynamic	1	5	40	8

CODEC Name	AVT Profile	Frame Length (ms)	Frame Size (bytes)	Bit Rate (kbps)	Sample Rate (kHz)
G729D	dynamic	10	8	6.4	8
G729E	dynamic	10	15	11.8	8
GSM-EFR	dynamic	20	31	12.2	8
iLBC	dynamic	20	38	13.33	8
iLBC	dynamic	30	50	15.2	8
BV16	dynamic	5	10	16	8
BV32	dynamic	5	20	32	16
RED	dynamic	10	160	128	8
VMR-WB	dynamic	20	34	13.6	8
SMV0	dynamic	20	22	8.8	8
evrc0	dynamic	20	22		8
evrcb0	dynamic	20	22		8
evrcwb0	dynamic	20	22		8
evrcwb0	dynamic	20	22		16
amr	dynamic	20	32		8
AMR/8000	dynamic	20	14	4.75	8
AMR/8000	dynamic	20	15	5.15	8
AMR/8000	dynamic	20	16	5.9	8
AMR/8000	dynamic	20	18	6.7	8
AMR/8000	dynamic	20	20	7.4	8
AMR/8000	dynamic	20	22	7.95	8
AMR/8000	dynamic	20	27	10.2	8
AMR/8000	dynamic	20	32	12.2	8
amr-wb	dynamic	20	61		16
amr-wb/16000	dynamic	20	18		16
amr-wb/16000	dynamic	20	24		16
amr-wb/16000	dynamic	20	33		16
amr-wb/16000	dynamic	20	37		16
amr-wb/16000	dynamic	20	41		16
amr-wb/16000	dynamic	20	47		16
amr-wb/16000	dynamic	20	51		16

CODEC Name	AVT Profile	Frame Length (ms)	Frame Size (bytes)	Bit Rate (kbps)	Sample Rate (kHz)
amr-wb/16000	dynamic	20	59		16
amr-wb/16000	dynamic	20	61		16

Creating a Media Profile

Note: Media Profiles is a function that is applicable to Cable mode only.

To create a media profile:

1. From the **Policy Server** section of the navigation pane, select **Media Profiles.**
   The content tree displays the **Media Profiles** group.
2. Select the **Media Profiles** group.
   The **Media Profile Administration** page opens in the work area, listing available media profiles.
3. Click **Create Media Profile.**
   The **New Media Profile** page opens.
4. Enter the following information:
   a) **Codec Name** — Unique media subtype assigned to the media profile.
      This is defined in the IANA MIME registration for the CODEC. Enter a string of up to 255 characters.
   b) **Transport Type** — Select from the following:
      - **RTP/AVP** (default) — RTP audio-video profile.
      - **RTP/SAVP** — RTP secure audio-video profile.
      - **RTP/AVPF** — RTP extended audio-video profile with feedback.
   c) **Payload Number** — The payload number.
      Valid payload numbers range from 0 through 127. Enter -1 to indicate an unknown payload number.

      Note: You cannot add a CODEC that is predefined with a payload number in the range of 0 to 96.
   d) **Sample Rate (kHz)** — The sampling rate of the CODEC in KHz.
      The valid range is an integer from 1 through 100 KHz.
   e) **Frame Size in Milliseconds** — The size of one audio frame in milliseconds.
      This is the length of time represented by one audio frame. A single RTP packet may contain multiple audio frames. The bitrate is calculated using the frame size in milliseconds, the frame size in bytes, and the packetization time. The valid range is 0 through 100 ms.
   f) **Frame Size in Bytes** — The size of one audio frame size in bytes.
      This is the size represented by one audio frame. A single RTP packet may contain multiple audio frames. The bitrate is calculated using the frame size in milliseconds, the frame size in bytes, and the packetization time. The valid range is 1 through 1,500 bytes.
   g) **Packetization Time** — The length of time, in milliseconds, represented by the media in a packet.

The bitrate is calculated using the frame size in milliseconds, the frame size in bytes, and the packetization time. The valid range is 1 through 100.

h) **Always Use Default Ptime** — Select to always use the default packetization time, ignoring the value received in the SDP message.

The default is unchecked.

5. Click **Save**.

The media profile is created.

Modifying a Media Profile

To modify a media profile:

1. From the **Policy Server** section of the navigation pane, select **Media Profiles**.
   The content tree opens.
2. From the content tree, select the **Media Profiles** group.
   The **Media Profile Administration** page opens, displaying the list of defined media profiles.
3. Select the media profile you want to modify.
   The profile information for the media displays.
4. Click **Modify**.
   The **Modify Media Profile** page opens.
5. Modify media profile information.
   For a description of the fields contained on this page, see *Creating a Media Profile*.
6. Click **Save**.

The media profile is modified.

Deleting a Media Profile

To delete a media profile:

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

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

The media profile is deleted.

Chapter 9

Managing Monitoring Keys

Topics:

- *About Monitoring Keys.....55*
- *Creating a Monitoring Key.....55*
- *Modifying a Monitoring Key.....56*
- *Deleting a Monitoring Key.....56*

This chapter describes how to create and manage monitoring keys in the CMP system.

In a wireless network, a monitoring key associates quota profiles with policy and charging control (PCC) and application detection control (ADC) rules for usage tracking.

Note: The actual options you see depend on whether or not your CMP system is configured in wireless Gx mode, wireless Gy mode, or both.

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 system.

The PCC Rule Profile is used to populate the Charging Rule Definition attribute-value pair (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 messages, and is compatible with both Release 9 and previous releases. 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 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

To create a monitoring key, perform the following steps:

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. Click **Create Monitoring Key**.
   The **New Monitoring Key** page opens.
4. Enter information 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. Click **Save**.

The monitoring key displays on the **Monitoring Key Administration** page. After you define monitoring keys, you can:

- Select them from the PCC Rule Profile when configuring quota profiles
- Use them in policy actions in the Policy Wizard

Modifying a Monitoring Key

To modify a monitoring key, perform the following steps:

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. 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 the monitoring key.

   For a description of the fields contained on this page, see *Creating a Monitoring Key*.
5. Click **Save**.

The monitoring key definition is modified.

Deleting a Monitoring Key

To delete a monitoring key, perform the following steps:

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 (trash can icon), located to the right of the monitoring key.
   - From the content tree, select the monitoring key and click **Delete**.

   A confirmation message displays.

3. Click **OK**.

The monitoring key is deleted.

Chapter 10

Managing Notification Servers

Topics:

- *About Notification Servers.....59*
- *Creating a Notification Server.....59*
- *Enabling Notification on an MPE device.....60*
- *Viewing a Notification Server.....60*
- *Modifying a Notification Server.....61*
- *Associating a Notification Server with an MPE device.....61*
- *Associating a Notification Server with a Configuration Template.....62*
- *Removing the Notification Server Association with an MPE device.....62*
- *Deleting a Notification Server.....63*

This chapter describes how to create and manage notification servers in the CMP system.

In a wireless network, a notification server controls event notifications driven by policy actions.

About Notification Servers

A notification server processes event notifications in response to policy actions for HTTP request messages. You configure notification servers through the CMP system with SMPP/XML mode enabled.

A notification server can be associated with one or more MPE devices.

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

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

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

Creating a Notification Server

To create a notification server, the CMP system must have the SMPP/XML mode enabled.

To create a notification server:

1. From the **Policy Server** section of the navigation pane, select **Notification Servers**.
   The content tree displays the **Notification Servers** group.
2. Select the **Notification Servers** group.
   The **Notification Server Administration** page opens in the work area.
3. Click **Create Notification Server**.
   The **New Notification Server** page opens.
4. Enter the **Name** (required) for the notification server.

   The name may contain up to 40 characters. When you configure policies using notification servers, you will use this name.
5. Enter a **Description / Location** (optional).

   The description is free-form text containing up to 255 characters.
6. Enter the **Destination URL** (required).

   Use the FQDN or the IP address in either IPv4 or IPv6 format (for example, *http://10.15.20.190:80*). This parameter can contain up to 255 characters. The SMSR creates a persistent connection to this end point.
7. Enter the **Connection Pool [1-5]**.

   Identifies the number of persistent connections to this end point (default is 1).
8. **Keep Alive Interval (seconds)**.

   Indicates the number of seconds to keep the persistent connection active. The valid range is 0 to 300 seconds. The default is 30.
9. In the **Policy Servers associated with this Notification Server** section, do one of the following:
   - Select **ALL** to associate the notification server with all MPE devices.

- Select individual MPE devices.
- Do not select any MPE devices.

10. Click **Save**.

The notification server is created.

After you create a notification server, you can associate it with MPE devices and use it in policy actions in the policy wizard.

Enabling Notification on an MPE device

To enable notification on an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays the **Policy Servers** group.
2. Select the policy server for notification.
   The **Policy Server Administration** page opens in the work area.
3. Click **Modify**.
   The **Modify Policy Server** page appears.
4. In the **Generic Notification Configuration** section, select **Notification Enabled**.
5. Click **Save**.
   The updated **Policy Server** page appears.

The CMP system updates the policy server's configuration to enable notification.

Viewing a Notification Server

To change the configuration of an existing notification server:

1. From the **Policy Server** section of the navigation pane, select **Notification Servers**.
   The content tree displays the **Notification Servers** group.
2. Select the **Notification Servers** group.
   The **Notification Server Administration** page opens in the work area and lists all the notification servers.
3. Select the notification server you want to view.
   The **Notification Server** page appears showing the current configuration for the selected server.
4. From this page:
   - Click **Modify** to change the server configuration.
   - Click **Delete** to remove the server from the system.

Modifying a Notification Server

To change the configuration of an existing notification server:

1. From the **Policy Server** section of the navigation pane, select **Notification Servers**.
   The content tree displays the **Notification Servers** group.
2. Select the **Notification Servers** group.
   The **Notification Server Administration** page opens in the work area and lists all the notification servers.
3. Select the notification server you want to change.
   The **Notification Server** page appears showing the current configuration for the selected server.
4. Click **Modify**.
   The **Modify Notification Server** page appears.
5. Edit the configuration settings as needed.

   Note: If you modify the notification server name and the server is associated with a policy, then the policy is redeployed with the modified name and the following message is displayed:`This notification server name has changed. The following policies have been re-deployed: *Policy Name(s)*`

   The changed notification server configuration is sent to the associated policy servers.
6. Click **Save**.
   The updated **Notification Server** page appears.

The notification server configuration is updated and the any associated policies are redeployed.

Associating a Notification Server with an MPE device

To associate a notification server with an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays the **Policy Servers** group.
2. From the listing of policy servers, select the specific MPE device.
   The **Policy Server Administration** page appears.
3. Select the **Policy Server** tab.
   The **Policy Server** page for the selected device appears.
4. Click **Modify**.
   The **Policy Server** page becomes editable.
5. In the section for **Notification Servers**, click **Manage**.
   A window displays listing the **Available** notification servers and the **Selected** servers.
6. From the **Available** servers list, select the notification server with which to associate the MPE device.
7. Click --> (right arrow icon).
   The selected notification server is added to the **Selected** listing.
8. Click **OK**.

9. Click **Save**.

The association of the MPE device with the notification server is created. If you remove a notification server, the association disappears from the **Notification Servers** listing.

Associating a Notification Server with a Configuration Template

To associate a notification server with a configuration template:

1. From the **Policy Server** section of the navigation pane, select **Configuration Template**.
   The content tree displays the **Templates** group.
2. From the listing of templates, select the specific **Configuration Template**.
   The **Configuration Template Administration** page appears.
3. Select the **Policy Server** tab.
   The **Policy Server** page for the selected template appears.
4. Click **Modify**.
   The **Modify Policy Server** page becomes editable.
5. In the section for **Notification Servers**, click **Manage**.
   A window appears listing the **Available** notification servers and the **Selected** servers.
6. From the **Available** servers list, select the notification server with which to associate the .
7. Click --> (right arrow icon).
   The selected notification server is added to the **Selected** listing.
8. Click **OK**.
9. Click **Save**.

The association of the configuration template with the notification server is created. If you remove a notification server, the association disappears from the **Notification Servers** listing.

Removing the Notification Server Association with an MPE device

To remove an association of a notification server with an MPE device:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.
   The content tree displays the **Policy Servers** group.
2. From the listing of policy servers, select the specific MPE device.
3. Select the **Policy Server** tab.
   The **Policy Server** page for the selected device appears.
4. Click **Modify**.
   The **Policy Server** page becomes editable.
5. In the section for **Notification Servers**, click **Manage**.
   A list displays the **Available** notification servers and the **Selected** servers.
6. In the **Selected** servers list, select the notification server to remove.
7. Click <-- (left arrow icom).

The selected notification server is removed from the **Selected** listing and appears in the **Available** listing.

8. Click **OK**.
9. Click **Save**.

The association of the MPE device with the notification server is removed. If you specified a new notification server, the new association appears in the **Notification Servers** listing.

Deleting a Notification Server

Note: You can only delete a notification server that is not associated with any of the following:

- Policy
- Policy table
- Policy server (MPE device)
- Policy server configuration template

See *Removing the Notification Server Association with an MPE device* for details on removing an association with an MPE device. See *Modifying a Policy* for details on modifying policies.

To delete a notification server:

1. From the **Policy Server** section of the navigation pane, select **Notification Servers**.
   The content tree displays the **Notification Servers** group.
2. Select the **Notification Servers** group.
   The **Notification Server Administration** page opens in the work area.
3. Delete the server using either of the following methods:
   - From the work area, click the **Delete** icon located to the right of the notification server.
   - From the content pane, select the notification server and click **Delete**.

   A message appears asking you to confirm the deletion.
4. Click **OK**.

The notification server is removed from the **Notification Server Administration** page.

Chapter 11

Managing Policy Counter Identifiers

Topics:

- *About Policy Counter IDs.....65*
- *Policy Counter ID Groups.....66*

This chapter describes how to create and manage policy counter IDs in the CMP system.

In a wireless network, a policy counter ID defines the name, optional description, and default online charging server (OCS) value for which status can be received from the OCS server. Policy counter IDs are used in policies, and grouped together here for ease of management.

About Policy Counter IDs

A policy counter ID defines the name, optional description, and default online charging server (OCS) value for which status can be received from the OCS server. After a policy counter ID is defined, you can use policy counter IDs in policies.

In the Sy reference point, an OCS acts as the server and the MPE device acts as the client. For a subscriber, the MPE device requests status from the OCS for a set of policy counter IDs. If the request is successful, the OCS returns the status information for the subscriber to the MPE device and an Sy session is created for the subscriber. The OCS automatically sets up a subscription for the requested policy counter IDs and then notifies the MPE device of any changes to those values.

The Sy protocol provides for four types of messages between the MPE device and the OCS:

1. For the MPE device to request status for an initial set of policy counter IDs and subscribe for notifications for those policy counter IDs
2. For the MPE device to request an update status and possibly update the policy counter ID subscription
3. For the OCS to notify the MPE device of a status change for a set of policy counter IDs for a subscriber
4. For the MPE device to end the Sy session with the OCS, cancelling all subscriptions associated with that session

You can define policy counter IDs in the CMP database and then refer to them in policies.

Creating a Policy Counter ID

To create a policy counter ID:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays the **Policy Counter ID** group. The default group is **ALL**.
2. Select the **Policy Counter ID** group.
   The **Policy Counter ID Administration** page opens in the work area.
3. Click **Create Policy Counter ID**.
   The **New Policy Counter ID** page opens.
4. Enter the **Name** (required).

   The name assigned to the Policy Counter ID. This is the name you use in policies. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
5. Enter the **Identifier** (required).

   Free-form text. This is the key between the MPE device and the OCS.
6. Enter a **Description**

   Free-form text.
7. Enter the **Default Status**.

   Free-form text. The default status for this policy counter ID.
8. Click **Save**.

The policy counter ID is defined in the CMP database and can be used in a policy.

Modifying a Policy Counter ID

To modify a policy counter ID:

1. From the navigation pane, select **Policy Counter ID**.
   The content tree displays the **Policy Counter ID** group.
2. From the content tree, select the **Policy Counter ID** group.
   The **Policy Counter ID Administration** page opens, displaying the list of defined Policy Counter IDs.
3. Select the Policy Counter ID you want to modify.
   Policy Counter ID information is displayed.
4. Click **Modify**.
   The **Policy Counter ID List** page opens.
5. Modify Policy Counter ID information as required.
6. Click **Save**.

The Policy Counter ID 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 Definitions Reference Guide*.

Deleting a Policy Counter ID

You cannot delete a policy counter ID that is being used in a deployed policy condition.

To delete a policy counter ID:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays the **Policy Counter ID** group.
2. From the content tree, select the **Policy Counter IDs** group.
   The **Policy Counter ID Administration** page opens, displaying the list of defined policy counter IDs.
3. Delete the policy counter ID using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the policy counter ID.
   - From the content tree, select the policy counter ID and click **Delete**.

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

The policy counter ID is deleted.

Policy Counter ID Groups

For organizational purposes, you can aggregate policy counter IDs into groups. After a policy counter ID group is created, it can be populated with individual policy counter IDs. The following subsections describe how to manage policy counter ID groups.

Creating a Policy Counter ID Group

To create a policy counter ID group:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays a list of Policy Counter ID groups; the initial group is **ALL**.
2. From the content tree, select the **ALL** group.
   The **Policy Counter ID Administration** page opens in the work area, listing all defined policy counter IDs.
3. Click **Create Group**.
   The **Create Group** page opens.
4. Enter the **Name** of the Policy Counter ID group.

   The name can be up to 250 characters long and must not contain quotation marks (") or commas (,).
5. (Optional) Enter a **Description** of the Policy Counter ID group.
6. Click **Save**.

The Policy Counter ID group is created.

Adding a Policy Counter ID to a Policy Counter ID Group

To add a policy counter ID to a policy counter ID group:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays a list of policy counter ID groups; the initial group is **ALL**.
2. From the content tree, select the policy counter ID group.
   The **Policy Counter ID Administration** page opens in the work area, displaying the contents of the selected policy counter ID group.
3. Click **Add Policy Counter ID**.
   The **Add Policy Counter ID** page opens, displaying the policy counter IDs not already part of the group.
4. Select the policy counter ID you to add. Use the Ctrl or Shift keys to select multiple policy counter IDs.
5. Click **Save**.

The policy counter ID is added to the policy counter ID group.

Modifying a Policy Counter ID Group

To modify a policy counter ID group:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays a list of policy counter IDs; the initial group is **ALL**.
2. From the content tree, select the policy counter ID group you want to modify.
   The **Policy Counter ID Administration** page opens in the work area.
3. Click **Modify**.
   The **Modify Group** page opens.
4. Edit the information.

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

5. Click **Save**.

The group is modified.

Deleting a Policy Counter ID from a Policy Counter ID Group

Deleting a policy counter ID from a policy counter ID group does not delete the ID. To delete a policy counter ID, see *Deleting a Policy Counter ID*.

To delete a policy counter ID from a policy counter ID group:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays the list of policy counter ID groups.
2. From the content tree, select the policy counter ID group.
   The **Policy Counter ID Administration** page opens in the work area, displaying the contents of the selected policy counter ID group.
3. Click (scissors icon), located to the right of the policy counter ID.
4. Click **Save**.

The policy counter ID is deleted from the group.

Deleting a Policy Counter ID Group

Deleting a policy counter ID group does not delete any policy counter IDs that are associated with the group. Profiles remain in the ALL group. You cannot delete the ALL group.

To delete a policy counter ID group:

1. From the **Policy Server** section of the navigation pane, select **Policy Counter ID**.
   The content tree displays the list of policy counter ID groups.
2. From the content tree, select the policy counter ID group.
   The **Policy Counter ID Administration** page opens in the work area, displaying the contents of the policy counter ID group.
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the group.

The policy counter ID group is deleted.

Chapter 12

Managing Policy Time Periods

Topics:

- *About Policy Time Periods.....70*
- *Creating a Time Period.....70*
- *Modifying a Time Period.....72*
- *Deleting a Time Period.....72*
- *About Time-of-Day Triggers.....72*

This chapter describes how to create and manage time periods in the CMP system.

In a wireless network, a policy time period is used in policy time-of-day conditions.

Note: Certain functions of policy time periods are not applicable to all releases including the following options:

- Different days of a month
- Specific day and time in a specific year

About Policy Time Periods

You can define a library of time periods to specify in policy time-of-day conditions and associate the time periods with multiple policies. Each time period can have one or more times slots defined. A time slot can be:

- Specific time of day.
- Different days of the week.
- Different days of a month.
- Specific years.
- Specific day and time in a specific year.
- Specific day and time in every year.

For example a single time period can have following time slots defined:

- Every Monday at 2 o'clock
- On the last day of the month
- On every Valentines day
- On May 17, 2016
- The first three days of March, July, and September

Creating a Time Period

Note: Certain functions of policy time periods are not applicable to all releases including the following options:

- Different days of a month
- Specific day and time in a specific year

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 general information for the time period, enter the following:
   a) **Name** (required) — Name of the time period.
      The name 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.
5. To configure time slots table, use the following table functions:

Note: Certain functions of managing policy time periods are not applicable to all releases including the following options:

- Different days of a month
- Specific day and time in a specific year

- **To add a time slot to the table** — Click **Add**; the **Add Time Slot** window opens. Configure values as appropriate:

  1. **Years** — Select one or more years.
  2. **Months** — Select one or more months.
  3. **Days** — Select one or more days of the month and the direction. To count the days in reverse order (from the last dsy of the month to the first), select **Reverse**.
  4. **Week-Days**—Select one or more week-day.
  5. **Start Time**—Select the starting time.
  6. **End Time**—Select the ending time.

  Note: Time slots cannot overlap. If time slots overlap, an message displays and the slots are not saved. See *Figure 3: Example of Time Slot overlap* for an example of overlapping time slots.

Figure 3: Example of Time Slot overlap

Table 2: Example Time Slot definitions shows how to configure time slots for some example situations.

Table 2: Example Time Slot definitions

Time Slot	Year	Month	Day
Every Valentine's day	null	Feb	14
January 10th 2016 only	2015	Jan	10
The first five days in every month for the first half of the year	null	Jan, Feb, Mar, Apr, May, Jun	1, 2, 3, 4, 5
The last five days in every month for the second half of 2015 and 2016	2015, 2016	Jul, Aug, Sep, Oct, Nov, Dec	Select **Reverse** and 1, 2, 3, 4, 5

- **To clone an attribute in the table** — Select an existing attribute in the table and click **Clone**; the **Clone** window opens with the information for the attribute. Make changes as required.
- **To edit an attribute in the table** — Select the attribute in the table and click **Edit**; the **Edit Response** window opens, displaying the information for the attribute. Make changes as required.
- **To delete an attribute from the table** — Select the attribute in the table and click **Delete**. A confirmation message displays. Click **Delete** to remove the attribute.

6. Click **Save**.

The time period is defined in the CMP database and can be used in a policy time condition.

Modifying 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. Select a time period.
   The **Time Period Administration** page opens.
4. Click **Modify**.
   The fields become editable.
5. Modify Time Period information.

   For information about the fields, see *Creating a Time Period*.
6. Click **Save**.

The time period is defined in the CMP database and can now be used 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 (trash can icon), located to the right of the time period.
   - From the content tree, select the time period and click **Delete**.

   A confirmation messge displays.
4. Click **OK**.

The time period is deleted.

About 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 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 set time and installs the peak policy rule.

The MPE device evaluates policies every 15 minutes, that is 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 ends the updates in progress and processes the new transition by updating the sessions based on the time periods for the new time period.

Time-of-day triggering must be enabled as part of MPE configuration. For more information, see the *CMP User's Guide*.

Chapter 13

Managing Presence Reporting Area Lists

Topics:

- *About Presence Reporting Area Lists.....75*
- *Presence Reporting Area List Case Study.....75*
- *Creating a Core Network Pre-Configured Presence Reporting Area List.....75*
- *Creating a UE-dedicated Presence Reporting Area List.....76*
- *Modifying a Presence Reporting Area List.....77*
- *Deleting a Presence Reporting Area List.....78*

This chapter describes how to create and manage Presence Reporting Area (PRA) lists in the CMP system.

In a wireless network, PRA lists are used to apply policies to users within or outside specific areas.

Note: Managing PRA lists is a function that is applicable to 3GPP mode only.

About Presence Reporting Area Lists

A PRA list is a list of areas in which user equipment presence is reported to the PCRF. PRA lists are used to create location-specific policies that are triggered and applied whenever the user equipment either enters or leaves a PRA. PRA list areas can be designated with various types of value, including tracking area identities (TAI), routing area identities (RAI), Macro eNodeB, Home eNodeB, E-UTRAN cell global identities (ECGI), service area identities (SAI), and cell global identities (CGI).

You can create two types of PRA list: Core Network pre-configured and UE-dedicated. A Core Network pre-configured PRA list is defined on the MME/SSGN side and is used by the CMP in policies. Core Network pre-configured PRA lists are used to create area-specific policies that apply to all or many subscribers on a network. A UE-dedicated PRA list is defined either in the CMP or in subscriber profiles. UE-dedicated PRA lists are used to create area-specific policies that apply to small groups of subscribers on a network.

Presence Reporting Area List Case Study

The following case study demonstrates how PRA lists can be used with policies on a wireless network.

A wireless carrier, Example Inc., uses PRA lists to apply policies to user equipment within specific areas. Example Inc. implements PRA lists in three scenarios: managing QoS in busy areas, allowing location sensitive services, and managing QoS in residential areas.

To manage QoS in busy areas, Example Inc. uses the Core Network pre-defined PRA list CN1. Whenever any subscriber on the network enters an area included in CN1, the PCRF receives a notification and applies a policy that reduces QoS for that subscriber until the subscriber leaves the area included in CN1.

To allow location sensitive services, Example Inc. uses the UE-dedicated PRA list UE1 to manage a service that can only be used while roaming. UE1 establishes a home area for a subscriber or small group of subscribers. Whenever a subscriber whose home area is included in UE1 and who pays for the roaming service leaves the area included in UE1, the PCRF receives a notification and applies a policy that enables the roaming service. Whenever the subscriber enters the area included in UE1, the PCRF receives a notification and applies a policy that disables the roaming service.

To manage QoS in residential areas, Example Inc. uses the UE-dedicated PRA list UE2 to establish a home area for a subscriber. Whenever the subscriber enters the home area UE2, the PCRF receives a notification to increase QoS for that subscriber until the subscriber leaves the home area UE2.

Creating a Core Network Pre-Configured Presence Reporting Area List

To create a Core Network pre-configured PRA list:

1. From the **Policy Server** section of the navigation pane, select **Presence Reporting Area Lists**. The content tree displays the **Presence Reporting Area Lists** group.
2. From the content tree, select the **Presence Reporting Area Lists** group.

The **Presence Reporting Area (PRA) List Administration** page opens in the work area.

3. Click **Create PRA List**.
   The **New PRA List** page opens.
4. Enter the following information:
   a) **Name** — The unique name assigned to the PRA list. The name can be up to 40 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** (optional) — Free-form text.
   c) **ID** — The unique identifying number of the PRA list. The ID must be a numeric value between 0 and 16777215.
   d) **Type** — Select **Core Network pre-configured**.
5. Click **Save**.

The PRA list is created in the CMP database and can now be used in a policy.

Creating a UE-dedicated Presence Reporting Area List

To create a UE-dedicated PRA list:

1. From the **Policy Server** section of the navigation pane, select **Presence Reporting Area Lists**.
   The content tree displays the **Presence Reporting Area Lists** group.
2. From the content tree, select the **Presence Reporting Area Lists** group.
   The **Presence Reporting Area (PRA) List Administration** page opens in the work area.
3. Click **Create PRA List**.
   The **New PRA List** page opens.
4. Enter the following information:
   a) **Name** — The unique name assigned to the PRA list. The name can be up to 40 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** (optional) — Free-form text.
   c) **ID** — The unique identifying number of the PRA list. The ID must be a numeric value between 0 and 16777215.
   d) **Type** — Select **UE-dedicated**.

   The **Area List** page opens in the work area.
5. From the **Area List** page, click **Add**.
   The **Add Area** window opens.
6. Select the type and enter the value.

   For valid type-value combinations, see *Area List Type-Value Combinations*.

   The area is added to the **Area List** page.
7. Click **Save**.

The PRA list is created in the CMP database and can now be used in a policy.

Area List Type-Value Combinations

Type	Value Format
TAI – Tracking Area Identity	**`MCC,MNC,TAC`**

Type	Value Format
RAI – Routing Area Identity	`MCC,MNC,LAC,RAC`
Macro eNodeB	`MCC,MNC,MENB`
Home eNodeB	`MCC,MNC,HENB`
ECGI – E-UTRAN Cell Global Identifier	`MCC,MNC,ECI`
SAI – Service Area Identity	`MCC,MNC,LAC,SAC`
CGI – Cell Global Identity	`MCC,MNC,LAC,CI`

Value	Value Restrictions
MCC – Mobile Country Code	Three decimal digits
MNC – Mobile Network Code	Two or three decimal digits
TAC – Type Allocation Code	A decimal number between 0 and 65535
LAC – Location Area Code	A decimal number between 0 and 65535
RAC – Routing Area Code	A decimal number between 0 and 65535
MENB – Macro eNodeB	A decimal number between 0 and 268435455
HENB – Home eNodeB	A decimal number between 0 and 268435455
SAC – Service Access Code	A decimal number between 0 and 65535
CI – Cell Identity	A decimal number between 0 and 65535

Modifying a Presence Reporting Area List

To modify a PRA list:

1. From the **Policy Server** section of the navigation pane, select **Presence Reporting Area Lists**.
   The content tree displays the **Presence Reporting Area Lists** group.
2. From the content tree, select the **Presence Reporting Area Lists** group.
   The **Presence Reporting Area (PRA) List Administration** page opens in the work area.
3. Select the PRA list you want to modify.
   The PRA list information is displayed.
4. Click **Modify**.
   The **Modify PRA List** page opens.
5. Modify PRA list information as required.

   For information about the fields, see *Creating a Core Network Pre-Configured Presence Reporting Area List* and *Creating a UE-dedicated Presence Reporting Area List*.
6. Click **Save**.

The PRA list is modified.

Deleting a Presence Reporting Area List

To delete a PRA list:

1. From the **Policy Server** section of the navigation pane, select **Presence Reporting Area Lists**.
   The content tree displays the **Presence Reporting Area Lists** group.
2. From the content tree, select the **Presence Reporting Area Lists** group.
   The **Presence Reporting Area (PRA) List Administration** page opens in the work area.
3. Delete the PRA list using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the PRA list.
   - From the content tree, select a PRA list and click **Delete**.

   A confirmation message appears.
4. Click **OK**.

The PRA list is deleted.

Chapter 14

Managing Quotas

Topics:

- *About Quotas.....80*
- *About Quotas Plans.....80*
- *About Quotas Passes.....86*

This chapter describes how to create and manage Gx and Gy quotas in the CMP system.

In a wireless network, 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. Quotas include pass, rollover, and top-up units.

Note: The actual options you see depend on whether or not your CMP system is configured in wireless Gx mode, wireless Gy mode, or both.

About Quotas

A quota specifies restrictions on the amount of data volume, active session time, or service-specific events that a subscriber can consume. A single quota can express limits on any combination of volume, time, or events. Quotas can be associated with a time period during which activity is measured. Using the CMP server, you can define quota profiles. A quota profile specifies default values for quotas and defines how quotas are implemented. There are two types of quota profiles:

Plan	For more information about quota plans, see *About Quotas Plans*.
Pass	For more information about quota passes, see *About Quotas Passes*.

About Quotas Plans

A quota plan describes a subscriber's basic, recurring service. Plans include policy characteristics such as time and volume limits. These characteristics can be computed automatically or through policy rules. Policy actions grant plans, based on a subscriber's tier or entitlement.

A basic quota refers to the quota associated with a plan and is used to handle recurring, periodic quotas typical of post-paid mobile data plans. The controls on a basic quota can be overridden by passes, rollovers, and top-ups.

Creating a Plan

In Gx mode, the MPE device can track and enforce a subscriber's total IP-CAN session time and volume usage 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, specific event, rollover information, and top-up information.

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 plan:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree displays the **Plans** and **Passes** groups.
2. Select the **Plans** group.
   The **Plan Administration** page opens in the work area.
3. Click **Create Plan**.
   The **New Plan** page opens.
4. Enter the following information:
   a) **Name** — The name of the plan. 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 whether the plan is assigned to an individual subscriber or a pool of subscribers. Select one of the following:

- **Subscriber** (default)
- **Pool**

Note: If you select **Pool**, items can be added to support the account (Max Leakage Threshold, Dynamic Grant, etc). After the plans are created, the plans are applied to subscribers.

d) **Enable Dynamic Grant** (optional) — Specifies whether to track grant dynamically for the subscriber. This allows 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.

e) **Max Leakage Threshold (MB)** — Maximum amount by which the usage can be exceeded. The default is 0 MB.

f) **Max Sessions Used For Dynamic Grant**— Number of simultaneous sessions used in the dynamic grant algorithm for granting quota. Enabled when **Enable Dynamic Grant** is selected. The range is 1–2147483647 (Max 32-bit integer). The default is 10 sessions.

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

g) **Minimum Grant Size**— The minimum plan amount granted by the MPE device. Enabled when **Enable Dynamic Grant** is selected. The value of the field depends upon the component (time/service-specific/volume) that is being granted by the MPE device:

- time — minimum number of seconds
- service-specific — minimum number of units
- volume (total/input/output) — minimum number of bytes

The default is 0.

Note: The value of the **Minimum Grant Size** field applies to all of the components that are granted by the MPE device. Make sure that the value reflects the minimum amount for all components. A low value could lead to a high number of messages being generated.

h) **Reset Frequency** — Select how often subscriber plan usage counters are reset: **Monthly** (default), **Weekly**, **Daily**, or **Never**.

- If you select **Monthly**, a **Billing Date Effective Name** field appears. Enter the name of a custom field from the subscriber or pool profile.
- If you select **Weekly**, a **Choose 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.
- If you select **Never**, go to step *Substep m*.

i) **Reset Time Variable** — Optionally, specify a variable allowing the reset time for the plan bucket to be based on any substitutable policy variable in the subscriber profile.
The MPE device uses the variable name and substitutes it to calculate the actual reset time for the plan 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 plan 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 date/time, 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 date/time in the future that is a multiple of a month away from the configured date/time, conserving the time of day.

- For a weekly plan bucket, specify a variable containing either a time of day, in which case the day of the week is taken from the configured fixed day of the week, or a date/time 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 plan bucket, specify a variable containing either a time of day or a date/time. In both cases, the MPE device computes the next reset time based on the time of day.

j) **Report Offset Limit (minutes)**—The maximum minutes the MPE device add to the rest time for the quota when it calculates the session validation time. The range is 0 to 180.

k) **Billing Date Effective Name** — Enter the name of the custom field in subscriber profiles to use for the SPR variable **NewBillingDateEffective**. The default is null. This is a global setting affecting all subscribers.

- To specify a local time in the SPR, the field must be in the format:

```
yyyy-mm-ddThh:mm:ss
```

- To specify a time zone (UTC offset), the field must be in the following format:

```
yyyy-mm-ddThh:mm:ssZ
```

For example, 2011-10-30T00:00:00-5:00).

l) **Collect Reset Statistics**—Enables the generation of reset statistics. If the reset frequency is set to **Never**, this field is hidden and the quota is never reset. The default is disabled.

m) **Initial Total Volume Limit (bytes)** — Gx or Gy mode. Specifies the initial value for total volume units granted by the plan. Select one of the following:

- **None** (default). If you select **None**, then total volume units are not granted.
- **Specify Variable** and enter a variable.
- **Specify Limit** and enter a value.

n) **Initial Upstream Volume Limit (bytes)** — Gx or Gy mode. Specifies the initial value for output volume units granted by the plan. Select one of the following:

- **None** (default). If you select **None**, then output volume units are not granted.
- **Specify Variable** and enter a variable.
- **Specify Limit** and enter a value.

o) **Initial Downstream Volume Limit (bytes)** — Gx or Gy mode. Specifies the initial value for input volume units granted by the plan. Select one of the following:

- **None** (default). If you select **None**, then input volume units are not granted.
- **Specify Variable** and enter a variable.
- **Specify Limit** and enter a value.

p) **Volume Threshold Percentage (%)** — Gy mode only. Enter a threshold percentage.

Below this percentage of volume quota, the charging traffic function must re-authorize.

q) **Initial Time Limit (seconds)** — Gx or Gy mode. Specifies the initial value for session time units granted by the plan. Select one of the following:

- **None** (default). If you select **None**, then time units are not granted.
- **Specify Variable** and enter a variable.
- **Specify Limit** and enter a value.

r) **Time Threshold Percentage (%)** — Gy mode only. Enter a threshold percentage.

Below this percentage of time quota, the charging traffic function must re-authorize.

s) **Initial Service Specific Limit (events)** — Gy mode only. Specifies the initial value for service specific units granted by the plan. Select one of the following:

- **None** (default). If you select **None**, then service specific units are not granted.
- **Specify Variable** and enter a variable.
- **Specify Limit** and enter a value.

t) **Event Threshold Percentage (%)** — Gy mode only. Enter a threshold percentage. When the event quota drops below this percentage, the charging traffic function must re-authorize. Select one of the following:

- **None** (default)
- **Specify Variable** and enter a variable.
- **Specify Limit** and enter a value.

u) **Interim Reporting Interval (seconds)** — Gy mode only. How often the charging traffic function (such as a GGSN) must report quota usage to the MPE device.

- **None** (default)
- **Specify Interval** and enter a value.

5. **Quota Exhaustion Action** — Gy mode only. The action the charging traffic function (such as a GGSN) takes when a subscriber reaches the quota grant:

- **N/A** (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. **Quota Convention** — Select the name of a quota convention (see *About Quota Conventions*). This selection associates the plan with a rollover or top-up.

   If you do not select a quota convention, then a default quota convention is assumed by the system. There is no rollover in a default quota convention.

7. Click **Save**.

The plan is defined in the CMP database and is displayed in the **Plans** group. The plan can now be used in a policy.

Modifying a Plan

To modify a plan:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree opens, displaying the **Plans** and **Passes** groups.
2. From the content tree, select the **Plans** group.
   The **Plan Administration** page opens, displaying the list of defined plans.
3. Select the plan you want to modify.
   The work area displays information about the plan.
4. Click **Modify**.
   The **Modify Plan** page opens.
5. Modify plan information as required.

   For a description of the fields contained on this page, see *Creating a Plan*.
6. Click **Save**.

The plan is modified.

Deleting a Plan

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

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree opens, displaying the **Plans** and **Passes** groups.
2. From the content tree, select the **Plans** group.
   The **Plan Administration** page opens, displaying the list of defined plans.
3. Delete the plan using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the plan.
   - From the content tree, select the plan and click **Delete**.

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

The plan is deleted.

Example: Creating and Using a Plan

An MPE device can grant time, data, or other service-specific units to subscribers. It can also limit grants based on quotas, either against plans or against limited exemptions such as passes, top-ups, and rollovers. The following is a simple wireless Gx example in which a monthly data usage quota is defined, and a policy is written for the MPE device to grant quota upon creation of a new session. The following values are defined and used:

- Plan name: MonthlyDataBasic
- Quota: 5 Gb (5,368,709,120 bytes) monthly
- Quota exhaustion action: Terminate

The policy rule is as follows:

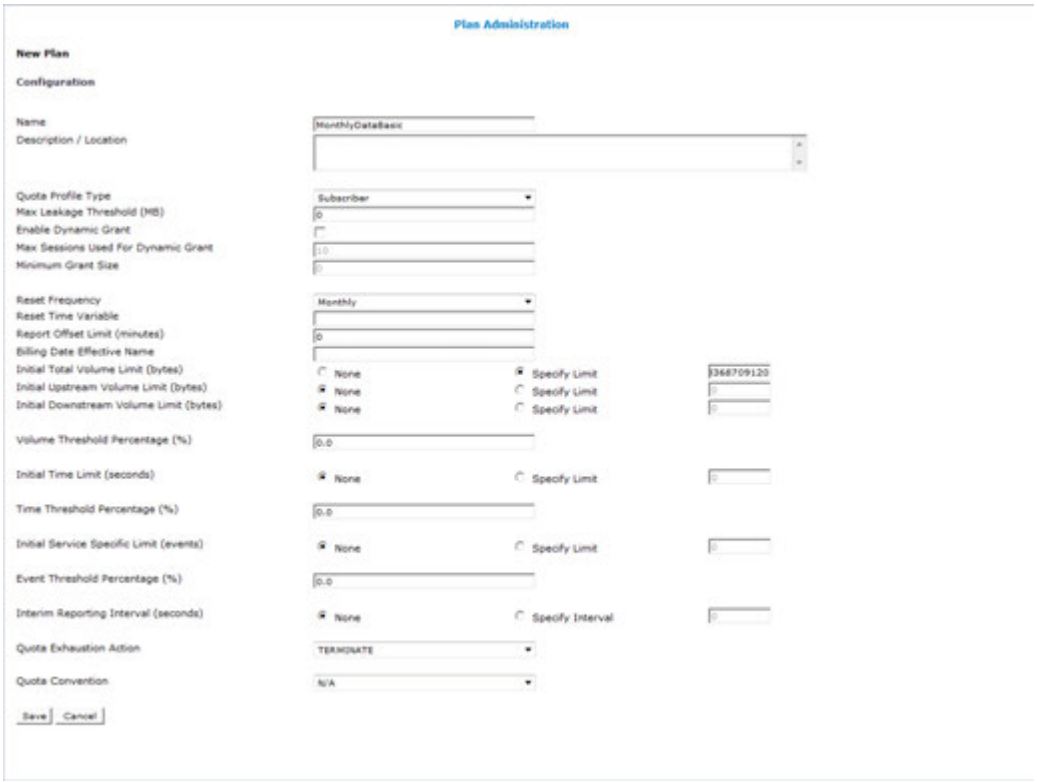
```
where the request is creating a new session
grant total volume to 100 percent used for MonthlyDataBasic
accept message
```

This procedure consists of tasks described elsewhere. The steps must be performed in the order shown.

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**, select the **Plans** folder, and create the plan.

   For more information, see *Creating a Plan*.

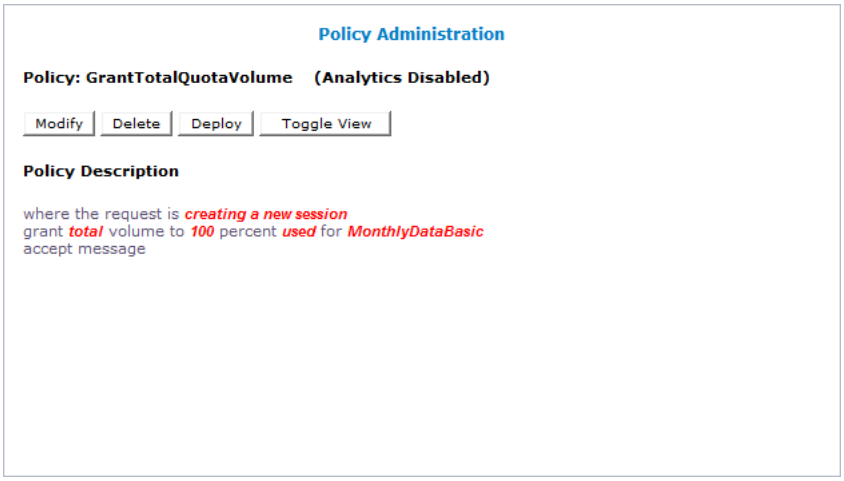
   The plan is defined in the CMP database.



2. From the **Policy Management** section of the navigation pane, select **Policy Library**, and define the policy.

   For more information, see *Creating a Policy*.

   The policy is defined in the CMP database.



3. From the **Policy Management** section of the navigation pane, select **Policy Library**, select the policy, and deploy it.

   For more information, see the *Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide*.

   The policy is deployed to MPE devices in the Policy Management network.

About Quotas Passes

A quota specifies restrictions on the amount of data volume, active session time, or service-specific events that a subscriber can consume. A single quota can express limits on any combination of volume, time, or events. Quotas can be associated with a time period during which activity is measured.

A pass is a one-time override that temporarily replaces or augments a subscriber's default plan or service.

For example, a subscriber who is normally not able to stream video to their device, but wants to view a special event, can purchase a pass that allows streaming.

Multiple passes can be assigned to the same subscriber. These passes are processed using the following criteria:

- The highest priority pass is processed first.
- If priorities are equal, the pass with the earliest expiration date/time is processed first.
- If expiration date/times are equal, the pass with the earliest purchase date/time is processed first.
- If purchase date/times are equal, the passes are processed in alphabetical order of the instance IDs.

The pass that is processed first according to these criteria is referred to as the 'best' pass.

Passes can be added to pass groups. Adding a pass to a pass group associates that pass to all other passes in the pass group.

Pass groups can be used to determine pass expiration extension. The expiration date/time value of a new pass can be extended to match an expiration date/time value in the future of any pass in the same pass group.

A pass can belong to only one pass group. If the pass group is deleted, then the group field for each pass in the pass group is set to null. If the name of the pass group is changed, then the group field for each pass in the pass group is set to the new name.

Creating a Pass

To create a pass:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree opens, displaying the **Passes** and **Plans** groups.
2. From the content tree, select the **Passes** group.
   The content tree displays a list of passes and groups.
3. From the content tree, select the **ALL** group.
   The **Pass Administration** page opens in the work area.
4. Click **Create Pass**.
   The **New Pass** page opens.
5. Enter the following information:
   a) **Name** — The name of the pass or top-up. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
   c) **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.
   d) **Max Leakage Threshold (MB)** — Maximum amount by which the usage can be exceeded. The default is 0 MB.
   e) **Max Sessions Used For Dynamic Grant**— Number of simultaneous sessions used in the dynamic grant algorithm for granting quota. Enabled when **Enable Dynamic Grant** is selected. The range is 1–2147483647 (2GB–1). The default is 10 sessions.

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

   f) **Minimum Grant Size**— The minimum plan amount granted by the MPE device. Enabled when **Enable Dynamic Grant** is selected. The value of the field depends upon the component (time/service-specific/volume) that is being granted by the MPE device:

      - time — minimum number of seconds
      - service-specific — minimum number of units
      - volume (total/input/output) — minimum number of bytes

      The default is 0.

      Note: The value of the **Minimum Grant Size** field applies to all of the components that are granted by the MPE device. Make sure that the value reflects the minimum amount for all components. A low value could lead to a high number of messages being generated.

   g) **Quota Profile Type** — Select whether the plan is assigned to an individual subscriber or a pool of subscribers. Select one of the following:

      - **Subscriber** (default)
      - **Pool**

Note: If you select **Pool**, items can be added to support the account (Max Leakage Threshold, Dynamic Grant, etc). After the plans are created, the plans are applied to subscribers.

h) **Priority** — Defines the order of use when a subscriber has multiple instances of a pass. Higher priority passes are used before lower priority passes. A higher number indicates a higher priority.

The range is -32768–32767 (max 16-bit short).

i) **Active Time Period** — The period during which the pass may be used.

j) **Initial Total Volume Limit (bytes)** — Gx or Gy mode. Specifies the initial value for total volume units granted by the pass. Select one of the following:

- **None** (default). If you select **None**, then total volume units are not granted.
- **Specify Limit** and enter a value.

k) **Initial Upstream Volume Limit (bytes)** — Gx or Gy mode. Specifies the initial value for output volume units granted by the pass. Select one of the following:

- **None** (default). If you select **None**, then output volume units are not granted.
- **Specify Limit** and enter a value.

l) **Initial Downstream Volume Limit (bytes)** — Gx or Gy mode. Specifies the initial value for input volume units granted by the pass. Select one of the following:

- **None** (default). If you select **None**, then input volume units are not granted.
- **Specify Limit** and enter a value.

m) **Initial Time Limit (seconds)** — Gx or Gy mode. Specifies the initial value for session time units granted by the pass. Select one of the following:

- **None** (default). If you select **None**, then time units are not granted.
- **Specify Limit** and enter a value.

n) **Initial Service Specific Limit (events)** — Gy mode only. Specifies the initial value for service specific units granted by the pass. Select one of the following:

- **None** (default). If you select **None**, then service specific units are not granted.
- **Specify Limit** and enter a value.

o) **Interim Reporting Interval (seconds)** — Gy mode only. The number of seconds after which the gateway must revalidate any grant with the MPE. Select one of the following:

- **None** (default)
- **Specify Interval** and enter a value.

p) **Duration** — The period after first use in which the pass must be used or expired.

q) **Expiration Date Extension Method** — The criteria used for extending an expiration date.

Possible values are:

- **NONE** — The expiration date/time value of this pass cannot be extended or used to extend the expiration date/time values of other passes.
- **Name** — The expiration date/time value of this pass can be used to extend the date/time value of passes in the same pass group.
- **Group** — The expiration date/time value of this pass can be extended to match the date/time value of any pass in the same pass group.

r) **Quota Exhaustion Action** — Gy mode only. The action to take when all units in the pass are exhausted.

Possible values are:

- **N/A** (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. Click **Save**.

The pass is defined in the CMP database and is displayed in the **Pass** group. The pass can now used in a policy.

Modifying a Pass

To modify a pass:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree opens, displaying the **Plans** and **Passes** groups.
2. From the content tree, select **Passes**.
   The content tree displays a list of passes and pass groups. The initial group is **ALL**.
3. Select a pass.
   The **Pass Administration** page opens in the work area.

   Note: If the pass has been added to a pass group, then the pass group name is shown in the **Group** field.

4. Click **Modify**.
   The **Modify Pass** page opens.
5. Modify pass information.
   For a description of the fields contained on this page, see *Creating a Pass*.

   Note: You cannot edit pass group information from this page. To assign the pass to a different pass group, you must remove the pass from the current pass group (see *Removing a Pass from a Pass Group* and add the pass to a new pass group (see *Adding a Pass to a Pass Group*).

6. Click **Save**.

The pass is modified.

Deleting a Pass

To delete a pass:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree opens, displaying the **Plans** and **Passes** groups.
2. From the content tree, select the **Passes** group.
   The content tree displays a list of passes and pass groups. The initial group is **ALL**.
3. From the content tree, select the **ALL** group.
   The **Pass Administration** page opens in the work area.
4. Delete the pass using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the pass.
   - From the content tree, select the pass and click **Delete**.

   A confirmation message displays.
5. Click **OK** to delete the pass.

The pass is deleted.

Creating a Pass Group

To create a pass group:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree displays the **Plans** and **Passes** groups.
2. From the content tree, select the **Passes** group.
   The content tree displays a list of passes and pass groups. The initial group is **ALL**.
3. Select the **ALL** group.
   The **Pass Administration** page opens in the work area.
4. click **Create Group**.
   The **Create Group** page opens in the work area.
5. Enter the following information:
   a) **Name** — The name of the pass group. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
6. Click **Save**.

The pass group is created.

Adding a Pass to a Pass Group

To add a pass to a pass group:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree displays the **Plans** and **Passes** groups.
2. From the content tree, select the **Passes** group.
   The content tree displays a list of passes and pass groups. The initial group is **ALL**.

3. From the content tree, select the pass group where you want to add the pass.
   The **Pass Administration** page opens in the work area.
4. Click **Add Pass**.
   The **Add Pass** page opens in the work area.
5. Select the pass that you want to add.

   Note: Passes can belong to only one pass group.

6. Click **Save**.

A pass is added to the selected pass group. See *Removing a Pass from a Pass Group* for instructions on removing a pass from a pass group.

Modifying a Pass Group

To modify a pass group:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree displays the **Plans** and **Passes** groups.
2. From the content tree, select the **Passes** group.
   The content tree displays a list of passes and pass groups. The initial group is **ALL**.
3. From the content tree, select the pass group you want to modify.
   The **Pass Group Administration** page opens in the work area.
4. Click **Modify**.
   The **Modify Group** page opens in the work area.
5. Modify the pass group information.

   Note: If you change the name of a pass group, then the **group** field for each pass in the pass group changes to the new name.

6. Click **Save**.

The pass group is modified.

Removing a Pass from a Pass Group

To remove a pass from a pass group:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree displays the **Plans** and **Passes** groups.
2. From the content tree, select the **Passes** group.
   The content tree displays a list of pass groups. The initial group is **ALL**.
3. From the content tree, select the pass group that contains the pass you want to remove.
   The **Pass Group Administration** page opens in the work area.
4. Click (scissors icon) located to the right of the pass.

The pass is removed from the pass group.

Deleting a Pass Group

Note: Deleting a pass group resets the group field of each pass in the pass group to null. The passes are not deleted from the system.

To delete a pass group:

1. From the **Policy Server** section of the navigation pane, select **Quota Profiles**.
   The content tree displays the **Plans** and **Passes** groups.
2. From the content tree, select **Passes**.
   The content tree displays a list of pass groups. The initial group is **ALL**.
3. From the content tree, select the pass group you want to delete.
   The **Pass Group Administration** page opens in the work area.
4. Click **Delete**.
   A confirmation message displays.
5. Click **OK** to delete the pass group.

The pass group is deleted.

Chapter 15

Managing Quota Conventions

Topics:

- *About Quota Conventions.....94*
- *Creating a Quota Convention.....94*
- *Modifying a Quota Convention.....95*
- *Associating a Quota Convention with a Plan....96*
- *Deleting a Quota Convention.....96*

This chapter describes how to manage the usage of rollovers and top-ups using the CMP system.

In a wireless network, a quota convention controls top-ups and rollovers of plans.

Note: The actual options you see depend on whether or not your CMP system is configured in wireless Gx mode, wireless Gy mode, or both.

About Quota Conventions

A quota convention controls top-ups and rollovers of plans.

Caution: If a plan contains more than one type of counter (for example, time and volume), then ALL of the counters for that entire plan must be exhausted before a rollover and/or top-up for either type of counter is activated. Depending on how policy rules are written (see *Understanding and Creating Policy Rules*), this functionality could lead to an unintended effect on the end-user's service. If the intent is to apply separate limits on different units, then separate quotas should be defined and independent top-ups or rollovers may be applied.

Rollover A rollover allows a subscriber to carry forward unused units from one billing cycle to another. For example, if a subscriber is allowed 10 gigabytes of data a month and only uses 9, the remaining gigabyte of data can be saved for use in the next month. Rollover units can accumulate and can be carried across multiple months. You can establish a quota convention that rollover units are consumed after plan units are exhausted, or before.

Top-up A top-up allows a subscriber to obtain additional units for an existing plan. For example, if a plan allows 20 gigabytes of traffic per month, but near the end of the month the subscriber has only 1 gigabyte left, the subscriber can obtain an additional 5 gigabytes. These units are used after the initial units are exhausted and do not roll over.

Multiple top-ups can be present and enforced in the database at the same time and are processed by the MPE device. Multiple top-ups can be assigned to the same subscriber. These top-ups are consumed in the following order:

- The highest priority top-up is consumed first.
- If priorities are equal, the top-up with the earliest expiration date/time is consumed first.
- If expiration date/times are equal, the top-up with the earliest purchase date/time is consumed first.
- If purchase date/times are equal, the top-ups are consumed in alphabetical order of the instance IDs.

The top-up that is processed first according to these criteria is referred to as the best top-up.

You can establish a quota convention that top-up units are consumed after rollover units are exhausted, or before. However, plan units are always consumed before top-up units.

Note: Top-ups are enabled using the **Quota Conventions** option. Top-up information is configured on the Subscriber Profile Repository (SPR) database. Refer to the Oracle Communications Enhanced Subscriber Profile Repository documentation for more information on the ESPR product.

Creating a Quota Convention

To create a quota convention:

1. From the **Policy Server** section of the navigation pane, select **Quota Conventions**.
   The content tree displays the **Quota Conventions** group.
2. Select the **Quota Conventions** group.
   The **Quota Convention Administration** page opens in the work area.
3. Click **Create Convention**.
   The **New Quota Convention** page opens.
4. Enter the following information:
   a) **Name** — The name of the quota convention. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description/Location** — Free-form text.
   c) **Rollover usage** — Specifies how rollover units are used with respect to top-up units.
      The possible values are:
      - **Default** — Rollover units are used before top-up units unless the highest priority top-up expires in the next 24 hours.
      - **Rollover after Top-up** — Top-up units are used before rollover units.
      - **Rollover before Top-up** — Rollover units are used before top-up units.
   d) **Interval percentage of the limits (%)** — The maximum percent of the units that can be rolled over during one billing cycle reset. The range is 0.0 – 100.0.
   e) **Max percentage of the limits (%)** — The maximum percent of the units that can be saved as a rolled limit at any time. The range is 0.0 – 1200.0.
   f) Enable the following options by selecting the associated checkbox:
      - **Rollover Time Units** — Roll over time.
      - **Rollover Total Volume** — Roll over total volume.
      - **Rollover Input Volume** — Roll over input volume.
      - **Rollover Output Volume** — Roll over output volume.
      - **Rollover Service Specific Units** — Roll over service-specific units.
      - **Discard Rollover on Rollover Calculation** — Rollover units are not saved beyond one cycle.
      - **Consume Rollover before Quota** — Rollover units are used before plan units.

        Note: Rollover units can be consumed before plan (quota) units, and top-up units can be consumed before rollover units. However, top-up units cannot be consumed before plan units.
      - **Enable Top-ups** — Enable top-up units.
5. Click **Save**.

The quota convention is defined in the CMP database and can be used in a policy.

Modifying a Quota Convention

To modify a quota convention:

1. From the **Policy Server** section of the navigation pane, select **Quota Conventions**.
   The content tree opens.
2. From the content tree, select the **Quota Conventions** group.

The **Quota Convention Administration** page opens, displaying the list of defined services.

3. Select the quota convention you want to modify.
   The work area displays information about the quota convention.
4. Click **Modify**.
   The **Modify Quota Convention** page opens.
5. Modify quota convention information as required.
   For a description of the fields contained on this page, see *Creating a Quota Convention*.
6. Click **Save**.

The quota convention is modified.

Associating a Quota Convention with a Plan

Associate a quota convention with a plan as follows:

1. Create a quota convention. See *Creating a Quota Convention*.
2. Create a plan or open an existing plan for modification. See *Creating a Plan* and *Modifying a Plan*.
3. In the **Quota Convention** field, select the name of the quota convention you want to associate with the plan.
4. Click **Save** to save your changes.

The quota convention is associated with a plan.

Deleting a Quota Convention

To delete a quota convention:

1. From the **Policy Server** section of the navigation pane, select **Quota Conventions**.
   The content tree displays the **Quota Conventions** group.
2. From the content tree, select the **Quota Conventions** group.
   The **Quota Convention Administration** page opens, displaying the list of defined quota conventions.
3. Delete the quota convention using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the quota convention.
   - From the content tree, select the quota convention and click **Delete**.

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

The quota convention is deleted.

Chapter 16

Managing RADIUS CoA Templates

Topics:

- *About RADIUS CoA Templates.....98*
- *Creating a RADIUS CoA Template.....98*
- *Modifying a RADIUS CoA Template.....100*
- *Deleting a RADIUS CoA Template 100*
- *Example of Creating and Using a RADIUS CoA Template.....101*

This chapter describes how to create, modify, and delete RADIUS Change of Authorization (CoA) templates.

In a wireless network, the MPE device can function as a RADIUS server by receiving, acknowledging, and responding to RADIUS messages from clients, and generating CoA messages to RADIUS entities.

Note: The actual options you see depend on whether or not your CMP system is configured in RADIUS mode.

About RADIUS CoA Templates

An MPE device can function as a Remote Authentication Dial In User Service (RADIUS) server in a wireless network. In this role it can perform the following actions:

- Receive a RADIUS message from a client system, acknowledge it, parse it, and then assemble and send a RADIUS Change of Authorization (CoA) message to some RADIUS client in the network to create, update, or delete services, which in this context are policies expressed using vendor-specific attributes (VSAs) or type-length-value structures (TLVs). Receipt of the message can trigger policy evaluation.
- Receive a subscriber update from an SPR system and then generate a CoA message to update or delete services. The identity of a subscriber is determined by parsing information in RADIUS messages using subscriber keys, which is then correlated with information obtained from the SPR system.
- Generate a CoA message to update or delete services because of the passage of time (keep-alive function).
- Evaluate and apply policies in response to RADIUS messages and supply CoA and other RADIUS messages. For example, the following CoA messages could potentially be processed:
  - 40: Disconnect-Request
  - 41: Disconnect-ACK
  - 42: Disconnect-NAK
  - 43: CoA-Request
  - 44: CoA-ACK
  - 45: CoA-NAK

Each vendor can use different or customized VSAs or TLVs. The CMP database includes a RADIUS dictionary that stores vendor, VSA, and TLV definitions. The dictionary includes standard IETF RADIUS TLVs. However, because RADIUS is an extensible protocol, new vendors, VSAs, and TLVs can appear at any time. You can define custom vendors, VSAs, and TLVs and store them in the RADIUS dictionary. To support efficient assembly of CoA messages, you can define CoA templates that can include both known and custom values. The template can contain VSA and TLV values to be included in the CoA message, or left blank. If left blank, the corresponding values from the request or the session are used. If no value is found, the VSA or TLV is not included in the CoA message.

The CMP system displays RADIUS functions only if the appropriate mode is enabled. Contact MOS before attempting to change operating modes.

For information about creating custom vendor definitions, see *Managing Custom Vendors*. For information about creating custom VSAs, see *Managing Custom VSAs*. For information about subscriber keys, see *Managing Subscriber Keys*.

Note: The actual options you see depend on whether or not your CMP system is configured in RADIUS mode.

Creating a RADIUS CoA Template

To create a RADIUS CoA template:

Note: The actual options you see depend on whether or not your CMP system is configured in RADIUS mode.

1. From the **Policy Server** section of the navigation pane, select **RADIUS CoA Template**.
   The content tree displays the **RADIUS CoA Template** group.
2. Select the **RADIUS CoA Template** group.
   The **RADIUS CoA Template Administration** page opens in the work area.
3. Click **Create RADIUS CoA Template**.
   The **New RADIUS CoA Template** page opens. You can now define a template by name and assign attributes to include in it.
4. Enter the **Name** you assign to the template.
5. To add an attribute:
   a) Click **Add**.
      The **Add Response** window opens.
   b) Select the available **Vendor** from the list:
      - **IETF** (default)
      - **3GPP**
      - **3GPP2**
      - **Camiant**
      - **Cisco**
      - **Cisco-BBSM**
      - **Cisco-VPN3000**
      - **Cisco-VPN5000**
      - **Juniper**
      - **Juniper-M-Series**
      - [defined custom vendors]

      Note: Any defined custom vendors are displayed at the end of the list. For information, see *Managing Custom Vendors*
   c) Select **TLV/VSA** from the list.
      The choices are extensive and are not listed here.

      Note: Any defined custom TLVs or VSAs are displayed at the end of the list. For information see *Managing Custom VSAs*.
   d) **Default Value** — Enter the default value for the TLV or VSA.
6. (Optional) To add, modify, or delete attributes:
   - Cloning an entry in the table
     1. Select an entry in the table.
     2. Click **Clone**. The **Clone** window opens with the information for the entry.
     3. Make changes as required.
     4. Click **Save**. The entry is added to the table
   - Editing an entry in the table
     1. Select the entry in the table.
     2. Click **Edit**. The **Edit Response** window opens, displaying the information for the entry.

3. Make changes as required.
4. Click **Save**. The entry is updated in the table.

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

7. Click **Save**.

The RADIUS CoA template is created.

Modifying a RADIUS CoA Template

To modify a RADIUS CoA template:

1. From the **Policy Server** section of the navigation pane, select **RADIUS CoA Template**.
   The **RADIUS CoA Template Administration** page opens in the work area and lists the defined RADIUS CoA templates.
2. Select the template you want to modify.
   The **RADIUS CoA Template Administration** page displays information about the template.
3. Click **Modify.**
   The **Modify RADIUS CoA Template** page opens.
4. Modify the template information as required.
   For a description of the fields contained on this page, see *Creating a RADIUS CoA Template*.
5. Click **Save**.

The RADIUS CoA template is modified and the changes are deployed to MPE devices.

Deleting a RADIUS CoA Template

To delete a RADIUS CoA template:

1. From the **Policy Server** section of the navigation pane, select **RADIUS CoA Template**.
   The **RADIUS CoA Template Administration** page opens in the work area, listing the defined RADIUS CoA templates.
2. Delete the RADIUS CoA template using one of the following methods:
   - From the work area, click (trash can icon) located to the right of the RADIUS CoA template.
   - From the content tree, select the RADIUS CoA template and click **Delete**.

   A confirmation message displays.
3. Click **OK**.

The RADIUS CoA template is deleted.

Example of Creating and Using a RADIUS CoA Template

In response to a RADIUS message such as `Accounting-Start`, an MPE device can use a RADIUS CoA template to send a policy, expressed using VSAs and TLVs, to a BNG device for a specific subscriber. The following is a simple example in which a RADIUS CoA template containing one VSA from a new vendor is defined, and a policy is written for the MPE device to send the RADIUS CoA to a BNG device upon receipt of a `RADIUS Accounting-Start` message. The following values are defined and used:

- Vendor name and ID: EquipTel (3561)
- VSA name: DSLF-Maximum-Interleaving-Delay-Downstream
- VSA code: 141
- VSA type: single-value integer
- CoA Template name: RADIUS CoA Template EquipTel

The policy rule is as follows:

```
where the RADIUS accounting request is RADIUS Accounting-Start
send CoA with RADIUS CoA Template EquipTel
accept message
```

This procedure consists of tasks described elsewhere. The steps must be performed in the order shown.

Note: The actual options you see depend on whether or not your CMP system is configured in RADIUS mode.

1. From the **Policy Server** section of the navigation pane, select **Custom Vendors**, and define the custom vendor.

   For more information, see *Creating a Custom Vendor*.

   The custom vendor is defined in the RADIUS dictionary.
2. From the **Policy Server** section of the navigation pane, select **Custom VSA Definitions**, and define the custom vendor.

   For more information, see *Creating a Custom VSA*.

   The custom VSA is defined in the RADIUS dictionary.
3. From the **Policy Server** section of the navigation pane, select **RADIUS CoA Template**, and define the RADIUS CoA template.

   For more information, see *Creating a RADIUS CoA Template*.

   The RADIUS CoA template is defined in the CMP database.
4. From the **Policy Management** section of the navigation pane, select **Policy Library**, and define the policy.

   For more information, see *Creating a Policy*.

   The policy is defined in the CMP database.
5. From the **Policy Management** section of the navigation pane, select **Policy Library**, select the policy, and deploy it.

   For more information, see *CMP Wireless User's Guide*.

   The policy is deployed to MPE devices in the Policy Management network.

The RADIUS CoA template is used as follows:

1. After the BNG device successfully authenticates a subscriber, it sends a `RADIUS Accounting-Start` message to the MPE device.
2. The MPE device fetches the subscriber's profile from an SPR database.
3. The MPE device subscribes to the SPR database for changes to the profile of the subscriber.
4. Based on the subscriber's profile and other conditions, the MPE device determines which policy and charging control (PCC) rule to install, and sends a RADIUS CoA request to install a service on the BNG device. The message includes the custom VSA from the custom vendor, as specified by the RADIUS CoA template.
5. The BNG device installs the service and sends an acknowledgment message to the MPE device.
6. The BNG device periodically sends Interim-Update messages, which the MPE device interprets as keep-alive messages indicating that the BNG device is still operational.

Chapter 17

Managing Retry Profiles

Topics:

- *About Retry Profiles.....104*
- *Creating a Retry Profile.....104*
- *Modifying a Retry Profile.....105*
- *Deleting a Retry Profile.....106*

This chapter describes how to create and manage retry profiles in the CMP system.

In a wireless network, 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.

About Retry Profiles

A retry profile specifies the circumstances under which installation of a Policy and Charging Control (PCC) or an application detection control (ADC) 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 or an ADC-Rule-Report. The retry action consists of repeatedly trying up to a maximum number of retry cycles consisting of several configurable parameters and an exponential back off algorithm to calculate the wait time between successive retry attempts. Generally, each retry cycle would consist of a small number of retry attempts and a relatively large **Back Off Interval** between each retry cycle.

For example, a Charging-Rule-Report reports a failure to establish a dedicated bearer. Using the configured Retry Profile, an attempt is made to establish a dedicated bearer after the **Initial Retry Interval**. Should the attempt fail, another retry attempt is made within the **Maximum Retry Interval** period. Attempts are repeated until the number of attempts reaches the **Maximum Retry Attempts**. This concludes a retry cycle. The next retry cycle begins after the configured time-period **Back Off Interval**.

Note: A retry profile can be applied by a policy rule trigger.

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

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 and lists any available retry profiles.
3. Click **Create Retry Profile**.
   The **New Retry Profile** page opens.
4. Enter the **Name** for the profile.

   Unique name assigned to the profile. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
5. Enter the **Description/Location**.

   Free-form text describing the profile.
6. Select the **Retry Profile Type** from the list:

   The available choices are:

   - For Wireless:

     PCC Retry Profile and **ADC Retry Profile** (default).
   - For Cable and Wireline:

Best Effort — Transmission opportunities are granted on a first-come, first-served basis. Appropriate for upstream service flows such as Web browsing, email, or instant messaging.

7. Enter the **Maximum Retry Attempt (per Retry Cycle)**.

   The maximum number of retry attempts during a retry cycle in the range from 1 to 10. The default is 5.

8. Enter the **Initial Retry Interval**.

   The length of time to wait, in seconds, after a reported failure or the end of the Back Off Interval before retrying. Enter a value from 0 to 30 seconds. The default is 10 seconds.

   Note: To specify a retry immediately after a reported failure, enter 0.

9. Enter the **Maximum Retry Interval**.

   The maximum wait, in seconds, after a reported failure or the end of the Back Off Interval before retrying during a retry cycle. Enter a value from 1 to 180 seconds. The default is 60 seconds.

10. Enter the **Back Off Interval**.

    The interval from 1 to 86400 seconds between successive retry cycles. The default is 300 seconds.

11. Enter the **Maximum Retry Cycles**.

    The number of retry cycles ranging from 1 to 4. The default value is 1 cycle.

12. **Rule Failure Code**

    The upper box lists available rule failure codes. The lower box lists rule failure codes installed in the profile.

    Note: 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 total number of retry attempts (**Maximum Retry Attempt** multiplied by the **Maximum Retry Cycles**) exceeds 12, the CMP displays a warning message that the configuration might increase the signaling load in the network and asks if you want to continue with the specified settings.

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

13. Click **Save**.

The retry profile is defined in the CMP database and can now be used in a policy.

Modifying a Retry Profile

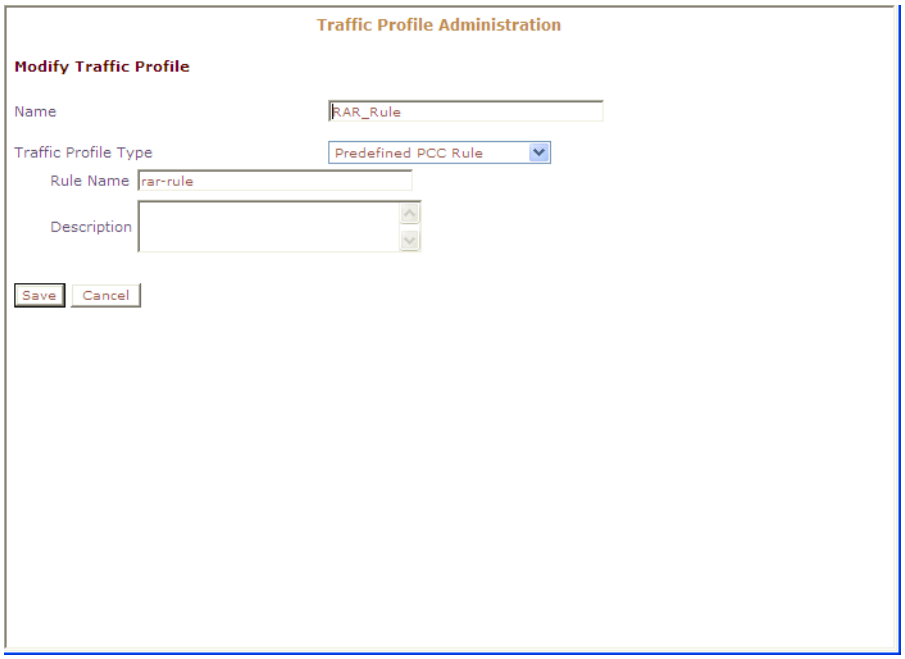
To modify a retry profile:

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.
   The profile information is displayed.
4. Click **Modify**.
   The **Modify Retry Profile** page opens.
5. Modify profile information.
   For a description of the fields contained on this page, see *Creating a Retry Profile*.
6. Click **Save**.

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 (trash can icon), located to the right of the retry profile.
   - From the content tree, select the retry profile and click **Delete**.

   A confirmation message displays.
4. Click **OK** to delete the retry profile.

The retry profile is deleted.

Note: If the retry profile is used in a policy action, the deletion fails.

Chapter 18

Managing Roaming Profiles

Topics:

- *About Roaming Profiles.....109*
- *Creating a Roaming Profile.....109*
- *Modifying a Roaming Profile.....111*
- *Deleting a Roaming Profile.....112*

This chapter describes how to create and manage roaming profiles in the CMP system.

A roaming profile allows a set of roaming attributes to be defined and then applied to specific subscribers.

About Roaming Profiles

Roaming Profiles are used in conjunction with the S9 interface. The S9 interface allows the PCRF to support LTE roaming services such as Voice over LTE. This is done be establishing S9 and Rx sessions between the Home PCRF (H-PCRF) and the Visiting PCRF (V-PCRF).

Roaming Profiles are used to allow or disallow S9 requests at the H-PCRF, and to validate messages coming from the H-PCRF and going to the V-PCRF. A V-PCRF also uses the roaming profile to decide whether to report UE Time zone and location information to the H-PCRF. You can define up to 50 profiles, each with different parameters.

S9 interface functionality must be turned on before roaming profiles can be used. By default, the PCRF cannot initiate or accept S9 requests. To turn initiate or accept on, modify the S9 settings using the **Policy Server** tab in the Policy Server configuration. If an MRA is deployed in the network, the primary and secondary DEA (or S9 peer) can be configured using the **MRA** tab located in the MRA configuration.

Note: At least one MRA Diameter Routing Peer must be defined to configure the primary/secondary DEA.

Creating a Roaming Profile

To create a roaming profile:

1. From the **Policy Server** section of the navigation pane, select **Roaming Profile**.
   The content tree displays the **Roaming Profile** group.
2. Select **Roaming Profile** group.
   The **Roaming Profile Administration** page opens in the work area, listing available roaming profiles.
3. Click **Create Roaming Profile**.
   The **New Roaming Profile** page opens.
4. On the **Configuration** tab, enter the following information:
   a) **Name** — Unique name assigned to the roaming profile. The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
   b) **Description** — Free-form text describing the profile. A maximum of 255 characters can be entered.
   c) **S9 Support** — Select the type of S9 interface support allowed for this roaming profile. The available choices are:
      - **None** (default)—S9 support is not allowed.
      - **Both**—S9 support is allowed for subscribers with MCC-MNC for both visiting and home functionalities.
      - **Visiting**—S9 support is allowed for visiting subscribers with MCC-MNC VPCRF functionality.
      - **Home**—S9 support is allowed for home subscribers with MCC-MNC HPCRF functionality.

      If **Both** or **Visiting** is selected, the **QoS Validation Parameters** tab becomes available.

d) **Report over S9** — Select the content to be reported using the S9 interface. The available content is **User Location** and **Timezone**. Both choices are unchecked (not reported) by default. This is option is enabled only when S9 support is either **Visiting** or **Both**.

5. If the **QoS Validation Parameters** tab is available, enter the following information:

a) **Uplink Aggregated Guaranteed Bitrate (bps)** — Enter the maximum uplink guaranteed bitrate to be allowed for a PDN connection across all GBR (Guaranteed Bit Rate) bearers.

Integer value in the inclusive range of 0 to 9,223,372,036,854,775,807 (without commas), that is, 0 to 2^{63}—1. If this field is left blank, no validation is performed.

b) **Downlink Aggregated Guaranteed Bitrate (bps)** — Enter the maximum downlink guaranteed bitrate to be allowed for a PDN connection across all GBR (Guaranteed Bit Rate) bearers.

Integer value in the inclusive range of 0 to 9,223,372,036,854,775,807 (without commas), that is, 0 to 2^{63}—1. If this field is left blank, no validation is performed.

c) **Uplink Aggregated Maximum Bitrate (bps) for Guaranteed Bitrate Bearers** — Enter the maximum uplink bitrate to be allowed for a PDN connection across all GBR (Guaranteed Bit Rate) bearers.

Integer value in the inclusive range of 0 to 9,223,372,036,854,775,807 (without commas), that is, 0 to 2^{63}—1. If this field is left blank, no validation is performed.

d) **Downlink Aggregated Maximum Bitrate (bps) for Guaranteed Bitrate Bearers** — Enter the maximum downlink bitrate to be allowed for a PDN connection across all GBR (Guaranteed Bit Rate) bearers.

Integer value in the inclusive range of 0 to 9,223,372,036,854,775,807 (without commas), that is, 0 to 2^{63}—1. If this field is left blank, no validation is performed.

e) **Uplink APN Aggregate Maximum Bitrate (bps)** — Specify the maximum aggregate bitrate associated with a specific access point (APN) for the uplink direction.

Integer value in the inclusive range of 0 to 9,223,372,036,854,775,807 (without commas), that is, 0 to 2^{63}—1. If this field is left blank, no validation is performed.

f) **Downlink APN Aggregate Maximum Bitrate (bps)** — Specify the maximum aggregate bitrate associated with a specific access point (APN) for the downlink direction.

Integer value in the inclusive range of 0 to 9,223,372,036,854,775,807 (without commas), that is, 0 to 2^{63}—1. If this field is left blank, no validation is performed.

g) **Acceptable Default EPS Bearer QoS** Under this heading are the following variables:

- **QoS Class Identifiers** — Check mark one or more QoS class identifiers (QCI) to be associated with this roaming profile or enter a value between 1 and 254 in the **Others** field and click **Add**. This identifies the set of Default EPS Bearer QCI values that are acceptable at the VPCRF. When one or more values is selected, the VPCRF function validates the QCI value from the Default-EPS-Bearer-QOS AVP, sent by the HPCRF against the configured set of values in the roaming profile. If no identifier is check marked, the default is 9. The options are:
  - **1 (Conversation Speech)**
  - **2 (Conversational)**
  - **3 (Streaming Speech)**
  - **4 (Streaming)**
  - **5 (Interactive with priority 1 signaling)**
  - **6 (Interactive with priority 1)**
  - **7 (Interactive with priority 2)**

- **8 (Interactive with priority 3)**
- **9 (Background)** (default)

- **ARP Priority Level (Comma Separated Values)** — This field identifies the set of Default EPS Bearer ARP Priority values that are acceptable at the VPCRF. The VPCRF function validates the ARP Priority value from the Default-EPS-Bearer-QOS AVP, sent by the HPCRF against the configured set of values in the roaming profile. When limited resources are encountered, the Allocation and Retention Priority (ARP) priority level tells the system to either accept or reject an establishment or modification of bearer request.

  Enter one or more priority values separated by a comma. Note that the VPCRF checks to see if the incoming message from the HPCRF contains the Default-EPS-Bearer-Qos AVP. If it does, the ARP Priority Level in that AVP is added to the list of selected values allowed by the roaming profile. Valid priority level values are 1 through 9. Default value is none (or empty).

- **ARP Preemption Capability** — This field configures whether preemption capability is enabled or disabled in the PCC action profile. Preemption aids in call admission control and lets the gateway accommodate higher priority bearers over lower priority bearers (for example, when resources are unusually limited or for emergency services), based on the ARP Priority Level and ARP Preemption Vulnerability. Options from the pulldown menu are **BOTH**, **PREEMPTION_CAPABILITY_ENABLED**, and **PREEMPTION_CAPABILITY_DISABLED**. The default value is **BOTH**. Note that the VPCRF checks to see if the incoming message from the HPCRF contains the Default-EPS-Bearer-Qos AVP. If it does, the ARP Preemption Capability in that AVP overrides any value selected here.
- **ARP Preemption Vulnerability** — This field identifies the Default EPS Bearer ARP Preemption Vulnerability values that are acceptable at the VPCRF. The VPCRF function validates the ARP Preemption Vulnerability value from the Default-EPS-Bearer-QOS AVP, sent by the HPCRF against the configured value in the roaming profile. Options from the pulldown menu are **Both**, **Preemption_vulnerability_enabled**, and **Preemption_vulnerability_disabled**. Default value is **Both**. Note that the VPCRF checks to see if the incoming message from the HPCRF contains the Default-EPS-Bearer-Qos AVP. If it does, the ARP Preemption Vulnerability in that AVP overrides any value selected here.

6. On the **Associated MCC-MNC Lists** tab, highlight the match lists in the **Available** column and click the right arrow (**>>**) button to move them to the **Associated** column.

   See *Managing Match Lists* for information on creating a match list.
7. Click **Save**.

The roaming profile is defined in the CMP database and can now be used in a policy.

Modifying a Roaming Profile

To modify a roaming profile:

1. From the **Policy Server** section of the navigation pane, select **Roaming Profile**.
   The content tree opens.
2. From the content tree, select the **Roaming Profile** group.
   The **Roaming Profile Administration** page opens, displaying the list of defined roaming profiles.

3. Select the profile you want to modify.
   Profile information is displayed.
4. Click **Modify**.
   The **Modify Roaming Profile** page opens.
5. Modify profile information as required.
   For a description of the fields contained on this page, see *Creating a Roaming Profile*.
6. Click **Save**.

The roaming profile is modified.

Deleting a Roaming Profile

Note: A roaming profile cannot be deleted if any policy is referencing it.

To delete a roaming profile:

1. From the **Policy Server** section of the navigation pane, select **Roaming Profile**.
   The content tree opens.
2. From the content tree, select the **Roaming Profile** group.
   The Roaming Profile Administration page opens, displaying the list of defined roaming profiles.
3. Delete the roaming profile using one of the following methods:
   - From the work area, click (trash can icon) located to the right of the roaming profile.
   - From the content tree, select the roaming profile and click **Delete**.

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

The roaming profile is deleted.

Chapter 19

Managing Service Classes

Topics:

- *About Service Classes.....114*
- *Creating a Service Class.....114*
- *Modifying a Service Class.....115*
- *Deleting a Service Class.....116*

This chapter defines how to create and manage service classes in the CMP system.

In a cable network, a service class corresponds to a DOCSIS traffic description defined in a cable modem termination system (CMTS).

Note: Service Classes is a function that is applicable to Cable mode only.

About Service Classes

A service class corresponds to a DOCSIS traffic description defined in a cable modem termination system (CMTS). You can define service classes using the CMP system, load them using the OSSI/XML interface, or discover them using the SNMP interface.

Note: Service Classes is a function that is applicable to Cable mode only.

Creating a Service Class

Note: Service Classes is a function that is applicable to Cable mode only.

To create a service class:

1. From the **Policy Server** section of the navigation pane, select **Service Classes**.
   The content tree displays the **Service Classes** group.
2. Select the **Service Classes** group.
   The **Service Class Administration** page opens in the work area, listing available service classes.
3. Click **Create Service Class**.
   The **New Service Class** page opens.
4. Enter the following information:
   a) **Name** — The name assigned to the service class.
   b) **Scheduling Type** — Select from the following:
      - **Downstream** (default) — Defined through a similar set of QoS parameters that are associated with the best-effort scheduling type on upstream service flows. Appropriate for all downstream service flows.
      - **Best Effort** — Transmission opportunities are granted on a first-come, first-served basis. Appropriate for upstream service flows such as Web browsing, e-mail, or instant messaging.
      - **Non Real Time Polling** — Cable modems are polled at a fixed interval for queued data. Appropriate for upstream service flows that require high throughput, and traffic that requires variable-sized data grants on a regular basis, such as high-bandwidth FTP.
      - **Real Time Polling** — Cable modems are polled at a fixed but short interval for queued data. Appropriate for upstream service flows of real-time traffic that generate variable-sized data packets on a periodic basis and have inflexible latency and throughput requirements, such as MPEG video.
      - **Unsolicited Grant Service** — A fixed-size grant is offered to service flows at fixed intervals without additional polling or interaction. Appropriate for upstream service flows of real-time traffic that generate fixed-size data packets on a periodic basis, such as VoIP.
      - **Unsolicited Grant Service with Activity Detect** — When there is activity, the CMTS sends unsolicited fixed grants at fixed intervals to the cable modem. When there is no activity, the CMTS sends unicast poll requests to the cable modem to conserve unused bandwidth. Appropriate for upstream service flows that include silence suppression.

   c) **Maximum Traffic Rate (bps)** — The maximum sustained rate, in bits per second, at which traffic can operate over the service flow.

      Enter an integer between 0 and 4294967295.

This field applies to the **Downstream**, **Best Effort**, **Non Real Time Polling**, and **Real Time Polling** scheduling types.

d) **Minimum Reserved Rate (bps)** — The guaranteed minimum rate, in bits per second, that is reserved for the service flow.

Enter an integer between 0 and 4294967295.

This field applies to the **Downstream**, **Best Effort**, **Non Real Time Polling**, and **Real Time Polling** scheduling types.

e) **Unsolicited Grant Size (bytes)** — The size, in bytes, of the individual data grants provided to the service flow.

Enter an integer between 0 and 65535.

This field applies to the **Unsolicited Grant Service** and **Unsolicited Grant Service with Activity Detect** scheduling types.

f) **Nominal Grant Interval (usecs)** — The nominal interval, in microseconds, between successive unsolicited data grant opportunities for this service flow.

Enter an integer between 0 and 4294967295.

This field applies to the **Unsolicited Grant Service** and **Unsolicited Grant Service with Activity Detect** scheduling types.

g) **Grants per Interval** — The actual number of data grants given to the service flow during each nominal grant interval.

Enter an integer between 0 and 127.

This field applies to the **Unsolicited Grant Service** and **Unsolicited Grant Service with Activity Detect** scheduling types.

5. Click **Save**.

The service class is defined in the CMP database and can now be used in a policy.

Modifying a Service Class

To modify a service class:

1. From the **Policy Server** section of the navigation pane, select **Service Classes**.
   The content tree opens.
2. From the content tree, select the **Service Classes** group.
   The **Service Class Administration** page opens, displaying the list of defined service classes.
3. Select the service class.
   Service class information is displayed.
4. Click **Modify**.
   The **Modify Service Class** page opens.
5. Modify service class information.
   For a description of the fields contained on this page, see *Creating a Service Class*.
6. Click **Save**.

The service class is modified.

Deleting a Service Class

To delete a service class:

1. From the **Policy Server** section of the navigation pane, select **Service Classes**.
   The content tree opens.
2. From the content tree, select the **Service Classes** group.
   The **Service Class Administration** page opens displaying the list of defined service classes.
3. Delete the service class using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the service class.
   - From the content tree, select the service class and click **Delete**.

   A confirmation message displays.
4. Click **OK** to delete the service class.

The service class is deleted.

Chapter 20

Managing Services and Rating Groups

Topics:

- *About Services.....118*
- *About Rating Groups.....119*

This chapter describes how to create and manage Gy services and rating groups in the CMP system.

About Services

In a wireless network, a service is an identification of a class of traffic:

- Voice
- Peer-to-peer
- 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: The actual options you see depend on whether or not your CMP system is configured in wireless Gx mode, wireless Gy mode, or both. For information on defining quotas, see *Managing Quotas*.

Creating a Service

Note: Services is a function that is applicable to Gy interfacing mode only.

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. 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** (default) or one of the rating groups defined in the CMP database.
   e) **Quota** — Select **None** (default) or one of the quotas defined in the CMP database.
5. Click **Save**.

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. Click **Save**.

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 (trash can icon), located to the right of the service.
   - From the content tree, select the service and click **Delete**.

   A conformation message displays.
4. Click **OK** to delete the service.

The service is deleted.

About Rating Groups

For organizational purposes, you can combine services into rating groups. Quotas apply to all the services in a rating group. After a rating group is created, you can populate it with services.

Note: Rating groups are applicable in the Gy interfacing mode only.

Creating a Rating Group

Note: Rating groups is a function that is applicable to Gy interfacing mode only.

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. 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** (default) or one of the quotas defined in the CMP.

5. Click **Save**.

The rating group is created and stored in the **Services & Rating Groups** folder.

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. Click **Add Service**.
   The **Add Service** page opens, displaying the services not already part of the group.
4. Select the service you want to add; use the Ctrl or Shift keys to select multiple services.
5. Click **Save**.

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 **Rating Group Administration** page opens displaying the information about the rating group.
3. Click **Modify**.
   The **Modify Rating Group** page opens.
4. Make changes. For information about the fields on this page, see *Creating a Rating Group*.
5. Click **Save**.

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.

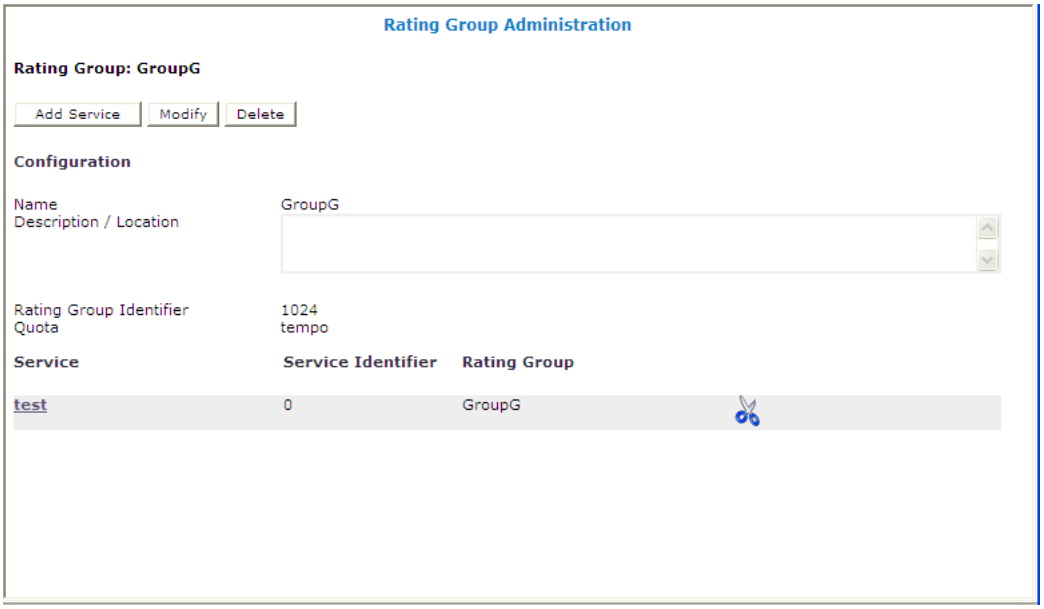
3. Remove the service using one of the following methods:
   - On the **Rating Group Administration** page, click the Remove icon, located to the right to the service you want to remove. The service is removed from the rating group immediately; there is no confirmation message.
   - From the content tree, select the service in the rating group; the **Service Administration** page opens, displaying information about the service. Click **Delete**. A conformation message displays. Click **OK**.

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.



3. Click **Delete**.
   A confirmation message displays.
4. Click **OK**.

The rating group is deleted.

Chapter 21

Managing Subscriber Keys

Topics:

- *About Subscriber Keys.....123*
- *Creating a Subscriber Key.....123*
- *Modifying a Subscriber Key.....125*
- *Deleting a Subscriber Key.....125*

This chapter describes how to create and manage subscriber keys in the CMP system.

In a wireless network, a subscriber key associates subscriber IDs with RADIUS messages for RADIUS accounting purposes.

Note: The actual options you see depend on whether or not your CMP system is configured for RADIUS CoA mode.

About Subscriber Keys

Note: Subscriber keys is a function that is applicable to RADIUS mode only. For more information on RADIUS configuration, see *CMP Wireless User's Guide*.

An MPE device must create a data session to track the life cycle of the request and process of any subsequent Interim-Update messages or a `RADIUS Accounting-Stop` message, when a `RADIUS Accounting-Start` message is received from:

- An AAA server or from a broadband network gateway (BNG) system
- A RADIUS Interim-Update message is received for an unknown session

To create this session, the MPE device determines a subscriber ID from the RADIUS message using subscriber keys. You configure subscriber keys using the CMP system. Subscriber keys are associated with individual BNG systems.

The subscriber key is a combination of specified type-length values (TLVs) or vendor-specific attributes (VSAs) found in the RADIUS message. The order in which the attribute values are combined is defined in the CMP system. After the subscriber key is computed, the key is matched against the subscribers defined on the MPE device:

- If no match is found, the MPE device initiates an SPR database lookup:
  - If the lookup succeeds, the request is parsed for creating a list of VSAs to be included in a RADIUS Change of Authorization (CoA) message and sent to the BNG system.
  - If the lookup fails and if the RADIUS configuration value **Validate User** is set to **true**, the request is rejected.
- If a match is found, the MPE device creates a dummy user instance to store necessary information for later use.

For more information on CoA messages, see *Managing RADIUS CoA Templates*.

Creating a Subscriber Key

Note: Subscriber keys is a function that is applicable to Radius CoA mode only.

To create a subscriber key:

1. From the **Policy Server** section of the navigation pane, select **Subscriber Keys**.
   The content tree displays the **Subscriber Keys** group.
2. Select the **Subscriber Keys** group.
   The **Subscriber Keys Administration** page opens in the work area.
3. Click **Create Subscriber Key**.
   The **New Subscriber Key** page opens.
4. Enter the **Name** you assign to the subscriber key.
   Enter a string.
5. Add a subscriber key.
   a) Click **Add**. The **Add Subscriber Key Field** window opens.

TLVs and VSAs are concatenated in the order in which you define them here.

b) **Vendor** — Select the available vendor from the list:

- **IETF** (default)
- **3GPP**
- **3GPP2**
- **Camiant**
- **Cisco**
- **Cisco-BBSM**
- **Cisco-VPN3000**
- **Cisco-VPN5000**
- **Juniper**
- **Juniper-M-Series**
- Any defined custom vendors are displayed at the end of the list; for more information, see *Managing Custom Vendors*

c) **TLV/VSA** — Select the TLV or VSA from the list.

The choices are extensive and are not listed here. Any defined custom TLVs or VSAs are displayed at the end of the list; for more information, see *Managing Custom VSAs*.

d) **Delimiter** — Enter the delimiter between fields used by the vendor.

e) Click **Save**.

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

- Cloning an entry in the table

  1. Select an entry in the table.
  2. Click **Clone**. The **Clone** window opens with the information for the entry.
  3. Make changes as required.
  4. Click **Save**. The entry is added to the table

- Editing an entry in the table

  1. Select the entry in the table.
  2. Click **Edit**. The **Edit Response** window opens, displaying the information for the entry.
  3. Make changes as required.
  4. Click **Save**. The entry is updated in the table.

- Deleting a value from the table

  1. Select the entry in the table.
  2. Click **Delete**. A confirmation message displays.
  3. Click **Delete** to remove the entry. The entry is removed from the table.

7. Click **Save**.

The subscriber key is displayed in the **Subscriber Keys Administration** page. After you define subscriber keys, they can be matched against subscribers currently known in the system.

Modifying a Subscriber Key

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

   For a description of the fields contained on this page, see *Creating a Subscriber Key*.
5. Click **Save**.

The subscriber key definition is modified.

Deleting a Subscriber Key

1. From the **Policy Server** section of the navigation pane, select **Subscriber Keys**.
   The **Subscriber Keys Administration** page opens in the work area, listing the defined subscriber keys.
2. Delete the subscriber key using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the subscriber key.
   - From the content tree, select the subscriber key and click **Delete**.

   A confirmation message displays.
3. Click **OK**.

The subscriber key is deleted.

Chapter 22

Managing Traffic Profiles

Topics:

- *About Traffic Profiles.....127*
- *About Traffic Profile Groups.....148*

This chapter defines how to create and manage traffic profiles in the CMP system.

A traffic profile is a set of values defined for parameters that are used in protocol messages within an MPE device.

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 the appropriate *CMP User's Guide*).
- They modify protocol messages, thus modifying the QoS for sessions managed by those messages (see *Creating a 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

To manage traffic profiles, see:

- *Creating a Wireless Traffic Profile*
- *Creating a Cable Traffic Profile*
- *Modifying a Traffic Profile*
- *Deleting a Traffic Profile*

About Traffic Profile Variables

You can configure individual fields in a traffic profile as variables. Traffic profile variables are evaluated when the policy executes the traffic profile that contains it. Traffic profile variables let you reuse traffic profiles for a range of situations without having to create additional profiles that might differ only in a few ways, or add traffic profiles to policy tables. Traffic profile variables are available for the following profile types:

- ADC Rule
- Diameter QoS
- PCC Profile
- PCC Rule

To use variables in a traffic profile, select the **Enable Dynamic Override** check box when creating or editing the profile. This displays fields in which you can enter variables for one or more profile values.

A variable supersedes any defined static value. If a variable is not available when it is evaluated, the static value is used and the existing traffic profiles continue to work as before. If neither a variable nor a static value is available, the parameter is ignored and the associated AVP is not included under the Charging-Rule-Definition AVP.

You can include the following classes of traffic profile variables:

Substitution variables	Predefined variables available during policy rule execution within an MPE device to allow for substitution of these variables for contextual information. For example, {*Time*} is replaced by the time value when a policy rule that references it is evaluated.
Policy table variables	Variables that reference a policy table column.
Policy evaluation variables	Variables that exist only for the lifetime of a policy evaluation cycle (that is, the process of evaluating all the policies for a single request or context).
Session state variables	State variables that have a value that is saved only while the session they are associated with is valid. After the session is terminated, session state variables no longer have a value and are no longer available for use in policies.
Subscriber local state variables	State variables that exist locally on the MPE device and have a value while the associated subscriber has at least one session on that device. After the last session is terminated, subscriber local state variables no longer have a value and are no longer available for use in policies.
Subscriber remote state variables	State variables that exist remotely in an SPR database and have a value while the associated subscriber exists in that database. Using subscriber remote state variables requires that an SPR or HSS database is configured and capable of storing these variables.

See *Example Traffic Profile Variables* for examples of traffic profile variables.

Example Traffic Profile Variables

The examples provided in this section represent each class of traffic profile variables:

Substitution Variable	{*Session.APNAggregateMaxBitrateUplink*} Replaced with the *APNAggregateMaxBitrateUplink* value currently saved in the session.
Policy Table Variable	{*PolicyTable.pccrule.GuaranteedBitrateUplink*} The policy table named **`pccrule`** is evaluated by looking at the *GuaranteedBitrateUplink* column in this table.
Policy Evaluation Variable	{*Policy.Variable.Uplink*} Replaced with the value of the policy variable named **`Uplink`** retrieved from the current policy evaluation cycle.
Session State Variable	{*Session.State.Uplink*} Replaced with the value of the state variable named **`Uplink`** retrieved from the session.
Subscriber Local State Variable	{*User.LocalState.Uplink*}

	Replaced with the value of the state variable named **`Uplink`** retrieved from the local user object on the MPE device.
Subscriber Remote State Variable	{*User.State.Uplink*} Replaced with the value of the state variable named **`Uplink`** retrieved from the SPR database.

Creating a Wireless Traffic Profile

To create a traffic profile in Wireless mode:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays a list of traffic profile group; the initial group is **ALL**.
2. Select the **Traffic Profiles** group.
   The **Traffic Profile Administration** page opens in the work area and lists available traffic profiles.
3. Click **Create Traffic Profile**.
   The **New Traffic Profile** page opens.
4. Enter the **Name** for the traffic profile.

   The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
5. Select the **Traffic Profile Type** from the list.

   The types of traffic profiles available depend on the mode in which the CMP system is operating. Wireless Mode contains the following traffic profile types:

   - **ADC Rule** (default) — an application detection control rule.
   - **Diameter QoS** — a policy and charging control rule.
   - **PCC Profile** — a policy and charging control profile.
   - **PCC Rule** — a policy and charging control rule.
   - **PCC Rule Extension** — a policy and charging control rule extension.
   - **Predefined ADC Rule** — a predefined ADC rule residing on the PCEF.
   - **Predefined ADC Rule Base** — a predefined group of ADC rules residing on the PCEF.
   - **Predefined PCC Rule** — a predefined PCC rule residing on the PCEF.
   - **Predefined PCC Rule Base** — a predefined group of PCC rules residing on the PCEF.
   - **Service Control Engine (SCE) Profile**— a predefined policy on the SCE.

6. Select to **Enable Dynamic Override** (available for ADC Rule, Diameter QoS, PCC Profile, and PCC Rule profiles).

   If you select this option, **Dynamic Value** fields appear enabling you to enter configuration parameters. You can enter variables for the configuration parameters. Variable names must be enclosed in curly braces ({}). For more information about dynamic overrides, see *About Traffic Profile Variables*.

7. Enter the parameters for the selected **Traffic Profile Type**.
   For example, in Wireless mode, if you choose **Diameter QoS** as the **Traffic Profile Type**, the page displays the fields described in *Diameter QoS Traffic Profile Configuration Parameters*.

   The following list details the configuration parameters for traffic profile types:

   - *ADC Rule Traffic Profile Configuration Parameters*
   - *Diameter QoS Traffic Profile Configuration Parameters*

- *PCC Profile Traffic Profile Configuration Parameters*
- *PCC Rule Traffic Profile Configuration Parameters*
- *Predefined PCC Rule Extension Traffic Profile Configuration Parameters*
- *Predefined ADC Rule Traffic Profile Configuration Parameters*
- *Predefined ADC Rule Base Traffic Profile Configuration Parameters*
- *Predefined PCC Rule Traffic Profile Configuration Parameters*
- *Predefined PCC Rule Base Traffic Profile Configuration Parameters*
- *SCE Profile Traffic Profile Configuration Parameters*

8. Click **Save**.

The traffic profile is defined in the CMP database and can now be used in a policy.

ADC Rule Traffic Profile Configuration Parameters

Parameter	Description
Rule Name	Uniquely identifies the ADC rule. Used to reference an ADC rule in communication between the MPE device and a PCEF within one IP-CAN session.
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).
Monitoring Key	Select a monitoring key that may apply to the ADC rule. For more information on monitoring keys, see *Managing Monitoring Keys*. The default is **N/A**.
Flow Status	Indicates whether the application traffic is enabled or disabled in either the uplink or downlink direction. Select from the following: • **N/A** (default) • **ENABLED_UPLINK** • **ENABLED_DOWNLINK** • **ENABLED** • **DISABLED**
TDF Application Identifier	Identifies the traffic that belongs to the application to which the rule applies.
TDF Redirect Support	Indicates whether the application traffic should be redirected to another controlled address. Select from the following: • **N/A** (default) • **REDIRECTION_DISABLED** • **REDIRECTION_ENABLED**
TDF Redirect Address Type	Specifies the format for the redirect address. Select from the following: • **N/A** (default) • **IPv4** • **IPv6**

Parameter	Description
	• **URL** • **SIP_URI**
TDF Redirect Server Address	The address of the TDF redirect server in the specified address type.
Mute Notification	Used to disable application detection notifications from the TDF device. Select from the following: • **N/A** (default) • **MUTE_REQUIRED**
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.

Diameter QoS Traffic Profile Configuration Parameters

Parameter	Description
QoS Class Identifier	Identifies the QoS class. Select from the following: • **N/A** (default) • **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: • **N/A** (default) • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**

Parameter	Description
ARP Preemption Vulnerability	Select from the following: • **N/A** (default) • **PREEMPTION_VULNERABILITY_ENABLED** • **PREEMPTION_VULNERABILITY_DISABLED**
Resource Allocation Notification	Indicates that the allocation of resources for the related PCC rules will be confirmed. Select from the following: • **N/A** (default) • **ENABLE_NOTIFICATION**

PCC Profile Traffic Profile Configuration Parameters

Parameter	Description
QoS Class Identifier	Identifies the QoS class. Select from the following: • **N/A** (default) • **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: • **N/A** (default) • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**

Parameter	Description
ARP Preemption Vulnerability	Select from the following: • **N/A** (default) • **PREEMPTION_VULNERABILITY_ENABLED** • **PREEMPTION_VULNERABILITY_DISABLED**
Monitoring Key	Select a monitoring key that may apply to the PCC profile. For more information on monitoring keys, see *Managing Monitoring Keys*. The default is **N/A**.
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 profile. Only applicable if online charging is enabled.
Reporting Level	Select from the following: • **N/A** (default) • **SERVICE_IDENTIFIER_LEVEL** • **RATING_GROUP_LEVEL** • **SPONSORED_CONNECTIVITY_LEVEL**
Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • **N/A** (default) • **DISABLE_ONLINE** • **ENABLE_ONLINE**
Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following: • **N/A** (default) • **DISABLE_OFFLINE** • **ENABLE_OFFLINE**
Metering Method	Defines how service data-flow traffic is metered for offline charging. Select from the following: • **N/A** (default) • **DURATION** • **VOLUME** • **DURATION_VOLUME** • **EVENT** **Note:** Event-based charging is only applicable to predefined PCC rules using a service data-flow filter and any PCC rule (predefined and dynamic) using an application detection identifier.
Flow Status	Select from the following: • **N/A** (default) • **ENABLED_UPLINK**

Parameter	Description
	• **ENABLED_DOWNLINK** • **ENABLED** • **DISABLED**
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.
Resource Allocation Notification	Indicates that the allocation of resources for the related PCC rules will be confirmed. Select from the following: • **N/A** (default) • **ENABLE_NOTIFICATION**
Required Access Info	Select from the following: • **N/A** (default) • **USER_LOCATION** — the subscriber's location • **MS_TIME_ZONE** — the mobile subscriber's time zone • **USER_LOCATION and MS_TIME_ZONE** — the (mobile) subscriber's location and time zone If this field is not set, the device uses the values sent in AF requests; otherwise, it uses the values set here.
Sponsor Identity	Name identifying a connectivity sponsor.
Application Service Provider Identity	Name identifying an application service provider.
Flow Descriptions	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. Used in the following cases: • An old traffic profile is imported, and the flow description is not an empty string. • An upgrade from an older version is in process and the existing traffic profile flow description is not an empty string. For all other cases, the **Use Flow Informations** fields indicate the IP flows.
Use Flow Informations	IP flow description, TOS traffic class, TOS traffic class mask, and flow direction information associated with the profile. Multiple Flow Informations can be added to the same traffic profile. This field is used instead of the **Flow Descriptions** field. **Note:** If the **Flow Descriptions** field is populated, then the **Use Flow Informations** field cannot be used. Click **Add** next to the **Use Flow Informations** field to access the Flow Information fields. Double-click each column to edit the values in the column. Click **Del** next to an existing Flow Information row to delete the row.

PCC Rule Traffic Profile Configuration Parameters

Parameter	Description
Rule Name	Name identifying the provisioned PCC rule. The name must not contain apostrophes ('). **QoS Class Identifier** Identifies the QoS class. Select from the following: • **N/A** (default) • **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: • **N/A** (default) • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**
ARP Preemption Vulnerability	Select from the following: • **N/A** (default) • **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 profile. Only applicable if online charging is enabled.

Parameter	Description
Monitoring Key	Select a monitoring key that may apply to the PCC profile. For more information on monitoring keys, see *Managing Monitoring Keys*. The default is **N/A**.
Reporting Level	Select from the following: • **N/A** (default) • **SERVICE_IDENTIFIER_LEVEL** • **RATING_GROUP_LEVEL** • **SPONSORED_CONNECTIVITY_LEVEL**
Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • **N/A** (default) • **DISABLE_ONLINE** • **ENABLE_ONLINE**
Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following: • **N/A** (default) • **DISABLE_OFFLINE** • **ENABLE_OFFLINE**
Metering Method	Defines how service data-flow traffic is metered for offline charging. Select from the following: • **N/A** (default) • **DURATION** • **VOLUME** • **DURATION_VOLUME** • **EVENT** **Note:** Event-based charging is only applicable to predefined PCC rules using a service data-flow filter and any PCC rule (predefined and dynamic) using an application detection identifier.
Flow Status	Select from the following: • **N/A** (default) • **ENABLED_UPLINK** • **ENABLED_DOWNLINK** • **ENABLED** • **DISABLED**
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.
Resource Allocation Notification	Indicates that the allocation of resources for the related PCC rules will be confirmed. Select from the following: • **N/A** (default)

Parameter	Description
	• **ENABLE_NOTIFICATION**
Required Access Info	Select from the following: • **N/A** (default) • **USER_LOCATION** — the subscriber's location • **MS_TIME_ZONE** — the mobile subscriber's time zone • **USER_LOCATION and MS_TIME_ZONE** — the (mobile) subscriber's location and time zone If this field is not set, the device uses the values sent in AF requests; otherwise, it uses the values set here.
Sponsor Identity	Name identifying a connectivity sponsor.
Application Service Provider Identity	Name identifying an application service provider.
PS to CS Session Continuity	Indicates that the service data flow carries video and allows for packet switch (PS) to circuit switch (CS) session continuity. Select from the following: • **N/A** (default) • **VIDEO_PS2CS_CONT_CANDIDATE**
Flow Descriptions	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*. Used in the following cases: • An old traffic profile is imported, and the flow description is not an empty string. • An upgrade from an older version is in process and the existing traffic profile flow description is not an empty string. For all other cases, the **Use Flow Informations** fields indicate the IP flows.
Use Flow Informations	IP flow description, TOS traffic class, TOS traffic class mask, and flow direction information associated with the profile. Multiple Flow Informations can be added to the same traffic profile. This field is used instead of the **Flow Descriptions** field. **Note:** If the **Flow Descriptions** field is populated, then the **Use Flow Informations** field cannot be used. To manage Flow Informations: 1. Click **Add** next to the **Use Flow Informations** field to access the Flow Information fields. 2. Double-click each column to edit the values in the column. 3. Click **Del** next to an existing Flow Information row to delete the row. **Note:** Variables are not available for this configuration parameter.

Predefined PCC Rule Extension Traffic Profile Configuration Parameters

Note: For the PCC Rule Profile Extension to be listed, you must have the Cisco Gx feature enabled.

Parameter	Description
Name	Name identifying the Predefined PCC Rule Extension. The name must not contain apostrophes (‘).
Volume Threshold	Enter a number between **1** and **9999999999**.
Service Flow Detection Trigger	Select from the following: • **N/A** (default) • **ENABLE** • **DISABLE**
Charging Rule Remove Trigger	Select from the following: • **N/A** (default) • **ENABLE** • **DISABLE**

Predefined ADC Rule Traffic Profile Configuration Parameters

Parameter	Description
Rule Name	Name identifying the Predefined ADC Rule. The name must not contain apostrophes (‘).
Description	Description of the rule.

Predefined ADC Rule Base Traffic Profile Configuration Parameters

Parameter	Description
Rule Name	Name identifying the Predefined ADC Rule Base. The name must not contain apostrophes (‘).
Description	Description of the rule base.

Predefined PCC Rule Traffic Profile Configuration Parameters

Parameter	Description
Rule Name	Name identifying the Predefined PCC Rule. The name must not contain apostrophes (‘).
Description	Description of the rule.
Monitoring Key	Select **N/A** or the name of a monitoring key defined in the CMP database. See *Managing Monitoring Keys* for information on monitoring keys.
ServiceFlowDetection	Select from the following: • **N/A** (default) • **ENABLE_DETECTION** **Note:** For ServiceFlowDetection to be listed, you must have the PCC Extensions mode enabled.

Predefined PCC Rule Base Traffic Profile Configuration Parameters

Parameter	Description
Rule Base Name	Name identifying the Predefined PCC Rule Base. The name must not contain apostrophes (').
Description	Description of the rule base.
ServiceFlowDetection	Select from the following: • **N/A** (default) • **ENABLE_DETECTION** **Note:** For ServiceFlowDetection to be listed, you must have the PCC Extensions mode enabled.

SCE Profile Traffic Profile Configuration Parameters

Note: For the SCE Profile to be listed, you must have the SCE-Gx feature enabled.

Parameter	Description
Name	Name identifying the SCE profile. The name must not contain apostrophes (').
Package ID	Identifier corresponding to a policy defined on the SCE.
Description	Description of the SCE profile.

Creating a Cable Traffic Profile

To create a traffic profile in Cable mode:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays a list of traffic profile group; the initial group is **ALL**.
2. Select the **Traffic Profiles** group.
   The **Traffic Profile Administration** page opens in the work area and lists available traffic profiles.
3. Click **Create Traffic Profile**.
   The **New Traffic Profile** page opens.
4. Enter the **Name** for the traffic profile.

   The name can be up to 255 characters long and must not contain quotation marks (") or commas (,).
5. Select the **Traffic Profile Type** from the list.

   The types of traffic profiles available depend on the mode in which the CMP system is operating. Cable Mode contains the following traffic profile types:

   - **Best Effort** (default) — Transmission opportunities are granted on a first-come, first-served basis. Appropriate for upstream service flows such as Web browsing, e-mail, or instant messaging.
   - **Diameter QoS** — a policy and charging control rule.

- **Downstream** — Defined through a similar set of QoS parameters that are associated with the best-effort scheduling type on upstream service flows. Appropriate for all downstream service flows.
- **Non-Real-Time Polling** — Cable modems are polled at a fixed interval for queued data. Appropriate for upstream service flows that require high throughput, and traffic that requires variable-sized data grants on a regular basis, such as high-bandwidth FTP.
- **RSVP Flow Spec** — Receivers initiate reservation requests for unidirectional data flows, and senders respond with path information.
- **Real-Time Polling** — Cable modems are polled at a fixed but short interval for queued data. Appropriate for upstream service flows of real-time traffic that generate variable-sized data packets on a periodic basis and have inflexible latency and throughput requirements, such as MPEG video.
- **Service Class** — The profile will use a service class that is configured on the CMTS.
- **Unsolicited Grant** — A fixed-size grant is offered to service flows at fixed intervals without additional polling or interaction. Appropriate for upstream service flows of real-time traffic that generate fixed-size data packets on a periodic basis, such as VoIP.
- **Unsolicited Grant with Activity Detection** — When there is activity, the CMTS sends unsolicited fixed grants at fixed intervals to the cable modem. When there is no activity, the CMTS sends unicast poll requests to the cable modem to conserve unused bandwidth. Appropriate for upstream service flows that include silence suppression.

6. Select to **Enable Dynamic Override** (available for Diameter QoS profiles).

   If you select this option, **Dynamic Value** fields are displayed for configuration parameters. You can enter variables for the configuration parameters. Variable names must be enclosed in curly braces ({}). For more information about dynamic overrides, see *About Traffic Profile Variables*.

7. Enter the parameters for the selected **Traffic Profile Type**.

   The set of fields displayed on the **Traffic Profile** page varies depending on the **Traffic Profile Type** you select.

   The following list details the configuration parameters for traffic profile types:

   - *Best Effort Traffic Profile Configuration Parameters*
   - *Diameter QoS Traffic Profile Configuration Parameters*
   - *Downstream Traffic Profile Configuration Parameters*
   - *Non-Real-Time Polling Traffic Profile Configuration Parameters*
   - *RSVP Flow Spec Traffic Profile Configuration Parameters*
   - *Real-Time Polling Traffic Profile Configuration Parameters*
   - *Unsolicited Grant Traffic Profile Configuration Parameters*
   - *Unsolicited Grant with Activity Detection Traffic Profile Configuration Parameters*

8. Click **Save**.

The traffic profile is defined in the CMP database and can now be used in a policy.

Best Effort Traffic Profile Configuration Parameters

Parameter	Description
Traffic Priority	Priority for the service flow. Higher-priority service flows are given preference over lower-priority service flows.

Parameter	Description
Request Transmission Policy	The interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. It also specifies whether requests can be piggybacked with data.
Max Sustained Traffic Rate (bps)	The maximum sustained rate, in bits per second, at which traffic can operate over the service flow.
Max Traffic Burst	The maximum burst size for the service flow.
Min Reserved Traffic Rate (bps)	The guaranteed minimum rate, in bits per second, that is reserved for the service flow.
Assumed Min Packet Size (bytes)	The assumed minimum packet size, in bytes, for which the minimum reserved traffic rate is provided.
Maximum Concatenated Bursts (bytes)	The maximum size, in bytes, of a concatenated frame (a group of frames) that a service flow can transmit.
Upstream Peak Traffic Rate	A four-byte unsigned integer field that specifies the peak traffic rate, in bits per second, that is allowed for a service flow. The range is 0 – 4,294,967,295 bps (4 Gbps–1).
Required Attribute Mask	A 32-bit mask that specifies whether certain attributes are required in a service flow.
Forbidden Attribute Mask	A 32-bit mask that specifies whether certain attributes are forbidden in a service flow.
Attribute Aggregation Rule Mask	A 32-bit mask that controls whether groups of attributes are either required or forbidden in a service flow.
Minimum Buffer	The lower limit for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is a value of 0, which indicates that there is no lower limit.
Target Buffer	The value for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). If the parameter is omitted or set to a value of 0, then the device selects any buffer size within the range of the minimum and maximum buffers, using a vendor-specific algorithm.
Maximum Buffer	The upper limit for the size of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is no limit.

Diameter QoS Traffic Profile Configuration Parameters

Parameter	Description
QoS Class Identifier	Identifies the QoS class. Select from the following: • **N/A** (default) • **1 = Conversational speech** • **2 = Conversational** • **3 = Streaming speech** • **4 = Streaming**

Parameter	Description
	• **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: • **N/A** (default) • **PREEMPTION_CAPABILITY_ENABLED** • **PREEMPTION_CAPABILITY_DISABLED**
ARP Preemption Vulnerability	Select from the following: • **N/A** (default) • **PREEMPTION_VULNERABILITY_ENABLED** • **PREEMPTION_VULNERABILITY_DISABLED**
Resource Allocation Notification	Indicates that the allocation of resources for the related PCC rules will be confirmed. Select from the following: • **N/A** (default) • **ENABLE_NOTIFICATION**

Downstream Traffic Profile Configuration Parameters

Parameter	Description
Traffic Priority	Priority for the service flow. Higher-priority service flows are given preference over lower-priority service flows.
Downstream Resequencing	
Max Sustained Traffic Rate (bps)	The maximum sustained rate, in bits per second, at which traffic can operate over the service flow.
Max Traffic Burst	The maximum burst size for the service flow.

Parameter	Description
Min Reserved Traffic Rate (bps)	The guaranteed minimum rate, in bits per second, that is reserved for the service flow.
Assumed Min Packet Size (bytes)	The assumed minimum packet size, in bytes, for which the minimum reserved traffic rate is provided.
Max Downstream Latency	The maximum latency for downstream service flows.
Downstream Peak Traffic Rate	A four-byte unsigned integer field, specifying the rate parameter P of a token-bucket based peak rate limiter for packets of a downstream service flow. This lets you define a **Max Traffic Burst** value for the **Max Sustained Traffic Rate** much larger than a maximum packet size, but still limit the burst of packets consecutively transmitted for a service flow.
Required Attribute Mask	A 32-bit mask that specifies whether certain attributes are required in a service flow.
Forbidden Attribute Mask	A 32-bit mask that specifies whether certain attributes are forbidden in a service flow.
Attribute Aggregation Rule Mask	A 32-bit mask that controls whether groups of attributes are either required or forbidden in a service flow.
Minimum Buffer	The lower limit for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is a value of 0, which indicates that there is no lower limit.
Target Buffer	The value for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). If the parameter is omitted or set to a value of 0, then the device selects any buffer size within the range of the minimum and maximum buffers, using a vendor-specific algorithm.
Maximum Buffer	The upper limit for the size of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is no limit.

Non-Real-Time Polling Traffic Profile Configuration Parameters

Parameter	Description
Traffic Priority	Priority for the service flow. Higher-priority service flows are given preference over lower-priority service flows.
Request Transmission Policy	The interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. It also specifies whether requests can be piggybacked with data.
Max Sustained Traffic Rate (bps)	The maximum sustained rate, in bits per second, at which traffic can operate over the service flow.
Max Traffic Burst	The maximum burst size for the service flow.
Min Reserved Traffic Rate (bps)	The guaranteed minimum rate, in bits per second, that is reserved for the service flow.

Parameter	Description
Assumed Min Packet Size (bytes)	The assumed minimum packet size, in bytes, for which the minimum reserved traffic rate is provided.
Nominal Polling Interval (microsec)	The nominal interval, in microseconds, between successive unicast request opportunities for this service flow.
Maximum Concatenated Bursts (bytes)	The largest transmission of concatenated frames, in bytes, that a modem can make on behalf of the service flow.
Upstream Peak Traffic Rate	A four-byte unsigned integer field that specifies the peak traffic rate, in bits per second, that is allowed for a service flow. The range is 0 – 4,294,967,295 bps (4 Gbps–1).
Required Attribute Mask	A 32-bit mask that specifies whether certain attributes are required in a service flow.
Forbidden Attribute Mask	A 32-bit mask that specifies whether certain attributes are forbidden in a service flow.
Attribute Aggregation Rule Mask	A 32-bit mask that controls whether groups of attributes are either required or forbidden in a service flow.
Minimum Buffer	The lower limit for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is a value of 0, which indicates that there is no lower limit.
Target Buffer	The value for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). If the parameter is omitted or set to a value of 0, then the device selects any buffer size within the range of the minimum and maximum buffers, using a vendor-specific algorithm.
Maximum Buffer	The upper limit for the size of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is no limit.

RSVP Flow Spec Traffic Profile Configuration Parameters

Parameter	Description
Service Number	Select from the following: • **N/A** (default) • **2 = Guaranteed Service** — controls the maximum delay and ensures no packet loss • **5 = Controlled Load Service** — appropriate for soft QoS applications
Token Bucket Rate (bytes/sec)	Defines how traffic will be injected into the inter network by the sending application.
Token Bucket Size (bytes)	The maximum amount of data that the flow can send at the peak rate.
Peak Data Rate (bytes/sec)	
Minimum Policed Unit (bytes)	

Parameter	Description
Maximum Packet Size (bytes)	
Rate (bytes/sec)	
Slack Term (microsec)	

Real-Time Polling Traffic Profile Configuration Parameters

Parameter	Description
Request Transmission Policy	The interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. It also specifies whether requests can be piggybacked with data.
Max Sustained Traffic Rate (bps)	The maximum sustained rate, in bits per second, at which traffic can operate over the service flow.
Max Traffic Burst	The maximum burst size for the service flow.
Min Reserved Traffic Rate (bps)	The guaranteed minimum rate, in bits per second, that is reserved for the service flow.
Assumed Min Packet Size (bytes)	The assumed minimum packet size, in bytes, for which the minimum reserved traffic rate is provided.
Nominal Polling Interval (microsec)	The nominal interval, in microseconds, between successive unicast request opportunities for this service flow.
Tolerated Poll Jitter (microsec)	The maximum amount of time, in microseconds, that unicast request intervals can be delayed beyond the nominal polling interval.
Maximum Concatenated Bursts (bytes)	The maximum size, in bytes, of a concatenated frame (a group of frames) that a service flow can transmit.
Upstream Peak Traffic Rate	A four-byte unsigned integer field that specifies the peak traffic rate, in bits per second, that is allowed for a service flow. The range is 0 – 4,294,967,295 bps (4 Gbps–1).
Required Attribute Mask	A 32-bit mask that specifies whether certain attributes are required in a service flow.
Forbidden Attribute Mask	A 32-bit mask that specifies whether certain attributes are forbidden in a service flow.
Attribute Aggregation Rule Mask	A 32-bit mask that controls whether groups of attributes are either required or forbidden in a service flow.
Minimum Buffer	The lower limit for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is a value of 0, which indicates that there is no lower limit.
Target Buffer	The value for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). If the parameter is omitted or set to a value of 0, then the device selects any buffer size within the range of the minimum and maximum buffers, using a vendor-specific algorithm.

Parameter	Description
Maximum Buffer	The upper limit for the size of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is no limit.

Unsolicited Grant Traffic Profile Configuration Parameters

Parameter	Description
Request Transmission Policy	The interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. It also specifies whether requests can be piggybacked with data.
Unsolicited Grant Size (bytes)	The size, in bytes, of the individual data grants provided to the service flow.
Grants Per Interval	The actual number of data grants given to the service flow during each nominal grant interval.
Nominal Grant Interval	The nominal interval between successive unsolicited data grant opportunities for this service flow.
Tolerated Grant Jitter (microsec)	The maximum amount of time, in microseconds, that the transmission opportunities can be delayed beyond the nominal grant interval.
Upstream Peak Traffic Rate	A four-byte unsigned integer field that specifies the peak traffic rate, in bits per second, that is allowed for a service flow. The range is 0 – 4,294,967,295 bps (4 Gbps–1).
Required Attribute Mask	A 32-bit mask that specifies whether certain attributes are required in a service flow.
Forbidden Attribute Mask	A 32-bit mask that specifies whether certain attributes are forbidden in a service flow.
Attribute Aggregation Rule Mask	A 32-bit mask that controls whether groups of attributes are either required or forbidden in a service flow.
Minimum Buffer	The lower limit for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is a value of 0, which indicates that there is no lower limit.
Target Buffer	The value for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). If the parameter is omitted or set to a value of 0, then the device selects any buffer size within the range of the minimum and maximum buffers, using a vendor-specific algorithm.
Maximum Buffer	The upper limit for the size of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is no limit.

Unsolicited Grant with Activity Detection Traffic Profile Configuration Parameters

Parameter	Description
Request Transmission Policy	The interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. It also specifies whether requests can be piggybacked with data.
Unsolicited Grant Size (bytes)	The size, in bytes, of the individual data grants provided to the service flow.
Grants Per Interval	The actual number of data grants given to the service flow during each nominal grant interval.
Nominal Grant Interval	The nominal interval between successive unsolicited data grant opportunities for this service flow.
Tolerated Grant Jitter (microsec)	The maximum amount of time, in microseconds, that the transmission opportunities can be delayed beyond the nominal grant interval.
Nominal Polling Interval (microsec)	The nominal interval, in microseconds, between successive unicast request opportunities for this service flow.
Tolerated Poll Jitter (microsec)	The maximum amount of time, in microseconds, that unicast request intervals can be delayed beyond the nominal polling interval.
Upstream Peak Traffic Rate	A four-byte unsigned integer field that specifies the peak traffic rate, in bits per second, that is allowed for a service flow. The range is 0 – 4,294,967,295 bps (4 Gbps–1).
Required Attribute Mask	A 32-bit mask that specifies whether certain attributes are required in a service flow.
Forbidden Attribute Mask	A 32-bit mask that specifies whether certain attributes are forbidden in a service flow.
Attribute Aggregation Rule Mask	A 32-bit mask that controls whether groups of attributes are either required or forbidden in a service flow.
Minimum Buffer	The lower limit for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is a value of 0, which indicates that there is no lower limit.
Target Buffer	The value for the size, in bits, of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). If the parameter is omitted or set to a value of 0, then the device selects any buffer size within the range of the minimum and maximum buffers, using a vendor-specific algorithm.
Maximum Buffer	The upper limit for the size of the buffer to be provided for a service flow. The range is 0 – 4,294,967,295 bits (4 Gb–1). The default is no limit.

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 displays a list of traffic profile group; the initial group is **ALL**.

2. Select the **Traffic Profiles** group.
   The **Traffic Profile Administration** page opens in the work area and lists available 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 the traffic profile section for your mode:
   - *Creating a Wireless Traffic Profile*
   - *Creating a Cable Traffic Profile*
6. Click **Save**.

The traffic profile is modified.

Deleting a Traffic Profile

Note: You cannot delete a traffic profile that is included in a policy or is deployed on an MPE device.

To delete a traffic profile:

1. From the **Policy Server** section of the navigation pane, select **Traffic Profiles**.
   The content tree displays a list of traffic profile group; the initial group is **ALL**.
2. Select the **Traffic Profiles** group.
   The **Traffic Profile Administration** page opens in the work area and lists available traffic profiles.
3. Delete the traffic profile using one of the following methods:
   - From the work area, click (trash can icon), located to the right of the traffic profile.
   - From the content tree, select the traffic profile and click **Delete**.

   A confirmation message displays.
4. Click **OK** to delete the traffic profile.

The traffic profile is deleted.

About Traffic Profile Groups

For organizational purposes, you can aggregate traffic profiles into groups. After a traffic profile group is created, it can be populated with individual traffic profiles. This section describes how to manage traffic profile groups:

- *Creating a Traffic Profile Group*
- *Creating a Wireless Traffic Profile*
- *Modifying a Traffic Profile Group*
- *Removing a Traffic Profile from a Traffic Profile Group*
- *Deleting a Traffic Profile Group*

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 group; the initial group is **ALL**.
2. Select the **Traffic Profiles** group.
   The **Traffic Profile Administration** page opens in the work area and lists available traffic profiles.
3. 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 250 characters long and must not contain quotation marks (") or commas (,).
5. (Optional) Enter a **Description / Location** of the traffic profile group.
6. Click **Save**.

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 group; the initial group is **ALL**.
2. From the content tree, select a Traffic Profile group.
   The **Traffic Profile Administration** page opens in the work area and lists the contents of the selected traffic profile group.
3. Click **Add Traffic Profile**.
   The **Add Traffic Profile** page opens and lists the traffic profiles that are not part of the group.
4. Click on the traffic profile you want to add; use the Ctrl or Shift keys to select multiple traffic profiles.
5. Click **Save**.

The selected traffic profiles are added to the traffic profile group.

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 group; 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. Click **Modify**.
   The **Modify Group** page opens.
4. Edit the **Name** or **Description / Location** fields.
   The name cannot contain quotation marks (") or commas (,).

5. Click **Save**.

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 a list of traffic profile group; the initial group is **ALL**.
2. From the content tree, select the traffic profile group.
   The **Traffic Profile Administration** page opens in the work area and lists the contents of the traffic profile group.
3. Remove the traffic profile using one of the following methods:
   - Click (scissors 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; 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 a list of traffic profile group; the initial group is **ALL**.
2. From the content tree, select the traffic profile group.
   The **Traffic Profile Administration** page opens in the work area and lists the contents of the selected traffic profile group.
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the group.

The traffic profile group is deleted.

Chapter 23

Understanding and Creating Policy Rules

Topics:

- *About Policy Rules.....152*
- *Structure and Evaluation of Policy Rules.....152*
- *Creating a Policy.....157*
- *Modes and the Policy Wizard.....162*
- *Organizing Policy Rules.....162*
- *Parameters Within Policy Rules.....162*
- *Conditions for Writing Policy Rules.....163*
- *Actions for Writing Policy Rules.....384*
- *Policy Rule Variables.....490*

This chapter describes policy rules and how to create them, and provides reference information on the policy rule conditions and actions available for carrier networks.

About Policy Rules

Policy rules dynamically control how an MPE device processes protocol messages as they pass through it. 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 system 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 in an if-then structure, consisting of a set of conditions that the MPE device compares to information extracted from protocol messages or obtained from subscriber records, 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 optionally selecting the logical operator **NOT** or using, where available, 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 have parameters (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 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.

After 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 grouping of one or more packet filters and associated information such as QoS, charging, or service information. A flow can be in a single direction (either upstream or downstream). A flow can be a collection of bandwidth parameters. Different protocols can have a different number of flows associated with a message.

   For example:

   - In Cable mode, the PCMM messages have only one flow per request.
   - In Wireless mode, the 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 refers to any device that creates a Gx session, such as a PGW or GGSN; the enforcement device associated 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, *policy1* and *policy4*, and two reference policies, *policy2* and *policy3* that are in a policy group, *group1*. 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 *policy1*, *policy2*, *policy3*, *policy4*.
- If the conditions in *policy1* evaluate to false, the order of execution would be *policy1*, *policy4*.
- if *policy2* includes the mandatory action `break from policy level`, the order of execution would be *policy1*, *policy2*, *policy4*.

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 Saving 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 can become deactivated. To prevent this from occurring, the session on the PCEF is set to validated 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
```

The same results can be obtained using a parent policy and the reference policies **`Bronze Policy`**, **`Silver Policy`**, and **`Gold Policy`** contained in a policy group named **`Tier 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 Policy

Policy rules are created and modified using the policy wizard in the CMP system. After the rule is 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 wireless policy as an example:

```
And
     where the request is creating a new session
     where the session is an application 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. 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 can have policy parameters pre-defined. This template can be modified.
   - **Copy Existing Policy** — The policy rule is created based on an existing policy rule, which you can modify.
5. Click **Next**.
   The **Tables** page opens.
6. Specify the tables you want to use in the policy. For more details on associating a table with a policy, see *Associating Policy Tables with a Policy Rule*.

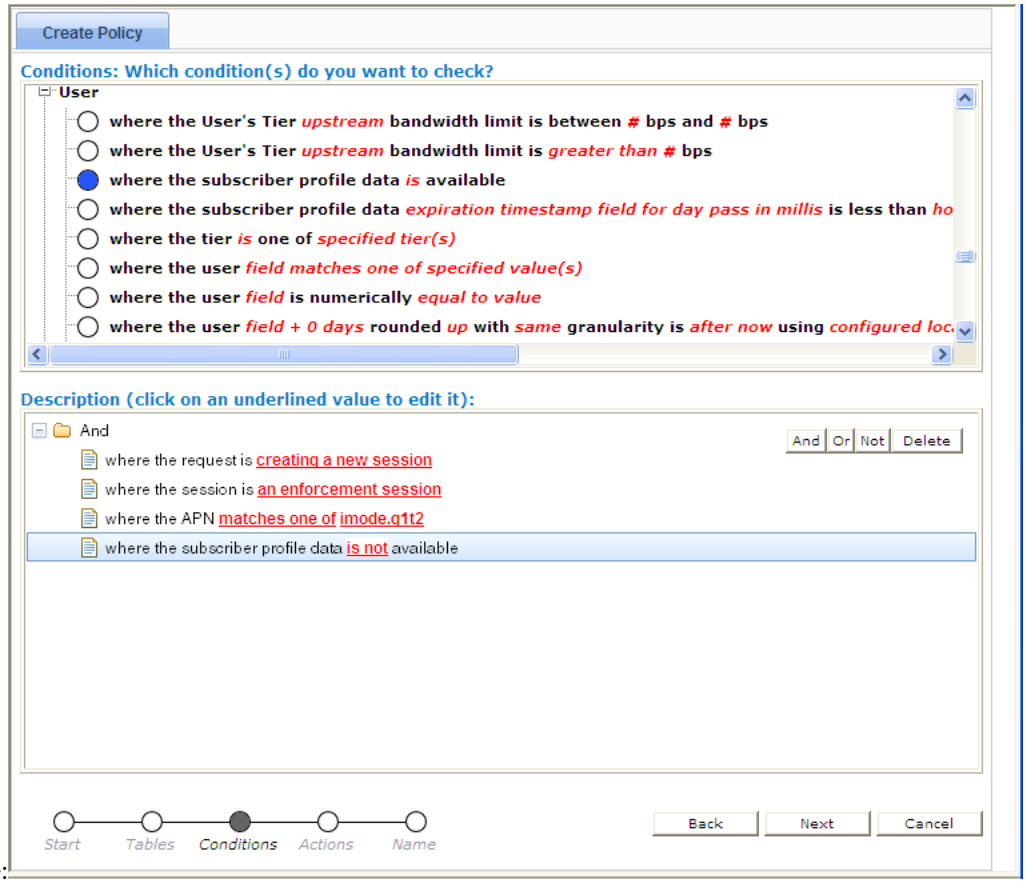
   If no tables are associated with the policy, click **Next**.
   - To specify multiple tables, click the selection icon (●) multiple times
   - To move a table so that it is evaluated earlier in the rule, click the up icon (▲)
   - To move a table so that it is evaluated later in the rule, click the down icon (▼)
   - To delete a table, click the delete icon (✕)
7. Click **Next**.
   The **Conditions** page opens.
8. Select the policy conditions.

   As a condition is selected, it appears in the **Description** area at the bottom of the page.

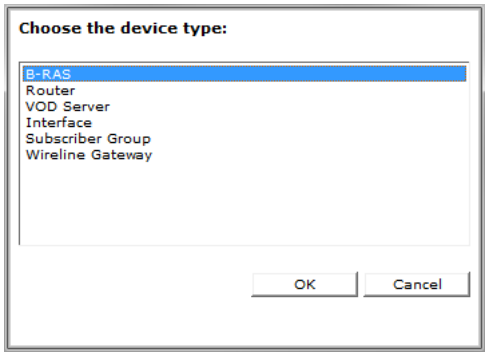
   You can select multiple conditions, enter multiple instances of each condition, change the order of conditions, group conditions logically, or remove conditions:
   - To enter multiple instances of a condition, click the selection icon (●) in the Conditions window multiple times.
   - To combine a logical 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 the evaluation order of a condition or to include the condition within a logical container, drag and drop the condition within the **Description** area. 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** area, and drag the condition into the container that appears (represented by a folder icon).
- To delete a condition or container from the rule, select the condition and click **Delete**. A confirmation message displays. Click **OK**.

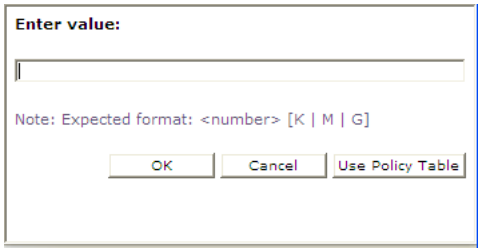
Tip: To add conditions directly to an existing container, select the container first. For example:



9. Configure parameters. information. If a policy condition includes a parameter that requires input, it displays red underlined text in the Description area.
   a) Click the red underlined text. A 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:

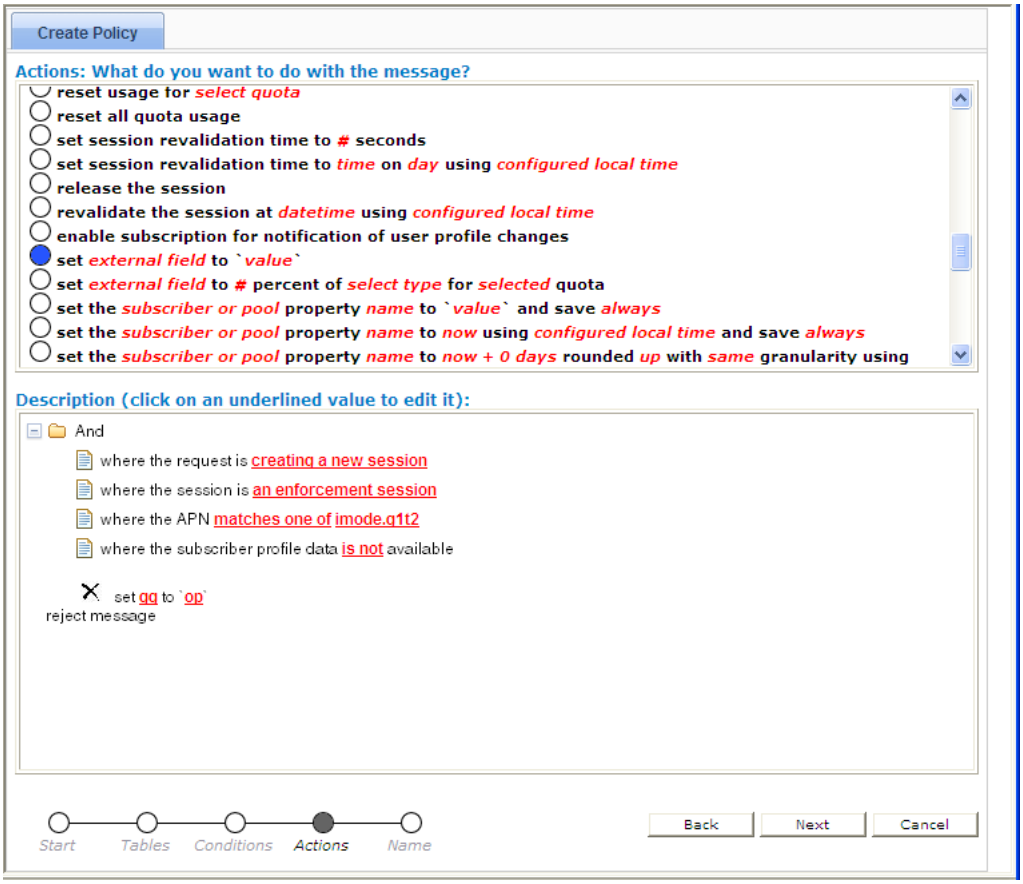


b) Click **OK**.

The popup window closes and the input is added to the policy condition.

10. Click **Next**.
    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. Click **Next**.
    The **Name** page opens.
13. Assign a unique name (uniqueness is not case sensitive) to the new policy rule.

    Note: The name can be up to 255 characters long and cannot contain the following characters: **< > \ ; & ' " =**

14. Click **Include in Analytics** to generate an analytics data stream for the policy.

    See the *Analytics Data Stream Reference* for more information on the Oracle Communications Policy Management Analytics product.

15. Click **Finish**.
    The **Create Policy** page closes.

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

After 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 because they are deployed automatically when called by a parent rule. See *Managing Policy Rules*.

Modes and the Policy Wizard

The policy wizard varies depending on the mode in which your CMP system is running. The mode configuration affects the following:

- Entire categories of conditions are made available or unavailable.
- Specific conditions and/or actions are made available or unavailable.
- Some conditions have a slightly different phrasing.
- The available values for some parameters vary.

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

Organizing Policy Rules

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

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

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

The CMP system 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*.

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. In this example, *greater than* is a single parameter, as is *100*, *upstream*, and *reserved*.

You can click 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:

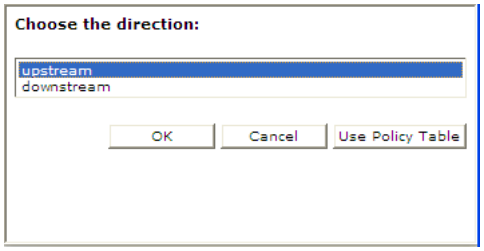


Figure 4: Example of a Parameter Pop-up

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

Conditions 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 *Policy Condition Categories*.

The conditions that are included within each of these categories are described in the sections that follow. Within each category, conditions are listed in alphabetical order. The parameters that can be modified within each condition are also detailed.

Policy Condition Categories

Variable Name	**Mode and Description**
Request	All Modes Conditions that are based on information that is explicitly contained within or related to the protocol message (request) that triggered the policy rule execution. See *Request Conditions*. **Note:** This category is disabled for the SPC mode.
Application	All Modes Conditions related to the application associated with the request. See *Application Conditions*. **Note:** This category is disabled for SPC mode.
Network DevicesNetwork Device Identity	All Modes 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. See *Network Devices Conditions*.

Variable Name	Mode and Description
Device Usage	All Modes 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. See *Device Usage Conditions*.
Mobility	Wireless Mode Conditions that are based on information associated with wireless networks that include mobile subscribers. See *Mobility Conditions*.
User	All Modes 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. See *User Conditions*. **Note:** This category is disabled for SPC mode.
Policy SDP Properties	Wireless Mode Conditions related to SDP properties that are used to check the codec type (offer/answer) for the device (remote/local). See *Policy SDP Properties Conditions*.
State Variables	Wireless Mode Conditions related to state variables in wireless networks. See *State Variables Conditions*.
Policy Context Properties	All Modes Conditions related to the context in which a policy is evaluated. See *Policy Context Property Conditions*.
Time of Day	All Modes Conditions related to the time at which the policy rules are being executed. See *Time-of-Day Conditions*.
Policy Counters	Wireless Mode Conditions related to policy counters stored in online charging systems (OCSs). See *Policy Counter Conditions*.
Notification	Wireless Mode Conditions related to notifications from Sh and Sy data sources. See *Notification Conditions*.
RADIUS	Wireless Mode Conditions related to RADIUS Change of Authorization (CoA) requests. See *RADIUS Conditions*.

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.

where at least one Filter-ID AVP exists

Mode

Wireless

Syntax

```
where at least one Filter-ID AVP exists
```

Parameters

None

Description

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

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

Mode

Wireless

Syntax

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

Parameters

action

One of the following:

- **ACTION_TERMINATE** (default)
- **ACTION_REDIRECT**
- **ACTION_RESTRICT_ACCESS**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Tests whether the current request contains a Final Unit Action (FUA) attribute-value pair (AVP) matching the specified FUA.

where at least one Final-Unit-Indication AVP exists

Mode

Wireless

Description

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

where at least one flow has media type that matches *specified type(s)*

Mode

Wireless

Syntax

`where at least one flow has media type that matches` *`media-type`*

Parameters

media-type

One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether at least one flow matches one or more of the specified media types.

Example

```
where at least one flow has media type that matches Video,Application
```

where at least one flow with media type *specified type(s)* has one of the statuses *specified status(s)*

Mode

Wireless

Syntax

`where at least one flow with media type` *`media-type`* `has one of the statuses` *`media-status`*

Parameters

media-type

One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

media-status

One or more of the following status type:

- **Enabled**
- **Enabled Uplink**
- **Enabled Downlink**
- **Disabled**
- **Removed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether at least one flow with one of the specified media types matches at least one of the specified statuses.

Example

```
where at least one flow with media type Video has one of the statuses
Enabled,Enabled Downlink
```

where Filter-ID AVP does not exist

Mode

Wireless

Syntax

```
where Filter-ID AVP does not exist
```

Parameters

None

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

where Final-Unit-Indication AVP does not exist

Mode

Wireless

Syntax
`where Final-Unit-Indication AVP does not exist`

Parameters

None

Description

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

where the AF-Application-ID *is* available

Mode

Wireless

Syntax
`where the AF-Application-ID` *`operator-binary`* `available`

Parameters
operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Checks for the presence or absence of the AF Application Identifier field. A valid AF Application identifier is any string describing the application, for example VoIP or streaming.

where the AF-Application *is* one of managed-applications

Mode

Wireless

Syntax

`where the AF-Application-ID operator-binary one of managed-applications`

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Determines whether the AF Application is a managed application.

where the AF-Application-ID matches one of *specified value(s)*

Mode

Cable, Wireless

Syntax

`where the AF-Application-ID matches one of value-list`

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Example

```
where the AF-Application-ID matches one of ptt-application-id
apply PTT to all flows in the request
continue processing message
```

where the Application-Service-Provider-Identity matches one of *specified Application Service Provider Identity(s)*

Mode

Wireless

Syntax

`where the Application-Service-Provider-Identity matches one of` *`value-list`*

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on whether the Application-Services-Provider-Identity AVP matches a list of application services providers. This condition supports sponsored data connectivity.

Example

The following condition is true if the Application-Services-Provider-Identity AVP matches either YouTube or FaceBook.

```
where the Application-Service-Provider-Identity matches one of
YouTube,FaceBook
```

where the bearer usage is *General*

Mode

Wireless

`where the bearer usage is` *`bearer-usage`*

Parameters

bearer-usage

One of the following:

- **General** (default)
- **IMS Signaling**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol message based on the user or equipment information.

where the Classifier parameters are equal to *specified value*

Mode

Cable

Syntax

`where the Classifier parameters are equal to classifier`

Parameters

classifier

One or more of the following:

- **PCMM Classifier (Extended) - Action**
- **PCMM Classifier (Extended) - Activation State**
- **PCMM Classifier (Extended) - Classifier Id**
- **PCMM Classifier (Extended) - Destination Mask**
- **PCMM Classifier (Extended) - Destination Port End**
- **PCMM Classifier (Extended) - Source Mask**
- **PCMM Classifier (Extended) - Source Port End**
- **PCMM Classifier (IPv6) - Destination Address**
- **PCMM Classifier (IPv6) - Destination Prefix Length**
- **PCMM Classifier (IPv6) - Flags**
- **PCMM Classifier (IPv6) - Flow Label**
- **PCMM Classifier (IPv6) - Next Header Type**
- **PCMM Classifier (IPv6) - Source Address**
- **PCMM Classifier (IPv6) - Source Prefix Length**
- **PCMM Classifier (IPv6) - tc-high**
- **PCMM Classifier (IPv6) - tc-low**
- **PCMM Classifier (IPv6) - tc-mask**
- **PCMM Classifier - Destination Address**
- **PCMM Classifier - Destination Port**
- **PCMM Classifier - DSCP/TOS Field**
- **PCMM Classifier - DSCP/TOS Mask**
- **PCMM Classifier - Priority**
- **PCMM Classifier - ProtocolId**
- **PCMM Classifier - Source Address**
- **PCMM Classifier - Source Port**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between different types of PCMM classifier parameters.

where the codec name for the flow *matches one of specified codec name(s)*

Mode

Cable, Wireless

Syntax

`where the codec name matches-op value-list`

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the codecs in the flow.

Example

```
where the codec name for the flow matches one of AMR-WB
```

where the DPI session is *a Gx Lite session*

Mode

Wireless

Syntax

`where the DPI session is dpi-session`

Parameters

dpi-session

One of the following:

- **a Gx Lite session** (default)
- **a Gx Plus session**
- **a SCE Gx session**
- **a TDF Solicit SD session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between types of DPI sessions.

where the enforcement session is *an IP-CAN session*

Mode

Wireless

Syntax

`where the enforcement session is` *`enforcement-session-type`*

Parameters

enforcement-session-type

One or more of the following:

- **an IP-CAN session** (default) — a Gx session
- **a gateway control session** — a Gxx session
- **a DPI enforcement session** — a Gx-Lite or Sd session
- **an S9 sub-session** — an S9 session

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between different types of enforcement sessions.

Example

```
where the request is creating a new session
And where the session is an enforcement session
And where the enforcement session is a S9 sub session
install EPS2-ims PCC rule(s) for session
accept message
```

where the event trigger is one of *specified trigger(s)*

Mode

Wireless

Syntax

`where the event trigger is one of` *`event-trigger`*

Parameters

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**
- **RAI_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**
- **APPLICATION_START**
- **APPLICATION_STOP**
- **ADC_REVALIDATION_TIMEOUT**
- **CHARGING_CORRELATION_EXCHANGE**
- **ACCESS_NETWORK_INFO_REPORT**
- **QOS_CHANGE**
- **RAT_CHANGE**
- **TFT_CHANGE**
- **PLMN_CHANGE**
- **IP_CAN_CHANGE**
- **RESOURCES_LIMITATION**
- **UE_TIME_ZONE_CHANGE**
- **USAGE_THRESHOLD_REACHED**
- **USAGE_REPORT**
- **TAI_CHANGE**
- **ECGI_CHANGE**
- **CELL_CONGESTED**
- **CELL_CLEAR**
- **SERVICE_FLOW_DETECTION**
- **APN_AMBR_MODIFICATION_FAILURE**
- **USER_CSG_INFORMATION_CHANGE**
- **DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE**
- **USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE**
- **USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the event trigger.

Examples

App Start policy

```
where the request is modifying an existing session
And where the event trigger is one of APPLICATION_START
And where the TDF-Application-Identifier matches one of TDFID01,TDFID02
install pcc_rule1 PCC rule(s) for session
continue processing message
```

App Stop policy

```
where the request is modifying an existing session
And where the event trigger is one of APPLICATION_STOP
And where the TDF-Application-Identifier matches one of TDFID01,TDFID02
remove pcc_rule1 PCC rule(s)
continue processing message
```

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

Mode

Wireless

Syntax

`where the Filter-Ids in the Final-Unit-Indication AVPs match one or more of value-list and the search type is search`

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

search

One of the following:

- **MATCH_ALL_FROM_ANY_REPORT** (default)
- **MATCH_NONE**
- **MATCH_ANYONE**
- **MATCH_ALL_FROM_ONE_REPORT**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the flow has *greater than #* grants per interval

Mode

Cable

Syntax

`where the flow has operator number grants per interval`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the number of grants per interval in the flow.

where the flow is *an application flow*

Mode

Cable, Wireless

Syntax

`where the flow is flow-type`

Parameters

flow-type

One or more of the following:

- **an application flow** (default)
- **a UE flow**
- **an application detection flow**
- **the default flow**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the type of flow:

- An application flow is created based on an application request, such as an Rx AAR message. Application flows are created in the context of an application session (for example, an Rx Media-Sub-Component message). In the context of policy and charging control, corresponding application flows are also created as part of the associated enforcement session (for example, a Gx PCC rule associated with the corresponding Rx Media-Sub-Component message).
- A UE flow is created based on a user equipment-initiated resource request, such as a GPRS PDP context creation or a UE-requested bearer resource modification.
- An application detection flow is created to identify the AVP Application_Detection_Information.
- For the Gx and Rx interfaces, the condition **where flow is the default flow** is deprecated, and always evaluates as false.

where the flow media type is one of *specified type(s)*

Mode

Cable, Wireless

Syntax

`where the flow(s) media type is one of` *`media-type`*

Parameters

media-type

One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the media type of the flow or flows.

where the flow media type *specified type(s)* is one of *specified status(s)*

Mode

Cable

Syntax

`where the flow media type` *`media-type`* `is one of` *`media-status`*

Parameters

media-type

One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

media-status

One or more of the following status type:

- **Enabled**
- **Enabled Uplink**
- **Enabled Downlink**
- **Disabled**
- **Removed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages that matches the media type and the status type of the flow.

where the flow media type *matches one of user defined media type(s)*

Mode

Wireless

Syntax

`where the flow media type` *`matches-op value-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects one or more protocol messages that match one or more user-defined media types.

where the flow packet filter *matches one of specified packet filter(s)*

Mode

Cable, Wireless

Syntax

`where the flow packet filter` *`matches-op value-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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`.

where the flow usage is one of *specified usage(s)*

Mode

Cable, Wireless

Syntax

`where the flow usage is` *`flow-usage-type`*

Parameters

flow-usage-type

One or more of the following:

- **No Information**
- **RTCP**
- **AF Signaling**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the flow usage.

where the IP-CAN bearer is *the primary bearer*

Mode

Wireless

Syntax

`where the IP-CAN bearer is` *`bearer-type`*

Parameters

bearer-type

One or more of the following:

- **the primary bearer** (default)
- **a secondary bearer**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the IP-CAN bearer type.

where the names of the installed PCC/ADC rules *contains one of specified PCC/ADC rule names*

Mode

Wireless

Syntax

`where the names of the installed PCC/ADC rules` *`containment value-list`*

Parameters

containment

One of the following:

- **contains one of** (default)
- **does not contain any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines whether an installed policy and charging control or application detection control rule contains a specified PCC or ADC rule name. See *Managing Traffic Profiles* for information on traffic profiles.

where the PCC rule being reinstalled *contains one of specified rule name(s)* and the retry *is* the final attempt

Mode

Wireless

Syntax

`where the PCC rule being reinstalled containment value-list and the retry operator-binary the final attempt`

Parameters

containment

One of the following:

- **contains one of** (default)
- **does not contain any of**

value-list

A comma-delimited list of values to compare against.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Checks for the presence or absence of one more PCC rules in a session based on the PCC rule names.

where the PCC/ADC rule being reinstalled contains one of *specified rule name(s)* and the retry *is* the final attempt

Mode

Wireless

Syntax

`where the PCC/ADC rule being reinstalled contains one of` *`value-list`* `and the retry` *`operator-binary`* `the final attempt`

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Reinstalls the specified policy and charging control or application detection control rule depending on whether this is the final retry attempt or not. See *Managing Traffic Profiles* for information on traffic profiles.

where the protocol being executed is *PCMM*

Mode

Cable

Syntax

`where the protocol being executed is` *`protocol`*

Parameters

protocol

One of the following:

- **PCMM** (default)
- **Diameter AF**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocols being executed.

where the QoS parameters in the flow are equal to *specified value*

Mode

Cable, Wireless

Syntax

`where the QoS parameters in the flow are equal to` *`profile-param`*

Parameters

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.

Wireless parameters:

- **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 AF Specific Actions**
- **Diameter APN-Aggregate-Max-Bitrate-DL**
- **Diameter APN-Aggregate-Max-Bitrate-UL**
- **Diameter APP Detection TDF-Flow-Description**
- **Diameter APP Detection TDF-Flow-Direction**
- **Diameter APP Detection TDF-Application-Identifier**
- **Diameter Bearer ARP Preemption Capability**
- **Diameter Bearer ARP Preemption Vulnerability**
- **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 Credit-Control Session Trigger Type**
- **Diameter Default EPS Bearer ARP Preemption Capability**
- **Diameter Default EPS Bearer ARP Preemption Vulnerability**

- **Diameter Default EPS Bearer ARP Priority Level**
- **Diameter Default EPS Bearer QCI**
- **Diameter Enforcement Session Bearer Control Mode Selection**
- **Diameter Enforcement Session Charging Condition Triggers**
- **Diameter Enforcement Session Event Triggers**
- **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 Reporting Reason**
- **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 Resource Allocation Notification**
- **Diameter PCC Rule Service Flow Detection**
- **Diameter PCC Rule Service-Identifier**
- **SCE Real-Time Monitoring**
- **SCE Vlink Downstream**
- **SCE Vlink Upstream**

Cable parameters:

- **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 Flow-Status**
- **PCMM AMID**
- **PCMM Classifier (Extended) - Action**
- **PCMM Classifier (Extended) - Activation State**
- **PCMM Classifier (Extended) - Classifier Id**
- **PCMM Classifier (Extended) - Destination Mask**
- **PCMM Classifier (Extended) - Destination Port End**
- **PCMM Classifier (Extended) - Source Mask**
- **PCMM Classifier (Extended) - Source Port End**
- **PCMM Classifier (IPv6) - Destination Address**
- **PCMM Classifier (IP6v6) - Destination Prefix Length**
- **PCMM Classifier (IPv6) - Flags**
- **PCMM Classifier (IPv6) - Flow Label**
- **PCMM Classifier (IPv6) - Next Header Type**
- **PCMM Classifier (IPv6) - Source Address**
- **PCMM Classifier (IPv6) - Source Prefix Length**
- **PCMM Classifier (IPv6) - tc-high**
- **PCMM Classifier (IPv6) - tc-low**
- **PCMM Classifier (IPv6) - tc-mask**
- **PCMM Classifier - Destination Address**
- **PCMM Classifier - Destination Port**
- **PCMM Classifier - DSCP/TOS Field**
- **PCMM Classifier - DSCP/TOS Mask**
- **PCMM Classifier - Priority**
- **PCMM Classifier - ProtocolId**
- **PCMM Classifier - Source Address**
- **PCMM Classifier - Source Port**
- **PCMM Gate Id**
- **PCMM GateSpec - DSCP/TOS Enabled**
- **PCMM GateSpec - DSCP/TOS Field**
- **PCMM GateSpec - DSCP/TOS Mask**
- **PCMM GateSpec - Session Class Id**
- **PCMM GateSpec - Timer T1 (secs)**
- **PCMM GateSpec - Timer T2 (secs)**
- **PCMM GateSpec - Timer T3 (secs)**
- **PCMM GateSpec - Timer T4 (secs)**
- **PCMM Traffic Profile - Authorized Assumed Minimum Reserved Traffic Rate Packet Size (bytes)**
- **PCMM Traffic Profile - Authorized Attribute Aggregation Rule Mask**
- **PCMM Traffic Profile - Authorized Downstream Peak Traffic Rate**

- **PCMM Traffic Profile - Authorized Downstream Resequencing**
- **PCMM Traffic Profile - Authorized Forbidden Attribute Mask**
- **PCMM Traffic Profile - Authorized Grants Per Interval**
- **PCMM Traffic Profile - Authorized Maximum Buffer**
- **PCMM Traffic Profile - Authorized Maximum Concatenated Bursts**
- **PCMM Traffic Profile - Authorized Maximum Downstream Latency**
- **PCMM Traffic Profile - Authorized Maximum Packet Size [M] (bytes)**
- **PCMM Traffic Profile - Authorized Maximum Sustained Traffic Rate (bps)**
- **PCMM Traffic Profile - Authorized Maximum Traffic Burst (bytes)**
- **PCMM Traffic Profile - Authorized Minimum Buffer**
- **PCMM Traffic Profile - Authorized Minimum Policed Unit [m] (bytes)**
- **PCMM Traffic Profile - Authorized Minimum Reserved Traffic Rate (bps)**
- **PCMM Traffic Profile - Authorized Nominal Grant Interval (microsec)**
- **PCMM Traffic Profile - Authorized Nominal Polling Interval (microsec)**
- **PCMM Traffic Profile - Authorized Peak Data Rate [p] (bytes/sec)**
- **PCMM Traffic Profile - Authorized Rate [R] (bytes/sec)**
- **PCMM Traffic Profile - Authorized Request Transmission Policy**
- **PCMM Traffic Profile - Authorized Required Attribute Mask**
- **PCMM Traffic Profile - Authorized Slack Term [S] (microsec)**
- **PCMM Traffic Profile - Authorized Target Buffer**
- **PCMM Traffic Profile - Authorized Token Bucket Rate [r] (bytes/sec)**
- **PCMM Traffic Profile - Authorized Token Bucket Size [b] (bytes)**
- **PCMM Traffic Profile - Authorized Tolerated Grant Jitter (microsec)**
- **PCMM Traffic Profile - Authorized Tolerated Poll Jitter (microsec)**
- **PCMM Traffic Profile - Authorized Traffic Priority (bytes/sec)**
- **PCMM Traffic Profile - Authorized Unsolicited Grant Size (bytes)**
- **PCMM Traffic Profile - Authorized Upstream Peak Traffic Rate**
- **PCMM Traffic Profile - Committed Assumed Minimum Reserved Traffic Rate Packet Size (bytes)**
- **PCMM Traffic Profile - Committed Attribute Aggregation Rule Mask**
- **PCMM Traffic Profile - Committed Downstream Peak Traffic Rate**
- **PCMM Traffic Profile - Committed Downstream Resequencing**
- **PCMM Traffic Profile - Committed Forbidden Attribute Mask**
- **PCMM Traffic Profile - Committed Grants Per Interval**
- **PCMM Traffic Profile - Committed Maximum Buffer**
- **PCMM Traffic Profile - Committed Maximum Concatenated Bursts**
- **PCMM Traffic Profile - Committed Maximum Downstream Latency**
- **PCMM Traffic Profile - Committed Maximum Packet Size [M] (bytes)**
- **PCMM Traffic Profile - Committed Maximum Sustained Traffic Rate (bps)**
- **PCMM Traffic Profile - Committed Maximum Traffic Burst (bytes)**
- **PCMM Traffic Profile - Committed Minimum Buffer**
- **PCMM Traffic Profile - Committed Minimum Policed Unit [m] (bytes)**
- **PCMM Traffic Profile - Committed Minimum Reserved Traffic Rate (bps)**
- **PCMM Traffic Profile - Committed Nominal Grant Interval (microsec)**
- **PCMM Traffic Profile - Committed Nominal Polling Interval (microsec)**

- **PCMM Traffic Profile - Committed Peak Data Rate [p] (bytes/sec)**
- **PCMM Traffic Profile - Committed Rate [R] (bytes/sec)**
- **PCMM Traffic Profile - Committed Request Transmission Policy**
- **PCMM Traffic Profile - Committed Required Attribute Mask**
- **PCMM Traffic Profile - Committed Slack Term [S] (microsec)**
- **PCMM Traffic Profile - Committed Target Buffer**
- **PCMM Traffic Profile - Committed Token Bucket Rate [r] (bytes/sec)**
- **PCMM Traffic Profile - Committed Token Bucket Size [b] (bytes)**
- **PCMM Traffic Profile - Committed Tolerated Grant Jitter (microsec)**
- **PCMM Traffic Profile - Committed Tolerated Poll Jitter (microsec)**
- **PCMM Traffic Profile - Committed Traffic Priority (bytes/sec)**
- **PCMM Traffic Profile - Committed Unsolicited Grant Size (bytes)**
- **PCMM Traffic Profile - Committed Upstream Peak Traffic Rate**
- **PCMM Traffic Profile - Envelope**
- **PCMM Traffic Profile - Reserved Assumed Minimum Reserved Traffic Rate Packet Size (bytes)**
- **PCMM Traffic Profile - Reserved Attribute Aggregation Rule Mask**
- **PCMM Traffic Profile - Reserved Downstream Peak Traffic Rate**
- **PCMM Traffic Profile - Reserved Downstream Resequencing**
- **PCMM Traffic Profile - Reserved Forbidden Attribute Mask**
- **PCMM Traffic Profile - Reserved Grants Per Interval**
- **PCMM Traffic Profile - Reserved Maximum Buffer**
- **PCMM Traffic Profile - Reserved Maximum Concatenated Bursts**
- **PCMM Traffic Profile - Reserved Maximum Downstream Latency**
- **PCMM Traffic Profile - Reserved Maximum Packet Size [M] (bytes)**
- **PCMM Traffic Profile - Reserved Maximum Sustained Traffic Rate (bps)**
- **PCMM Traffic Profile - Reserved Maximum Traffic Burst (bytes)**
- **PCMM Traffic Profile - Reserved Minimum Buffer**
- **PCMM Traffic Profile - Reserved Minimum Policed Unit [m] (bytes)**
- **PCMM Traffic Profile - Reserved Minimum Reserved Traffic Rate (bps)**
- **PCMM Traffic Profile - Reserved Nominal Grant Interval (microsec)**
- **PCMM Traffic Profile - Reserved Nominal Polling Interval (microsec)**
- **PCMM Traffic Profile - Reserved Peak Data Rate [p] (bytes/sec)**
- **PCMM Traffic Profile - Reserved Rate [R] (bytes/sec)**
- **PCMM Traffic Profile - Reserved Request Transmission Policy**
- **PCMM Traffic Profile - Reserved Required Attribute Mask**
- **PCMM Traffic Profile - Reserved Slack Term [S] (microsec)**
- **PCMM Traffic Profile - Reserved Target Buffer**
- **PCMM Traffic Profile - Reserved Token Bucket Rate [r] (bytes/sec)**
- **PCMM Traffic Profile - Reserved Token Bucket Size [b] (bytes)**
- **PCMM Traffic Profile - Reserved Tolerated Grant Jitter (microsec)**
- **PCMM Traffic Profile - Reserved Tolerated Poll Jitter (microsec)**
- **PCMM Traffic Profile - Reserved Traffic Priority (bytes/sec)**
- **PCMM Traffic Profile - Reserved Unsolicited Grant Size (bytes)**
- **PCMM Traffic Profile - Reserved Upstream Peak Traffic Rate**

- **PCMM Traffic Profile - Service Class Name**
- **PCMM Traffic Profile - Service Number**
- **PCMM Traffic Profile - Type**
- **PCMM Transaction Id**
- **PCMM User Id**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on values of specific parameters in the protocol message for which there may be an explicit condition. Depending on the parameter chosen, you may be prompted to enter the value to compare against.

where the QoS upgrade is *supported*

Mode

Wireless

Syntax

`where the QoS upgrade is support-option`

Parameters

support-option

One of the following

- **not supported**
- **supported** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines whether the QoS upgrade is supported.

where the quota is *requested*

Mode

Wireless

Syntax

`where the quota is quota-change-type`

Parameters

quota-change-type

One or more of the following:

- **requested** (default)
- **debited**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the type of change to the quota. See *Managing Quotas* for information about defining quotas.

where the quota usage rating conditions changed trigger is one of *specified values*

Mode

Wireless

Syntax

```
where the quota usage rating conditions changed trigger is one of
trigger-type
```

Parameters

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**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the quota usage rating conditions changed. See *Managing Quotas* for information about defining quotas.

where the quota usage reporting reason is one of *specified values*

Mode

Wireless

Syntax

`where the quota usage reporting reason is one of` *`reporting-reason`*

Parameters

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**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the quota usage reporting reason. See *Managing Quotas* for information about defining quotas.

where the RAN-NAS-Release-Cause is *Protocol Type* and *Cause Type*

Mode

Wireless

Syntax

`where the RAN-NAS-Release-Cause is protocol-type and cause-type`

Parameters

protocol-type

- **S1AP Cause**
- **EMM Cause**
- **ESM Cause**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

cause-type

- **n/a**
- **S1AP - Radio Network Layer**
- **S1AP - Transport Layer**
- **S1AP - NAS**
- **S1AP - Protocol**
- **S1AP - Miscellaneous**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines the RAN-NAS-Release-Cause in the request.

where the reauth is triggered by *specified type(s)*

Mode

Wireless

Syntax

`where the reauth is triggered by containment`

Parameters

containment

One or more of the following:

- **TOD**
- **NOTIFICATION**
- **REVALIDATION_TIMEOUT**

Description

Tests whether an RAR is triggered by a the specific event.

where the reauth is triggered by subscriber profile update with notification type *specified type(s)*

Mode

Wireless

Syntax

`where the reauth is triggered by subscriber profile update with notification type` *`specified type(s)`*

Parameters

specified type(s)

One of the following:

- **USER**
- **SUBSCRIBER_POOL**
- **DYNAMIC_QUOTA**
- **POOL_DYNAMIC_QUOTA**
- **ENTITY_STATE**
- **POOL_ENTITY_STATE**
- **QUOTA_ENTITY_USAGE**
- **POOL_QUOTA_ENTITY_USAGE**

Description

Checks whether the RAR is triggered by PNR with changes for the specified type.

Example

The following policy will release the session if the DATA_LIM for the subscriber is changed from non-zero to zero.

```
where the reauth is triggered by subscriber profile update with
notification type SUBSCRIBER_POOL
And where at least one of pool fields DATA_LIM have been updated
And where the policy context property {Previous.Pool.DATA_LIM} is
numerically greater than 0
release the session
accept message
```

The following policy will ignore an RAR that is triggered by the PNR at user level.

```
where the reauth is triggered by subscriber profile update with
notification type USER
accept message
```

where the reauth request is triggered by scheduled task containing *Service key* with *action*

Mode

Wireless

Syntax

`where the reauth request is triggered by scheduled task containing` *`Service key`* `with` *`action`* `action`

Parameters

service

- **Service**
- **User Session Policy**
- **Billing Day**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

key

Name(s) of a specific entity.

- For Service, the key is a Service Code.
- For User Session Policy, the key is a Policy Code
- For Billing Day, the key is set to any.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

action

The action to take for the service.

- **reset**
- **activate** (default)
- **deactivate**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines if the reauth request is triggered by a scheduled task in the specific service using a specific action (activate or deactivate).

where the reauthorization reason is *REASON_REVALIDATION_TIMEOUT*

Mode

Wireless

Syntax

`where the reauthorization reason is` *`reason`*

Parameters

reason

One of the following:

- **REASON_DEFAULT**
- **REASON_AUDIT**
- **REASON_TOD**
- **REASON_LI**
- **REASON_RELEASE_SESSION**
- **REASON_POLICY**
- **REASON_NOTIFICATION**
- **REASON_RETRY**
- **REASON_AF**
- **REASON_REVALIDATION_TIMEOUT** (default)
- **REASON_USER_SCHEDULED_TASK**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines the type of RAR message that is used to reset the usage for a quota.

where the request AVP Media-Component-Description *exists*

Mode

Cable, Wireless

Syntax

`where the request AVP Media-Component-Description` *`accessibility`*

Parameters

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Determines whether the AVP Media-Component-Description is accessible.

where the request AVP *name exists*

Mode

Wireless

Syntax

`where the request AVP avp accessibility`

Parameters

avp

AVP in one of the following formats:

```
name:vendorID
```

or a full path

```
[avp_name1]:vendorID.[avp_name2]:vendorID…
```

for the members of the grouped AVPs

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

accessibility

One of the following:

- **exists** (default)
- **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.

where the request AVP *name* value *contains one of value(s)*

Mode

Wireless

Syntax

`where the request AVP avp value containment value-list`

Parameters

avp

AVP in the format:

```
name:vendorID
```

or a full path

```
[avp_name1]:vendorID.[avp_name2]:vendorID…
```

for the members of the grouped AVPs

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

containment

One of the following:

- **contains one of** (default)
- **does not contain any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Performs a lookup of the sub-strings in the AVP value. It is possible to check multiple sub-string entries at on time. 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.

where the request AVP *name* value *is* contained in Match Lists *select lists*

Mode

Wireless

Syntax

`where the request AVP avp value operator-binary contained in Match Lists match-list`

Parameters

avp

AVP in one of the following formats:

```
name:vendorID
```

or a full path

```
[avp_name1]:vendorID.[avp_name2]:vendorID…
```

for the members of the grouped AVPs

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Compares the specified AVP value with the values or variables from the specified match list. The condition is where the request AVP name value matches one of the values. The values can be evaluated for equality as well as inequality. To evaluate an AVP value for inequality, the condition **matches one of** must be changed to **does not match any of**.

Note: The condition supports both loaded base Diameter AVPs and third-party AVPs.

where the request AVP *name* value is numerically *equal to value*

Mode

Wireless

Syntax

`where the request AVP avp value is numerically operator value`

Parameters

avp

AVP in one of the following formats:

```
name:vendorID
```

or a full path

```
[avp_name1]:vendorID.[avp_name2]:vendorID…
```

for the members of the grouped AVPs

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**

- **equal to**
- **not equal to**

The default for this condition is **equal to**.

value

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the request AVP *name* value *matches one of value(s)*

Mode

Wireless

Syntax

`where the request AVP avp matches-op value-list`

Parameters

avp

AVP in one of the following formats:

```
name:vendorID
```

or a full path

```
[avp_name1]:vendorID.[avp_name2]:vendorID…
```

for the members of the grouped AVPs

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the values. The values can be evaluated for equality as well as inequality. To evaluate an AVP value for inequality, the variable **matches one of** must be changed to **does not match any of**.

Note: The condition supports both loaded base Diameter AVPs and third-party AVPs.

where the request is *creating a new flow*

Mode

Cable, Wireless

Syntax

`where the request is` *`change-type`*

Parameters

change-type

One or more of the following:

- **creating a new flow** (default)
- **modifying an existing flow**
- **provisioning a default flow**
- **terminating an existing flow**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocol messages based on the type of operation being performed on the flow.

where the request is *creating a new session*

Mode

Cable, Wireless

Syntax

`where the request is` *`request-type`*

Parameters

request-type

One or more of the following:

- **creating a new session** (default)
- **modifying an existing session**
- **re-authorizing an existing session**

- **terminating an existing session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocol messages based on the type of operation being performed on the session for the subscriber.

Examples

App Start policy

```
where the request is modifying an existing session
And where the event trigger is one of APPLICATION_START
And where the TDF-Application-Identifier matches one of TDFID01,TDFID02
install pcc_rule1 PCC rule(s) for session
continue processing message
```

App Stop policy

```
where the request is modifying an existing session
And where the event trigger is one of APPLICATION_STOP
And where the TDF-Application-Identifier matches one of TDFID01,TDFID02
remove pcc_rule1 PCC rule(s)
continue processing message
```

where the request is for *downstream* bandwidth

Mode

Wireline

Syntax

`where the request is for qos-direction bandwidth`

Parameters

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Distinguishes between protocol messages based on the direction of bandwidth that is being updated.

where the request is for *reserved* bandwidth

Mode

Cable, Wireless

Syntax

`where the request is for qos-status bandwidth`

Parameters

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocol messages based on the type of bandwidth that is being updated.

where the request *is* for *specified class of* traffic

Mode

Cable, Wireline

Syntax

`where the request operator-binary for class-of-service traffic`

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

class-of-service

Select one or more from the list.

For Cable mode:

- **Best Effort**
- **Non Real-Time Polling**
- **Real-Time Polling**
- **UGS**
- **Background**
- **Conversational**

- **Streaming**
- **Interactive**

For Wireline mode:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocol messages based on the class of service for the network traffic that is being updated.

where the request is for *upstream* bandwidth

Mode

Cable, Wireless

Syntax

`where the request is for` *`qos-direction`* `bandwidth`

Parameters

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocol messages based on the direction of bandwidth that is being updated.

where the request is reporting quota usage using *monitoring key*

Mode

Wireless

Syntax

`where the request is reporting quota usage using` *`mon-key`*

Parameters

mon-key

Name(s) of a monitoring key in the CMP database.

Description

Verifies if the request is reporting any usage with the specified monitoring key. See *Managing Quotas* for information on quotas.

Example

```
where the request is reporting quota usage using VOIIP
grant total volume to Min of 20M bytes and 100 percent used for DATA_Plan
 using SESS
continue processing message
```

where the request is reporting session quota usage

Mode

Wireless

Syntax

```
where the request is reporting session quota usage
```

Parameters

None

Description

Verifies if the request is reporting usage for the quota on the session level. See *Managing Quotas* for information on quotas.

Example

```
where the request is reporting session quota usage
grant total volume to Min of 20M bytes and 100 percent used for DATA_Plan
 using SESS
continue processing message
```

where the request MPS Identifier *matches one of value(s)*

Mode

Cable, Wireless

Syntax

```
where the MPS Identifier matches-op value-list
```

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines whether the MPS Identifier matches a specified value(s).

where the request *supports* feature *name*

Mode

Wireless

Syntax

```
where the request supports feature value-list
```

Parameters

supports

One of the following:

- **supports** (default)
- **does not support**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines whether the request supports a specified feature.

where the requested *downstream* bandwidth is *greater than #* and *less than #* bps

Mode

Wireline

Syntax

```
where the requested qos-direction bandwidth is operator-greater bandwidth
and operator-less bandwidth bps
```

Parameters

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

Description

Selects protocol messages based on the direction and amount of bandwidth being requested, relative to a numeric value range.

where the requested guaranteed *downstream* bandwidth is *greater than #* bps

Mode

Wireline

Syntax

`where the requested guaranteed` *`qos-direction bandwidth`* `is` *`operator bandwidth`* `bps`

Parameters

qos-direction

One of the following:

- **upsteam** (default)

- **downsteam**

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

Description

Selects protocol messages based on the amount of bandwidth being requested in a specific direction relative to a numeric value.

where the requested guaranteed *upstream* bandwidth is *greater than #* bps

Mode

Cable, Wireless

Syntax

`where the requested guaranteed` *`flow-direction`* `bandwidth is` *`operator bandwidth`* `bps`

Parameters

flow-direction

One of the following:

- **upstream**
- **downstream**
- **upstream or downstream** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the amount of bandwidth being requested in a specific direction relative to a numeric value.

where the requested maximum *upstream* bandwidth is *greater than specified* bps

Mode

Cable, Wireless

Syntax

`where the requested maximum` *`flow-direction`* `bandwidth is` *`operator bandwidth`* `bps`

Parameters

flow-direction

One of the following:

- **upstream**
- **downstream**
- **upstream or downstream** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the maximum amount of bandwidth being requested in a specific direction relative to a numeric value.

Example

```
And
    where the request is creating a new session
    where the session is an application session
   where the requested maximum upstream or downstream bandwidth is greater
 than 2400 bps
reject message
```

where the requested media component description reservation priority is one of *specified*

Mode

Cable, Wireless

Syntax

`where the requested media component description reservation priority is one of` *`priority`*

Parameters

priority

One or more of the following:

- **DEFAULT**
- **PRIORITY_ONE**
- **PRIORITY_TWO**
- **PRIORITY_THREE**
- **PRIORITY_FOUR**
- **PRIORITY_FIVE**
- **PRIORITY_SIX**
- **PRIORITY_SEVEN**
- **PRIORITY_EIGHT**
- **PRIORITY_NINE**
- **PRIORITY_TEN**
- **PRIORITY_ELEVEN**
- **PRIORITY_TWELVE**
- **PRIORITY_THIRTEEN**
- **PRIORITY_FOURTEEN**
- **PRIORITY_FIFTEEN**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects Rx protocol messages based on the requested media component description reservation priority.

where the requested minimum *upstream* bandwidth is *greater than specified* bps

Mode

Cable, Wireless

Syntax

`where the requested minimum` *`flow-direction`* `bandwidth is` *`operator bandwidth`* `bps`

Parameters

flow-direction

One of the following:

- **upstream**
- **downstream**
- **upstream or downstream** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the minimum amount of bandwidth being requested in a specific direction relative to a numeric value.

Example

```
And
    where the request is creating a new session
    where the session is an application session
    where the requested minimum upstream bandwidth is greater than 10000
 bps
reject message
```

where the requested QCI is one of *specified*

Mode

Cable, Wireless

Syntax

`where the requested QCI is one of class-of-service`

Parameters

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)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the QoS class identifier (QCI).

where the requested quota is one of *select quota*

Mode

Wireless

Syntax

`where the requested quota is one of quota-name`

Parameters

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the requested quotas. See *Managing Quotas* for information about defining quotas.

where the requested rating group is one of *select rating group*

Mode

Wireless

Syntax

`where the requested rating group is one of rating-group-name`

Parameters

rating-group-name

Names of rating groups that are defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the subscriber's rating group. See *Managing Services and Rating Groups* for information on services.

where the requested service class *matches one of specified name(s)*

Mode

Cable

Syntax

`where the requested service class matches-op service-class-name`

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

service-class-name

Names of service classes that are defined in the CMP database or that have been discovered via SNMP.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the service class name in the request. See *Managing Traffic Profiles* for information on service classes.

where the requested services are *select service*

Mode

Wireless

Syntax

`where the requested services are service-profile-name`

Parameters

service-profile-name

Names of service classes that are defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the services in the request. See *Managing Services and Rating Groups* for information on services.

where the requested session reservation priority is one of *specified*

Mode

Cable, Wireless

Syntax

`where the requested session reservation priority is one of` *`priority`*

Parameters

priority

One or more of the following:

- **DEFAULT**
- **PRIORITY_ONE**
- **PRIORITY_TWO**
- **PRIORITY_THREE**
- **PRIORITY_FOUR**
- **PRIORITY_FIVE**
- **PRIORITY_SIX**
- **PRIORITY_SEVEN**
- **PRIORITY_EIGHT**
- **PRIORITY_NINE**
- **PRIORITY_TEN**
- **PRIORITY_ELEVEN**
- **PRIORITY_TWELVE**
- **PRIORITY_THIRTEEN**
- **PRIORITY_FOURTEEN**
- **PRIORITY_FIFTEEN**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects Rx protocol messages based on the requested session reservation priority.

where the requested time limit is *greater than #* seconds

Mode

Cable

Syntax

`where the requested time limit is operator seconds seconds`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

seconds

A numeric value that specifies time in units of seconds.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the specified time limit.

where the requested time limit is unlimited (or unspecified)

Mode

Cable

Syntax

`where the requested time limit is unlimited (or unspecified)`

Parameters

None

Description

Selects protocol messages that have no time limit.

where the requested *upstream* APN aggregate maximum bitrate is *greater than #* bps

Mode

Wireless

Syntax

`where the requested flow-direction APN aggregate maximum bitrate is operator bandwidth bps`

Parameters

flow-direction

One of the following:

- **upstream**
- **downstream**
- **upstream or downstream** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the maximum bitrate being requested for an access point name (APN) in a specific direction relative to a numeric value.

where the requested volume limit is *greater than #* kilobytes

Mode

Cable

Syntax

`where the requested volume limit is operator bandwidth kilobytes`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the specified volume limit.

where the requested volume limit is unlimited or unspecified

Mode

Cable

Syntax

```
where the requested volume limit is unlimited or unspecified
```

Parameters

None

Description

Selects protocol messages that have no volume limit.

where the Required-Access-Info *matches one of value(s)*

Mode

Wireless

Syntax

where the Required-Access-Info *matches-op info*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

info

One or more of the following actions:

- **USER_LOCATION**
- **MS_TIME_ZONE**
- **USER_LOCATION and MS_TIME_ZONE**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This condition lets you take action based on the value of the Rx Required-Access-Info AVP field.

Example

```
where the Required-Access-Info matches one of USER_LOCATION
```

where the roaming profile for the session is one of Roaming Profile *name*

Mode

Wireless

Syntax

`where the roaming profile for the session is one of Roaming Profile` *`profile-name`*

Parameters

profile-name

Select a profile name from the list of available Roaming Profiles.

Description

This condition lets you identify the current roaming profile associated with the Rx, Gx or the S9 sub session. See *Managing Roaming Profiles* for information on roaming profiles.

where the rule report contains one of *specified rule name(s)* and the final unit action is one of *specified values* and the rule status is *active*

Mode

Wireless

Syntax

`where the rule report contains one of` *`value-list`* `and the final unit action is one of` *`action`* `and the rule status is` *`field`*

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

action

One of the following:

- **TERMINATE**
- **REDIRECT**
- **RESTRICT_ACCESS**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

One of the following:

- **active** (default)

- **inactive**
- **temporarily_inactive**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on whether the message contains a specified rule name, reported final unit action, and status received in a rule report.

where the rule report contains one of *specified rule name(s)* and the rule status is *active*

Mode

Wireless

Syntax

`where the rule report contains one of` *`value-list`* `and the rule status is` *`field`*

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

One of the following:

- **active** (default)
- **inactive**
- **temporarily_inactive**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on whether a rule name and a status was received in a rule report.

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)*

Mode

Wireless

Syntax

```
where the rule report contains one of value-list and the rule status is
field and the rule failure code is one of failcode
```

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

One of the following:

- **active** (default)
- **inactive**
- **temporarily_inactive**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

failcode

One of the following:

- **UNKNOWN_RULE_NAME**
- **RATING_GROUP_ERROR**
- **SERVICE_IDENTIFIER_ERROR**
- **GW_PCEF_MALFUNCTION**
- **RESOURCES_LIMITATION**
- **MAX_NR_BEARERS_REACHED**
- **UNKNOWN_BEARER_ID**
- **MISSING_BEARER_ID**
- **MISSING_FLOW_INFORMATION**
- **RESOURCE_ALLOCATION_FAILURE**
- **UNSUCCESSFUL_QOS_VALIDATION**
- **INCORRECT_FLOW_INFORMATION**
- **PS_TO_CS_HANDOVER**
- **TDF_APPLICATION_IDENTIFIER_ERROR**
- **NO_BEARER_BOUND**
- **FILTER_RESTRICTIONS**
- **AN_GW_FAILED**
- **MISSING_REDIRECT_SERVER_ADDRESS**
- **CM_END_USER_SERVICE_DENIED**
- **CM_CREDIT_CONTROL_NOT_APPLICABLE**
- **CM_AUTHORIZATION_REJECTED**
- **CM_USER_UNKNOWN**
- **CM_RATING_FAILED**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on whether a rule name or names, status, and failure code are received in a rule report.

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

Mode

Wireless

Syntax

```
where the rule report contains one of value-list and the rule status is
field and the rule failure code is one of failcode and the maximum retry
count operator-binary reached
```

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

One of the following:

- **active** (default)
- **inactive**
- **temporarily_inactive**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

failcode

One of the following:

- **UNKNOWN_RULE_NAME**
- **RATING_GROUP_ERROR**
- **SERVICE_IDENTIFIER_ERROR**
- **GW_PCEF_MALFUNCTION**
- **RESOURCES_LIMITATION**
- **MAX_NR_BEARERS_REACHED**
- **UNKNOWN_BEARER_ID**
- **MISSING_BEARER_ID**
- **MISSING_FLOW_INFORMATION**
- **RESOURCE_ALLOCATION_FAILURE**
- **UNSUCCESSFUL_QOS_VALIDATION**
- **INCORRECT_FLOW_INFORMATION**
- **PS_TO_CS_HANDOVER**

- **TDF_APPLICATION_IDENTIFIER_ERROR**
- **NO_BEARER_BOUND**
- **FILTER_RESTRICTIONS**
- **AN_GW_FAILED**
- **MISSING_REDIRECT_SERVER_ADDRESS**
- **CM_END_USER_SERVICE_DENIED**
- **CM_CREDIT_CONTROL_NOT_APPLICABLE**
- **CM_AUTHORIZATION_REJECTED**
- **CM_USER_UNKNOWN**
- **CM_RATING_FAILED**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Selects protocol messages based on whether a rule name or names, status, failure code, and the maximumretry count are reached in a rule report. The maximum retry count is the result of multiplying the Maximum Retry Attempts by the Maximum Retry Cycles (see *Creating a Retry Profile* for details on configuring retry attempts).

where the rule report contains RAN-NAS-Release-Cause and is *Protocol Type* and *Cause Type*

Mode

Wireless

Syntax

`where the rule report contains RAN-NAS-Release-Cause and is` *`protocol-type`* `and` *`cause-type`*

Parameters

protocol-type

- **S1AP Cause**
- **EMM Cause**
- **ESM Cause**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

cause-type

- **n/a**
- **S1AP - Radio Network Layer**

- **S1AP - Transport Layer**
- **S1AP - NAS**
- **S1AP - Protocol**
- **S1AP - Miscellaneous**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines the value of RAN-NAS-Release-Cause in the Charging-Rule-Report.

where the rule report for the flow has status *active*

Mode

Wireless

Syntax

`where the rule report for the flow has status` *`field`*

Parameters

field

One of the following:

- **active** (default)
- **temporarily_inactive**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Tests whether the status of the rule for the flow matches the specified status.

where the *select type* is contained in Match Lists *select lists*

Mode

Wireless

Syntax

`where the` *`field`* `is contained in Match Lists` *`match-list`*

Parameters

field

One or more of the following:

- **Serving Gateway Address** — IP address of the serving gateway
- **APN** — Access Point Name

- **User Equipment IMEISV**
- **User Equipment MEID**
- **User Equipment ESN**
- **User Equipment MAC**
- **USER IMSI** — User International Mobile Subscriber Identity
- **USER E.164** — User E.164 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 LAC
- **Service Area Code** — Unique identifier of a SAC
- **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
- **MPS Identifier** — MPS-Identifier AVP
- **AF Application Id**
- **User MCC-MNC** — Identifies a user MCC-MNC
- **Sponsor Identity** — Sponsor identity AVP
- **App Service Provider Id** — Application services provider identity AVP
- **Entitlements** — A defined entitlement
- **TWAN_SSID** — The SSID for the trusted WLAN (TWAN), in ASCII string format
- **TWAN_BSSID** — The BSSID for the TWAN, in MAC address format
- **TWAN_PLMNId** — The PLMN identifier for the TWAN, in MCC-MNC address format
- **TWAN_OperatorName** — The Operator Name for the TWAN
- **TWAN_RelayIdentity** — The Relay Identity type for the TWAN, in IP address or FQDN format
- **TWAN_CircuitId** — The relay Circuit ID for the TWAN

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 Lists
Black1,Black2,Black3
```

where the *select type* is not contained in Match Lists *select lists*

Mode

Wireless

Syntax

`where the field is not contained in Match Lists match-list`

Parameters

field

One or more of the following:

- **Serving Gateway Address** — IP address of the serving gateway
- **APN** — Access Point Name
- **User Equipment IMEISV**
- **User Equipment MEID**
- **User Equipment ESN**
- **User Equipment MAC**
- **USER IMSI** — User International Mobile Subscriber Identity
- **USER E.164** — User E.164 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 (MCC), Mobile Network Code (MNC)
- **Cell Identifier**
- **Location Area Code** — Unique identifier of a LAC
- **Service Area Code** — Unique identifier of a SAC
- **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
- **MPS Identifier** — MPS-Identifier AVP
- **AF Application Id**
- **User MCC-MNC** — User Mobile Country Code (MCC), Mobile Network Code (MNC)
- **Sponsor Identity** — Sponsor identity AVP
- **App Service Provider Id** — Application services provider identity AVP
- **Entitlements** — A defined entitlement

- **TWAN_SSID** — The SSID for the trusted WLAN (TWAN), in ASCII string format
- **TWAN_BSSID** — The BSSID for the TWAN, in MAC address format
- **TWAN_PLMNId** — The PLMN identifier for the TWAN, in MCC-MNC address format
- **TWAN_OperatorName** — The Operator Name for the TWAN
- **TWAN_RelayIdentity** — The Relay Identity type for the TWAN, in IP address or FQDN format
- **TWAN_CircuitId** — The relay Circuit ID for the TWAN

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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,SAC is not contained in Match Lists
BLACK1,BLACK2,BLACK3
```

where the service info status is one of *specified*

Mode

Cable, Wireless

Syntax

`where the service info status is one of status`

Parameters

status

One of the following:

- **FINAL_SERVICE_INFORMATION**
- **PRELIMINARY_SERVICE_INFORMATION**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects Rx protocol messages based on the service information status.

where the Service-URN is one of *specified value(s)*

Mode

Cable, Wireless

Syntax

`where the Service-URN is one of value-list`

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects Rx protocol messages based on the value of the Service-URN field.

where the session is *an enforcement session*

Mode

Cable, Wireless

Syntax

`where the session is session-type`

Parameters

session-type

One of the following:

- **an enforcement session** (default)
- **an application session**
- **a credit control session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Distinguishes between protocol messages that are operating on different sessions.

where the session granted quota using *monitoring key is* valid

Mode

Wireless

Syntax

```
where the session granted quota using mon-key operator-binary valid
```

Parameters

mon-key

Name(s) of a monitoring key in the CMP database.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Verifies that the session has been granted usage for the specified monitoring key. See *Managing Quotas* for information on quotas.

Example

```
where the session granted quota using VOIP is not valid
grant total volume to Min of 20M bytes and 100 percent used for DATA_Plan
 using SESS
continue processing message
```

where the session granted session level quota *is* valid

Mode

Wireless

Syntax

```
where the session granted session level quota using operator-binary valid
```

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Verifies that the session has been granted usage on the session level. See *Managing Quotas* for information on quotas.

Example

```
where the session granted session level quota is not valid
grant total volume to Min of 20M bytes and 100 percent used for DATA_Plan
 using SESS
continue processing message
```

where the SessionClassID is *specified value*

Mode

Cable

Syntax

`where the SessionClassID is unit`

Parameters

unit

A number between 0 and 255.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on the value of the SessionClassID field.

where the specific action is one of *specified action(s)*

Mode

Wireless

Syntax

`where the specific action is one of action`

Parameters

action

One or more of the following actions:

- **SERVICE_INFORMATION_REQUEST**
- **CHARGING_CORRELATION_EXCHANGE**
- **INDICATION_OF_LOSS_OF_BEARER**

- **INDICATION_OF_RECOVERY_OF_BEARER**
- **INDICATION_OF_RELEASE_OF_BEARER**
- **INDICATION_OF_ESTABLISHMENT_OF_BEARER**
- **INDICATION_OF_IP_CAN_CHANGE**
- **INDICATION_OF_OUT_OF_CREDIT**
- **INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION**
- **INDICATION_OF_FAILED_RESOURCES_ALLOCATION**
- **USAGE_REPORT**
- **ACCESS_NETWORK_INFO_REPORT**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This condition lets you take action based on the value of the Specific-Action AVP field within an Rx RAA message.

where the Sponsor-Identity matches one of *specified Sponsor Identity(s)*

Mode

Wireless

Syntax

`where the Sponsor-Identity matches one of` *`value-list`*

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on whether the Sponsored-Identity AVP matches a list of sponsors. This condition supports sponsored data connectivity.

Example

The following condition is true if the Sponsored-Identity AVP matches either ESPN or FIFA:

```
where the Sponsor-Identity matches one of ESPN,FIFA
```

where the TDF-Application-Identifier matches one of *specified TDF application id(s)*

Mode

Wireless

Syntax

where the TDF-Application-Identifier matches one of *value-list*

Parameters

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Examples

App Start policy

```
where the request is modifying an existing session
And where the event trigger is one of APPLICATION_START
And where the TDF-Application-Identifier matches one of TDFID01,TDFID02
install pcc_rule1 PCC rule(s) for session
continue processing message
```

App Stop policy

```
where the request is modifying an existing session
And where the event trigger is one of APPLICATION_STOP
And where the TDF-Application-Identifier matches one of TDFID01,TDFID02
remove pcc_rule1 PCC rule(s)
continue processing message
```

where the user field *field is* available

Mode

Wireless

Syntax

`where the user field string operator-binary available`

Parameters

string

A string representing the name of a field.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Determines whether a specified user field is available.

where top-up instance being granted for *select type* using *monitoring key is* valid

Mode

Wireless

Syntax

`where top-up instance being granted for` *`select type`* `using` *`mon-key operator-binary`* `valid`

Parameters

select type

Select a data plan.

mon-key

Name(s) of a monitoring key in the CMP database.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Determines whether a specified plan is valid for top-up instance.

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.

where *AMID* is the application manager ID

Mode

Cable, Wireless

Syntax

`where number is the application manager ID`

Parameters

number

A 32-bit numeric value that is greater than 0.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the access manager ID in the message.

where *AppType* is the application type

Mode

Cable

Syntax

`where number is the application type`

Parameters

number

A 16-bit numeric value that is greater than 0.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the application type in the message (this is a sub-field within the AMID).

where the application is latency sensitive

Mode

Cable, Wireless

Syntax

`where the application is latency sensitive`

Parameters

None

Description

Triggers a policy when the associated application is latency sensitive (can be set in the CMP system when applications are defined).

where the application *is* one of *specified name*

Mode

Cable, Wireless

Syntax

`where the application` *`operator-binary`* `one of` *`app-name`*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the associated application.

where the application will be using *greater than #* and *less than #* bps *specified class of* bandwidth

Mode

Wireline

Syntax

`where the application will be using` *`operator-greater bandwidth`* `and` *`operator-less bandwidth`* `bps` *`class-of-service`* `bandwidth`

Parameters

operator-greater

One of the following:

- **greater than or equal to**

- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the associated application as it relates to a defined range. This can be further qualified by the allocation class of service of the bandwidth. The total represents the amount of bandwidth that is allocated if the current request is approved.

where the application will be using *greater than #* and *less than # downstream* sessions

Mode

Wireline

Syntax

`where the application will be using` *`operator-greater number`* `and` *`operator-less number qos-direction`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined range and direction. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using *greater than #* and *less than # specified class of* sessions

Mode

Wireline

Syntax

`where the application will be using operator-greater number and operator-less number class-of-service sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined range. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using *greater than #* bps *upstream reserved* bandwidth

Mode

Cable, Wireless

Syntax

```
where the application will be using operator-greater bandwidth bps
qos-direction qos-status bandwidth
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the application will be using *greater than # specified class of* sessions

Mode

Wireline

Syntax

`where the application will be using` *`operator-greater number class-of-service`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined threshold. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using *greater than #* bps *upstream reserved* bandwidth

Mode

Wireline

Syntax

`where the application will be using` *`operator-greater bandwidth`* `bps` *`qos-direction qos-status`* `bandwidth`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

qos-status

One of the following:

- **reserved** (default)
- **committed**

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.

where the application will be using *greater than #* bps of *specified class* of bandwidth

Mode

Wireline

Syntax

```
where the application will be using operator-greater bandwidth bps of
class-of-service bandwidth
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

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 the allocation class of service of the bandwidth. The total represents the amount of bandwidth that is allocated if the current request is approved.

where the application will be using *greater than #* sessions

Syntax

```
where the application will be using operator-greater number sessions
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

Description

Triggers a policy based on the total number of sessions used by the associated application as it relates to a defined threshold. The total represents the number of sessions that are allocated if the current request is approved.

where the application will be using *greater than # upstream reserved* flows

Mode

Cable, Wireless

Syntax

`where the application will be using` *`operator-greater bandwidth qos-direction qos-status`* `flows`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where there is no application associated with the request

Mode

Cable, Wireless

Syntax

```
where there is no application associated with the request
```

Parameters

None

Description

Triggers a policy when there is no associated application.

Network Devices Conditions

Network Devices 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 *CMP User's Guide* for information on defining the network elements available in your network.

where the An-Gw status is *active*

Mode

Wireless

Syntax

```
where the An-Gw status is active
```

Parameters

active

An-Gw status is either active or inactive.

Click **OK**.

Click **OK**.

Description

Triggers a policy based on whether the An-Gw status is active or not.

where # is the CMTS blade index

Mode

Cable

Syntax

`where number is the CMTS blade index`

Parameters

number

A numeric value between 0 and 255.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for a specific CMTS blade (based on the index number of the blade).

where # is the CMTS channel index

Mode

Cable

Syntax

`where number is the CMTS channel index`

Parameters

number

A numeric value between 0 and 255.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for a specific CMTS channel (based on the index number of the channel).

where the cable modem IP address is *specified address*

Mode

Cable

Syntax

`where the cable modem IP address is ip-address`

Parameters

ip-address

An IPv4 or IPv6 address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for a specific cable modem (based on its IP address).

where the cable modem IP address is in *specified subnet*

Mode

Cable

Syntax

`where the cable modem IP address is in subnet`

Parameters

subnet

- An IPv4 subnet in CIDR notation (for example, 1.2.3.0/24).
- An IPv6 subnet (for example, fc00::1006/64).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for cable modems whose IP address falls within a specific subnet.

where the cable modem MAC address is *specified address*

Mode

Cable

Syntax

`where the cable modem MAC address is mac-address`

Parameters

mac-address

MAC address, in the format *hh:hh:hh:hh:hh:hh*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for protocol messages that are using the MAC address of the cable modem. To evaluate this condition, the MPE device must be configured with cable modem provisioning information.

where the device name *matches one of specified name(s)*

Mode

Cable, Wireless

Syntax

`where the device name` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the device name matches one or more wildcard match patterns.

where the device type *is specified type*

Mode

Cable, Wireless, Wireline

Syntax

`where the device type` *`operator-binary device-type`*

Parameters

operator-binary

One of the following:

- **is** (default)

- **is not**

device-type

In Cable mode, one or more of the following:

- **CMTS**
- **Blade**
- **Channel**
- **Cable Modem**
- **CPE**

In Wireless mode, one or more of the following:

- **PDSN**
- **GGSN**
- **HomeAgent**
- **HSGW**
- **PGW**
- **SGW**
- **DPI**

In Wireline mode, one or more of the following:

One or more of the following:

- **B-RAS**
- **Router**
- **VOD Server**
- **Interface**
- **Subscriber Group**
- **Wireline Gateway**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the device type for which it is evaluated.

where the endpoint IP address is in *specified subnet*

Mode

Cable, Wireless

Syntax

`where the endpoint IP address is in` *`subnet`*

Parameters

subnet

- An IPv4 subnet in CIDR notation (for example, 1.2.3.0/24).

- An IPv6 subnet (for example, fc00::1006/64).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for endpoints whose IP address falls within a specific subnet.

where the endpoint IP address is *specified address*

Mode

Cable, Wireless

Syntax

`where the endpoint IP address is ip-address`

Parameters

ip-address

An IPv4 or IPv6 address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for a specific endpoint (based on its IP address).

where the network element name *matches one of specified name(s)*

Mode

Cable, Wireless, Wireline

Syntax

`where the network element name matches-op value-list`

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the name of the network element for which it is being evaluated.

where the network element type *is specified type*

Mode

Cable, Wireless, Wireline

Syntax

`where the network element type` *`operator-binary element-type`*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

element-type

In Cable mode, the following:

- **CMTS**

In Wireless mode, one or more of the following:

- **GGSN**
- **PDSN**
- **HomeAgent**
- **HSGW**
- **PGW**
- **SGW**
- **DPI**

In Wireline mode, one or more of the following:

One or more of the following:

- **B-RAS**
- **Router**
- **VOD Server**
- **Subscriber Group**
- **Wireline Gateway**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the type of network element for which it is being evaluated. 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.

where the network element's description field is equal to *specified description(s)*

Mode

Wireless, Wireline

Syntax

`where the network element's description field is equal to value`

Parameters

value

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated if the Description field of the network element matches the specified string.

where the network element's diameter identity *matches one of specified description(s)*

Mode

Wireless

Syntax

`where the network element's diameter identity matches-op value-list`

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

The wildcards * (asterisk) and ? (question mark) are allowed.

Description

Triggers a policy that is evaluated based on the diameter identity of the network element.

where the remote MPE is *unavailable*

Mode

Wireless

Syntax

```
where the remote MPE is status
```

Parameters

status

One of the following:

- available
- unavailable

Click **OK**.

Description

Checks whether the remote site in a geo-redundant configuration is available or not.

Example

```
AND
where the enforcement session is an IP-CAN session
where the remote MPE is unavailable
set session revalidation time to 18000 seconds
```

where the request is not using the cable modem IP address

Mode

Cable

Syntax

```
where the request is not using the cable modem IP address
```

Parameters

None

Description

Triggers a policy that is only evaluated for protocol messages that are not using the IP address of the cable modem. In order to know this, the MPE device must be configured with cable modem provisioning information.

where the request is using the cable modem IP address

Mode

Cable

Syntax

```
where the request is using the cable modem IP address
```

Parameters

None

Description

Triggers a policy that is only evaluated for protocol messages that are not using the IP address of the cable modem. In order to know this, the MPE device must be configured with cable modem provisioning information.

where the User Equipment ESN *matches one of specified ESN value(s)*

Mode

Wireless

Syntax

`where the User Equipment ESN` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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`.

where the User Equipment IMEISV *matches one of specified IMEISV value(s)*

Mode

Wireless

Syntax

`where the User Equipment IMEISV` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the User Equipment MAC *matches one of specified MAC value(s)*

Mode

Wireless

Syntax

`where the User Equipment MAC` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific Media Access Control (MAC) values (based on matching wildcard patterns). A MAC address is formatted as six groups of two hexadecimal digits separated by colons (:) or hyphens (-).

where the User Equipment MEID *matches one of specified MEID value(s)*

Mode

Wireless

Syntax

`where the User Equipment MEID` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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`.

Device Usage Conditions

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.

where the device will be handling *greater than #* and *less than #* bps of *specified class of* sessions

Mode

Wireline

Syntax

`where the device will be handling` *`operator-greater number`* `and` *`operator-less number`* `bps of` *`class-of-service`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined range. This can be further qualified by the class of service of the sessions. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than #* and *less than #* bps of *specified class of* bandwidth

Mode

Wireline

Syntax

`where the device will be handling` *`operator-greater bandwidth`* `and` *`operator-less bandwidth`* `bps of` *`class-of-service`* `bandwidth`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined range. This can be further qualified by the class of service of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than #* and *less than #* percent of *downstream* capacity

Mode

Wireline

Syntax

```
where the device will be handling operator-greater bandwidth and
operator-less bandwidth percent of qos-direction bandwidth
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the percentage of capacity used by the current device as it relates to a defined range. This can be further qualified by the direction of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than #* and *less than # specified class of* sessions

Mode

Wireline

Syntax

`where the device will be handling` *`operator-greater number`* `and` *`operator-less number class-of-service`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**

- **less than** (default)

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined range. This can be further qualified by the class of service of the sessions. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than #* bps *downstream* bandwidth

Mode

Wireline

Syntax

```
where the device will be handling operator-greater bandwidth bps
qos-direction bandwidth
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined threshold and direction. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than #* bps of *specified class of* bandwidth

Mode

Wireline

Syntax

```
where the device will be handling operator-greater bandwidth bps of
class-of-service bandwidth
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the current device as it relates to a defined threshold. This is further qualified by the class of service of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than #* bps *upstream reserved* bandwidth

Mode

Cable, Wireless

Syntax

`where the device will be handling` *`operator bandwidth`* `bps` *`qos-direction qos-status`* `bandwidth`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the device will be handling *greater than #* bps *upstream reserved* bandwidth in total for *specified application*

Mode

Cable, Wireless

Syntax

```
where the device will be handling operator bandwidth bps bandwidth
qos-direction qos-status bandwidth in total for app-name
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

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.

where the device will be handling *greater than #* bps *reserved* bandwidth in total for *specified class of* traffic

Mode

Cable

Syntax

```
where the device will be handling operator bandwidth bps qos-status bandwidth
in total for class-of-service traffic
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**
- **Real-time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total amount of bandwidth allocated for specific classes of service by the current device as it relates to a defined threshold. This can be further qualified by the allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than # downstream* sessions

Mode

Wireline

Syntax

`where the device will be handling` *`operator-greater number qos_direction`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

See common parameters.

qos-direction

See common parameters.

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined direction and threshold. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than #* percent of *downstream* capacity

Mode

Wireline

Syntax

`where the device will be handling` *`operator percent`* `percent of` *`qos-direction`* `capacity`

Parameters

operator

One of the following:

- **greater than or equal to**

- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

percent

A numeric value.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

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 the direction of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than #* percent of *reserved* capacity for *specified class of* traffic

Mode

Cable

Syntax

```
where the device will be handling operator percent percent of qos-status
capacity for class-of-service traffic
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

percent

An integer value between 0 and 100.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**
- **Real-time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the percent of bandwidth capacity allocated for specific classes of service by the current device as it relates to a defined threshold. This can be further qualified by the allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the device will be handling *greater than #* percent of *upstream reserved* capacity

Mode

Cable, Wireless

Syntax

`where the device will be handling` *`operator percent`* `percent of` *`qos-direction qos-status`* `capacity`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

percent

An integer value between 0 and 100.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the device will be handling *greater than #* percent of *upstream reserved* capacity for *specified application*

Mode

Cable, Wireless

Syntax

`where the device will be handling` *`operator percent`* `percent of` *`qos-direction qos-status`* `capacity for` *`app-name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

percent

An integer value between 0 and 100.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

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.

where the device will be handling *greater than # reserved* flows in total for *specified class of* traffic

Mode

Cable

Syntax

`where the device will be handling` *`operator number qos-status`* `flows in total for` *`class-of-service`* `traffic`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**
- **Real-time Polling**
- **UGS**

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total number of flows for specific classes of service used by the current device as it relates to a defined threshold. This can be further qualified by the allocation status of the flows. The total represents the number of flows that are allocated if the current request is approved.

where the device will be handling *greater than # specified class of* sessions

Mode

Wireline

Syntax

`where the device will be handling` *`operator-greater number class-of-service`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One or more of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions used by the device as it relates to a defined threshold. The total represents the number of sessions that are allocated if the current request is approved.

where the device will be handling *greater than # upstream reserved* flows

Mode

Cable, Wireless

Syntax

`where the device will be handling` *`operator number qos-direction qos-status`* `flows`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the device will be handling *greater than # upstream reserved* flows in total for *specified application*

Mode

Cable, Wireless

Syntax

`where the device will be handling` *`operator number qos-direction qos-status`* `flows in total for` *`app-name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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).

where network initiated requests are *supported*

Mode

Wireless

Syntax

`where network initiated requests are support`

Parameters

support

One of the following:

- **not supported**
- **supported** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated when network initiated requests are or are not supported.

where the APN *matches one of specified APN value(s)*

Mode

Wireless

Syntax

`where the APN matches-op match-list`

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific access point name (APN) values (based on matching wildcard patterns). A valid APN value is any domain name; for example: `network.operator.com`.

where the BSID *matches one of specified Bsid value(s)*

Mode

Wireless

Syntax

`where the BSID` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific BSID values (based on matching wildcard patterns).

where the Cell Identifier *matches one of specified CI value(s)*

Mode

Wireless

Syntax

`where the Cell Identifier` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the cell state is *specified*

Mode

Wireless

Syntax

`where the cell state is` *`state`*

Parameters

state

One of the following:

- **congested**
- **not congested**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is evaluated based on the level of congestion in the cell.

where the E-UTRAN Cell Identifier *matches one of specified ECI value(s)*

Mode

Wireless

Syntax

`where the E-UTRAN Cell Identifier` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific E-UTRAN Cell Identifier values (based on matching wildcard patterns).

where the IP address of the Serving Gateway *matches one of specified address(es)*

Mode

Wireless

Syntax

`where the IP address of the Serving Gateway` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific Serving Gateway addresses (based on matching wildcard patterns).

where the IP address of the Serving PCF *matches one of specified address(es)*

Mode

Wireless

Syntax

`where the IP address of the Serving PCF` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific Serving PCF addresses (based on matching wildcard patterns).

where the IP-CAN type is *specified*

Mode

Wireless

Syntax

`where the IP-CAN type is` *`ip-can-type`*

Parameters

ip-can-type

One or more of the following:

- **3GPP GPRS**

- **3GPP EPS**
- **Non_3GPP EPS**
- **3GPP2**
- **WiMAX**
- **DOCSIS**
- **xDSL**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for a protocol message with a specific IP-CAN type.

where the Location Area Code *matches one of specified LAC value(s)*

Mode

Wireless

Syntax

`where the Location Area Code` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the mobile session *supports* sponsored connectivity

Mode

Wireless

Syntax

`where the mobile session` *`support`* `sponsored connectivity`

Parameters

support

One of the following:

- **does not support**
- **supports** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that evaluates whether or not the mobile session supports sponsored data connectivity. This condition supports sponsored data connectivity for both Gx and Rx requests.

Example

The following condition evaluates as true of the mobile session supports sponsored data connectivity:

```
where the mobile session supports sponsored connectivity
```

where the MSTimezone DST is *configured daylight savings in hours*

Mode

Wireless

Syntax

`where the MSTimezone DST is offset`

Parameters

offset

One of the following:

- **0 hours**
- **1 hour**
- **2 hours**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated if the applied Daylight Saving Time offset for the location of a mobile subscriber/mobile station (MS) matches the parameter.

where the MSTimezone offset is *configured timezone offset*

Mode

Wireless

Syntax

`where the MSTimezone offset is offset`

Parameters

offset

Greenwich Mean Time (GMT) time zone offset.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated if the applied time zone for a mobile subscriber/mobile station (MS) matches the parameter.

where the RAT type is *specified*

Mode

Wireless

Syntax

`where the RAT type is rat-type`

Parameters

rat-type

One or more of the following:

- **GERAN**
- **UTRAN**
- **HSPA Evolution**
- **UMA/GAN**
- **EUTRAN**
- **WLAN**
- **CDMA2000 1x**
- **HRPD**
- **UMB**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 a high rate packet data (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
```

where the Routing Area Code *matches one of specified RAC value(s)*

Mode

Wireless

Syntax

`where the Routing Area Code` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific RAC values (based on matching wildcard patterns).

where the Routing Area Identifier *matches one of specified RAI value(s)*

Mode

Wireless

Syntax

`where the Routing Area Identifier` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the Service Area Code *matches one of specified SAC value(s)*

Mode

Wireless

Syntax

`where the Service Area Code` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the Serving MCC-MNC *matches one of specified MCC-MNC value(s)*

Mode

Wireless

Syntax

`where the Serving MCC-MNC` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the *CMP User's Guide* for information on mapping serving gateways to MCCs and MNCs.

where the subscribed PRA area *matches one of specified PRA area(s)*

Mode

Wireless mode with the 3GPP mode enabled.

Syntax

`where the subscribed PRA area` *`matches-op pra-areas`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

pra-areas

One of the following:

- **predefined PRA lists** — select one or more defined PRA lists

- **manual input** — enter the identifier for the PRA in hexadecimal format or a custom PRA from a subscriber profile in the format *{User.CustomField}*. For information on creating custom fields in subscriber profiles, see your CMP User's Guide.
- **default area** — the PRA to which the user equipment is already subscribed, if any.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific PRA values. If **default area** is selected as the definition for the parameter *pra-areas*, the policy is only evaluated if the user equipment is already subscribed to a PRA.

where the Tracking Area Code *matches one of specified TAC value(s)*

Mode

Wireless

Syntax

`where the Tracking Area Code matches-op match-list`

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific Tracking Area Code values (based on matching wildcard patterns).

where the UE is *inside/outside* subscribed PRA area

Mode

Wireless mode with the 3GPP mode enabled.

Syntax

`where the UE is location subscribed PRA area`

Parameters

location

One of the following:

- **inside**
- **outside**

Description

Triggers a policy that is only evaluated when the user equipment is or is not inside the subscribed PRA.

User Conditions

User conditions are related to the quota pool, 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. The following conditions are available.

where at least one of *subscriber or pool* fields *named* have been updated

Syntax

`where at least one of subscriber fields field-name have been updated`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

field-name

String.

Description

Triggers a policy based on whether at least one flow with one of the specified media types matches at least one of the specified statuses.

Example

The following policy will release the session if the DATA_LIM for the subscriber is changed from non-zero to zero.

```
where the reauth is triggered by subscriber profile update with
notification type SUBSCRIBER_POOL
And where at least one of pool fields DATA_LIM have been updated
And where the policy context property {Previous.Pool.DATA_LIM} is
numerically greater than 0
release the session
accept message
```

where the account id *matches one of specified id(s)*

Mode

Cable, Wireline

Syntax

`where the account id` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific user ID values (based on matching wildcard patterns). See *CMP User Guide* for information on managing subscriber accounts.

where the account will be handling *greater than #* and *less than #* percent of *downstream* limit

Mode

Wireline

Syntax

`where the account will be handling` *`operator-greater percent`* `and` *`operator-less percent`* `percent of` *`qos-direction`* `limit`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

operator-less

One of the following:

- **less than or equal to**

- **less than** (default)

percent

A numeric value.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the percent of the bandwidth limit used by the account related to a defined range. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be handling *greater than #* percent of *downstream* limit

Mode

Wireline

Syntax

`where the account will be handling` *`operator percent`* `percent of` *`qos-direction`* `limit`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

percent

A numeric value.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the percent of the bandwidth limit used by the account as it relates to a defined threshold. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be handling *greater than #* percent of *upstream reserved* limit

Mode

Cable

Syntax

`where the account will be handling` *`operator percent`* `percent of` *`qos-direction qos-status`* `limit`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

percent

An integer value between 0 and 100.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the percent of the bandwidth limit used by the account as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total is the bandwidth allocated if the request is approved.

where the account will be using *greater than #* and *less than #* bps *downstream* bandwidth

Mode

Wireline

Syntax

`where the account will be using` *`operator-greater bandwidth`* `and` *`operator-less bandwidth`* `bps` *`qos-direction`* `bandwidth`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined range. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be using *greater than #* and *less than # downstream* sessions

Mode

Wireline

Syntax

`where the account will be handling` *`operator-greater number`* `and` *`operator-less number qos-direction`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the number of sessions for a specific direction of service used by the account as it relates to a defined range. The total is the number of sessions allocated if the request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be using *greater than #* bps *downstream* bandwidth

Mode

Wireline

Syntax

```
where the account will be using operator bandwidth bps qos-direction
bandwidth
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined threshold. This can be further qualified by the direction of the bandwidth. The total is the bandwidth allocated if the request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be using *greater than #* bps of *specified class of* bandwidth

Mode

Wireline

Syntax

```
where the account will be using operator-greater number bps of
class-of-service bandwidth
```

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined threshold. This can be further qualified by the class of service of the bandwidth. The total is the amount of bandwidth allocated if the request is approved.

where the account will be using *greater than # downstream* sessions

Mode

Wireline

Syntax

```
where the account will be using operator number qos-direction sessions
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Description

Triggers a policy based on the total number of sessions used by the associated account as it relates to a defined threshold. This can be further qualified by the direction of the sessions. The total represents the number of sessions that are allocated if the current request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be using *greater than # specified class of* sessions

Mode

Wireline

Syntax

`where the account will be using` *`operator-greater number class-of-service`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions for specific classes of service used by the account as it relates to a defined threshold. This can be further qualified by the class of the sessions. The total is the number of sessions allocated if the request is approved. See *CMP User Guide* for information on managing subscriber accounts.

where the account will be using *greater than #* bps upstream bandwidth in total for *specified application*

Mode

Cable

Syntax

```
where the account will be using operator bandwidth bps upstream bandwidth
in total for app-name
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total amount of bandwidth allocated for specific applications by the associated account as it relates to a defined threshold. The total represents the bandwidth that is allocated if the current request is approved. See *Managing Application Profiles* for information on applications.

where the account will be using *greater than #* bps *reserved* bandwidth in total for *specified class of* traffic

Mode

Cable

Syntax

`where the account will be using` *`operator bandwidth`* `bps` *`qos-status`* `bandwidth in total for` *`class-of-service`* `traffic`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**

- **Real-time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total amount of bandwidth for specific classes of service used by the associated accounts as it relates to a defined threshold. This can be further qualified by the allocation status of the bandwidth. The total represents the amount of bandwidth that are allocated if the current request is approved.

where the account will be using *greater than #* bps *upstream reserved* bandwidth

Mode

Cable

Syntax

```
where the account will be using operator bandwidth bps qos-direction
qos-status bandwidth
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total amount of bandwidth used by the account as it relates to a defined threshold. This can be further qualified by both the direction and allocation status of the bandwidth. The total is the bandwidth allocated if the request is approved.

where the account will be using *greater than # reserved* flows in total for *specified class of* traffic

Mode

Cable

Syntax

```
where the account will be using operator number qos-status flows in total
for class-of-service traffic
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**
- **Real-time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total number of flows for specific classes of service used by the associated accounts as it relates to a defined threshold. This can be further qualified by the allocation status of the flows. The total represents the number of flows that are allocated if the current request is approved.

where the account will be using *greater than #* upstream flows in total for *specified application*

Mode

Cable

Syntax

`where the account will be using` *`operator number`* `upstream flows in total for` *`app-name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total number of flows for specific applications used by the associated accounts as it relates to a defined threshold. The total represents the number of flows that are allocated if the current request is approved. See *Managing Application Profiles* for information on applications.

where the account will be using *greater than # upstream reserved* flows

Mode

Cable

Syntax

`where the account will be using` *`operator number qos-direction qos-status`* `flows`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total number of flows used by the associated account 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.

where the *subscriber or pool* does not have any of the *named* entitlements

Mode

Wireless

Syntax

`where the subscriber does not have any of the value-list entitlements`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See the *CMP Wireless User's Guide* for information on entitlements.

where the *subscriber or pool* does not have at least one of the *named* entitlements

Mode

Wireless

Syntax

`where the subscriber does not have at least one of the value-list entitlements`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See the *CMP Wireless User's Guide* for information on entitlements.

where the *subscriber or pool field + 0 days rounded up* with *same* granularity is *after now* using *configured local time*

Mode

Wireless

Syntax

`where the subscriber field-name direction duration granularity1 rounded rounding with granularity2 granularity is datetime-compare datetime using time-zone`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field-name

String representing a datetime.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

direction

One of the following, indicating future or past:

- **+** (default)
- **-**

duration

Positive integer.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

granularity1

The calculated datetime is expressed in this granularity:

- **days** (default)

- **months**
- **hours**
- **minutes**

rounding

One of the following, indicating rounding up or down:

- **up**
- **down**

granularity2

Rounding, either up or down, is expressed in this granularity:

- **same** (same as *granularity1*)
- **months**
- **days**
- **hours**
- **minutes**

datetime-compare

One of the following:

- **after** (default)
- **before**
- **at or before**
- **at or after**

datetime

One of the following:

- The local date-time **now** (default)
- A policy variable
- A date-time in the format: `yyyy-mm-ddThh:mm:ss+UTCoffset`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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

subscriber 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.

Example

```
where the FamilyPlanGold PromoEnrollTime + 10 days rounded up with same
granularity is before now using configured local time
```

where the *subscriber or pool field exists*

Mode

Wireless

Syntax

`where the subscriber fieldname accessibility`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

fieldname

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

accessibility

One of the following:

- **exists** (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 subscriber pool data.

where the *subscriber or pool field exists* before update

Mode

Wireless

Syntax

```
where the subscriber fieldname accessibility before update
```

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

fieldname

String.

accessibility

One of the following:

- **exists** (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 if the pool or subscriber existed before provisioning. For information on quota pools, see *Managing Quotas*.

where the *subscriber or pool field* is *in* the current billing cycle using *configured local time*

Mode

Wireless

Syntax

```
where the subscriber field-name is comparison-op the current billing cycle
using time-zone
```

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

comparison-op

One of the following:

- **in** (default)
- **not in**
- **before**
- **after**

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 subscriber 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.

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.

where the *subscriber or pool field is* modified via notification

Mode

Wireless

Syntax

```
where the subscriber field-name operator-binary modified via notification
```

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Triggers a policy that is evaluated based on the reception of a notification of a change to the subscriber or subscriber pool field value.

where the *subscriber or pool field* is numerically *equal to value*

Mode

Wireless

Syntax

`where the subscriber field-name is numerically operator value`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **equal to**.

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 $2^{63}-1$).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 subscriber pool.

Example

```
where the FamilyPlanGold total-session-count is numerically less than 5
```

where the *subscriber or pool field matches one of specified value(s)*

Mode

Wireless

Syntax

```
where the subscriber field-name matches-op match-list
```

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 subscriber pool.

where the *subscriber or pool field* prior to notification *matches one of specified value(s)*

Mode

Wireless

Syntax

`where the subscriber field-name prior to notification matches-op match-list`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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) prior to notification for the subscriber or subscriber pool.

where the *subscriber or pool* has all of the *named* entitlements

Mode

Wireless

Syntax

`where the subscriber has all of the value-list entitlements`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See the *CMP Wireless User's Guide* for information on entitlements.

where the *subscriber or pool* has at least one of the *named* entitlements

Mode

Wireless

Syntax

`where the subscriber has at least one of the value-list entitlements`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See the *CMP Wireless User's Guide* for information on entitlements.

where the *subscriber or pool* profile data *is* available

Mode

Wireless

Syntax

`where the subscriber profile data operator-binary available`

Parameters

subscriber

One of the following:

- **subscriber** (default) — Individual subscriber
- **pool** — Subscriber pool defined on the SPR

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Triggers a policy based on whether subscriber or subscriber pool data is or is not available.

where the pool type is *basic*

Mode

Wireless

Syntax

`where the pool type is pool-type`

Parameters

pool-type

Select one of the following:

- **basic**
- **enterprise**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated if the pooled quota group type matches the selected type.

Example

```
where the pool type is enterprise
```

where the subscriber profile data *expiration timestamp field for day pass in millis* is less than *hours from expiration* hours from expiring

Mode

Wireless

Syntax

`where the subscriber profile data` *`field-name`* `is less than` *`number`* `hours from expiring`

Parameters

field-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the value of a subscriber profile timestamp field is less than the specified number of hours away.

where the tier *is* one of *specified tier(s)*

Mode

Cable, Wireless, Wireline

Syntax

`where the tier` *`operator-binary`* `one of` *`tiers`*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

tiers

A comma-separated list of names of one more tiers defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is or is not evaluated for one or more specific tiers. See *CMP User Guide* for information on managing tiers.

where the tier will be handling *greater than #* and *less than # specified class of* sessions

Mode

Wireline

Syntax

`where the tier will be handling` *`operator-greater number`* `and` *`operator-less number class-of-service`* `session`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions for a specific class of service used by the tier as it relates to a defined range. The total is the number of sessions allocated if the request is approved. See *CMP User Guide* for information on managing tiers.

where the tier will be handling *greater than # specified class of* sessions

Mode

Wireline

Syntax

`where the tier will be handling` *`operator-greater number class-of-service`* `sessions`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total number of sessions for a specific class of service used by the tier as it relates to a defined threshold. The total is the number of sessions allocated if the request is approved. See *CMP User Guide* for information on managing tiers.

where the tier will be using *greater than #* bps of *specified class of* bandwidth

Mode

Wireline

Syntax

`where the tier will be using` *`operator-greater number`* `and` *`operator-less number`* `bps of` *`class-of-service`* `bandwidth`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the tier as it relates to a defined threshold. This is further qualified by the class of service of the bandwidth. The total is the amount of bandwidth allocated if the request is approved. See *CMP User Guide* for information on managing tiers.

where the tier will be using *greater than #* and *less than #* bps of *specified class of* bandwidth

Mode

Wireline

Syntax

`where the tier will be using` *`operator-greater number`* `and` *`operator-less number`* `bps of` *`class-of-service`* `bandwidth`

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

number

A numeric value.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**
- **Real-time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Description

Triggers a policy based on the total amount of bandwidth used by the tier as it relates to a defined range. This can be further qualified by the class of service of the bandwidth. The total is the amount of bandwidth allocated if the request is approved. See *CMP User Guide* for information on managing tiers.

where the user E.164 phone number *matches one of specified number(s)*

Mode

Wireless

Syntax

`where the E.164 phone number` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user has *greater than #* of passes named *select type*

Mode

Wireless

Syntax

`where the user has` *`operator number`* `of passes named` *`pass_name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pass_name

Select a name from the pass selection pop-up.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the number of selected passes.

where the user has *greater than #* of rollover units of type *unit type* for plan *plan name* and usage *usage type*

Mode

Wireless

Syntax

`where the user has operator number of rollover units of type unit_type for plan plan_name and usage usage_type`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

unit_type

One of the following:

- **Time**
- **Volume**
- **Service Specific**
- **Uplink Volume**
- **Downlink Volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

plan_name

Select a name from the plan selection pop-up.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

usage_type

One of the following:

- **Limit**
- **Available**

- **Consumed**

  Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the number of rollover units of a selected unit type for a selected plan and selected usage type.

where the user has *greater than #* of top-ups for plan *select type*

Mode

Wireless

Syntax

`where the user has` *`operator number`* `of top-ups for plan` *`plan-name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

plan-name

Select a name from the plan selection pop-up.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the number of top-ups in the selected plan.

where the user IMSI *matches one of specified number(s)*

Mode

Wireless

Syntax

`where the user IMSI` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user is a *home* user

Mode

Wireless

Syntax

`where the user is a` *`user-type`* `user`

Parameters

user-type

One of the following:

- **home**
- **visiting**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Defines the user type. A user is local (home) when the MCC-MNC from the IMSI matches an MCC-MNC configured in the home MCC-MNC match list(s); otherwise, the user is visiting. If the IMSI is not available, the user is deemed local.

where the user is using *greater than #* bytes in *total* volume for *selected* quota

Mode

Wireless

Syntax

`where the user is using` *`operator number`* `bytes in` *`service-type`* `volume for` *`quota-name`* `quota`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 (default). See *Managing Quotas* for information on quotas.

where the user is using *greater than #* percent and *less than #* percent of *select type* for *selected* quota

Mode

Wireless

Syntax

`where the user is using` *`operator extended-percent`* `percent and` *`operator extended-percent`* `percent of` *`service-type`* `for` *`quota-name`* `quota`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than** for the first occurance and **less than** for the second.

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

service-type

One of the following:

- **time**
- **total volume**
- **uplink volume**
- **downlink volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user is using *greater than #* percent of *select type* for *selected* quota

Mode

Wireless

Syntax

```
where the user is using operator extended-percent percent of service-type
for quota-name quota
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

service-type

One of the following:

- **time**
- **total volume**
- **uplink volume**
- **downlink volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user is using *greater than #* seconds in total for *selected* quota

Mode

Wireless

Syntax

`where the user is using operatorseconds seconds in total for quota-name quota`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

seconds

A numeric value that specifies time in units of seconds.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user is using *greater than #* service-specific units for *selected* quota

Mode

Wireless

Syntax

`where the user is using` *`operator number`* `service-specific units for` *`quota-name`* `quota`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user is using dynamic quota for *selected*

Mode

Wireless

Syntax

`where the user is using dynamic quota for` *`quota-name`*

Parameters

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This condition allows the PCRF to send SMS messages when the user's quota usage reaches a certain usage ratio. It checks to see if the user is using any dynamic quota of a specified quota profile. See *Managing Quotas* for information on quotas.

where the user is using *greater than #* percent *select type* of dynamic quota for *selected*

Mode

Wireless

Syntax

`where the user is using` *`operator number`* `percent` *`service-type`* `of dynamic quota for` *`quota-name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

number

A number with the maximum of 6 decimals within the range: 0-10000.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

service-type

One of the following:

- **time**
- **total volume**
- **uplink volume**
- **downlink volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This condition allows the PCRF to send SMS messages when the user's quota usage reaches a certain usage ratio. It checks to see whether the used service unit (USU) of a dynamic quota of a specified quota profile exceeds the specified percent for the specified type. See *Managing Quotas* for information on quotas.

where the user is using *greater than #* percent and *less than #* percent *select type* of dynamic quota for *selected*

Mode

Wireless

Syntax

`where the user is using` *`operator-greater number`* `percent and` *`operator-less number`* `percent of` *`service-type`* `for dynamic` *`quota-name`*

Parameters

operator-greater

One of the following:

- **greater than or equal to**
- **greater than** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-less

One of the following:

- **less than or equal to**
- **less than** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

number

A number with the maximum of 6 decimals within the range: 0-10000.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

service-type

One of the following:

- **time**
- **total volume**
- **uplink volume**
- **downlink volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This condition allows the PCRF to send SMS messages when the user's quota usage reaches a certain usage ratio. It checks to see whether the used service unit (USU) of a dynamic quota of a specified quota profile is within the specified percent range for the specified type. See *Managing Quotas* for information on quotas.

where the user NAI *matches one of specified id(s)*

Mode

Wireless

Syntax

`where the user NAI` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific NAI values (based on matching wildcard patterns).

where the user realm *matches one of specified realm(s)*

Mode

Wireless

Syntax

`where the user realm` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific realms (based on matching wildcard patterns).

where the user *Service key exists*

Mode

Wireless

Syntax

```
where the user service key field accessibility
```

Parameters

service

One of the following:

- **Service**
- **User Session Policy**
- **User Location**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

key

Name(s) of a specific entity.

- For Service, the key is a Service Code.
- For User Session Policy, the key is a Policy Code
- For User Location, the key is a Location Code.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

The name of a field belonging to the selected service.

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Determines if the selected service exists.

where the user *Service key field contains one of specified value(s)*

Mode

Wireless

Syntax

```
where the user service key field containment value-list
```

Parameters

service

- **Service** (default)
- **User Session Policy**
- **User Location**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

key

Name(s) of a specific entity.

- For Service, the key is a Service Code.
- For User Session Policy, the key is a Policy Code
- For User Location, the key is either a Location Code or a Policy Code.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

The name of a field belonging to the selected service.

containment

One of the following:

- **contains one of** (default)
- **does not contain any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines if the entity field contains the specified value.

where the user *Service key field matches one of value(s)*

Mode

Wireless

Syntax

```
where the user service key field matches-op match-list
```

Parameters

service

- **Service**
- **User Session Policy**
- **User Location**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

key

Name(s) of a specific entity.

- For Service, the key is a Service Code.
- For User Session Policy, the key is a Policy Code
- For User Location, the key is either a Location Code or a Policy Code.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

The name of a field belonging to the selected service.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy when the specified fields match the selected entity.

where the user *Service key field* prior to notification *matches one of* previous value

Mode

Wireless

Syntax

`where the user` *`service key field`* `prior to notification` *`matches-op`* `previous value`

Parameters

service

- **Service**
- **User Session Policy**
- **User Location**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

key

Name(s) of a specific entity.

- For Service, the key is a Service Code.
- For User Session Policy, the key is a Policy Code
- For User Location, the key is either a Location Code or a Policy Code.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

field

The name of a field belonging to the selected service.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

Description

Determines if the field value of a service changed because of a notification request from SPR.

where the user *Service key* is *in* the activation timeframe using *configured local time*

Mode

Wireless

Syntax

```
where the user service key is comparison-op the activation timeframe using
time-zone
```

Parameters

service

- **Service** (default)
- **User Session Policy**
- **User Location**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

key

Name(s) of a specific entity.

- For Service, the key is a Service Code.
- For User Session Policy, the key is a Policy Code
- For User Location, the key is a Location Code.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

comparison-op

One of the following:

- **in** (default)
- **not in**
- **before**
- **after**

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Determines if the specific entity is active by comparing the start/end time for the entity with the current time.

where the user SIP URI *matches one of specified URI(s)*

Mode

Wireless

Syntax

`where the user SIP URI` *`matches-op match-list`*

Parameters

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated for one or more specific SIP URI values (based on matching wildcard patterns).

where the user will be handling *greater than #* percent of *upstream reserved* limit

Mode

Wireless

Syntax

`where the user will be handling` *`operator percent`* `percent of` *`qos-direction`* `for` *`qos-status`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

percent

An integer value between 0 and 100.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user will be using *greater than #* bps *upstream reserved* bandwidth

Mode

Wireless

Syntax

`where the user will be using` *`operator bandwidth`* `bps` *`qos-direction qos-status`* `bandwidth`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second

m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total amount of bandwidth allocated. 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.

where the user will be using *greater than #* bps *upstream reserved* bandwidth in total for *specified application*

Mode

Wireless

Syntax

`where the user will be using` *`operator bandwidth`* `bps` *`qos-direction qos-status`* `bandwidth in total for` *`app-name`*

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**

- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user will be using *greater than # upstream reserved* flows

Mode

Wireless

Syntax

`where the user will be using` *`operator number qos-direction qos-status`* `flows`

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the user will be using *greater than #* bps *reserved* bandwidth in total for *specified class of* traffic

Mode

Wireless

Syntax

```
where the user will be using operator bandwidth bps qos-status bandwidth
in total for class-of-service traffic
```

Parameters

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

class-of-service

In Wireless mode, one (or more) of the following:

- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Cable mode, one (or more) of the following:

- **Best Effort**
- **Non Real-time Polling**
- **Real-time Polling**
- **UGS**
- **Background**
- **Conversational**
- **Streaming**
- **Interactive**

In Wireline mode, one of the following:

- **Standard Definition**
- **High Definition**

One of the following:

- **Standard Definition**
- **High Definition**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the total amount of bandwidth allocated for specific classes of service by the associated subscriber as it relates to a defined threshold. This can be further qualified by the allocation status of the bandwidth. The total represents the bandwidth that is allocated if the current request is approved.

where the user will be using *greater than # upstream reserved* flows in total for *specified application*

Mode

Wireless

Syntax

`where the user will be using` *`operator number qos-direction qos-status`* `flows in total for` *`app-name`*

Parameters

operator

One of the following:

- **greater than or equal to**

- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

qos-status

One of the following:

- **reserved** (default)
- **committed**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

app-name

Names of an application. The application must exist in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the User's Tier *downstream* bandwidth limit is between # bps and # bps

Mode

Wireline

Syntax

`where the User's Tier` *`qos-direction`* `bandwidth limit is between` *`bandwidth`* `bps and` *`bandwidth`* `bps`

Parameters

qos-direction

One of the following:

- **upsteam**
- **downsteam** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the appropriate *CMP User's Guide* for information on tiers.

Example

```
where the User's Tier downstream bandwidth limit is between 2M bps and 25M bps
```

where the User's Tier *downstream* bandwidth limit is *greater than #* bps

Mode

Wireline

Syntax

`where the User's Tier` *`qos-direction`* `bandwidth limit is` *`operator bandwidth`* `bps`

Parameters

qos-direction

One of the following:

- **upsteam**
- **downsteam** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the appropriate *CMP User's Guide* for information on tiers.

Example

```
where the User's Tier downstream bandwidth limit is less than or equal to 25M
bps
```

where the User's Tier *upstream* bandwidth limit is *greater than #* bps

Mode

Cable, Wireless

Syntax

```
where the User's Tier qos-direction bandwidth limit is operator bandwidth
bps
```

Parameters

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

The default for this condition is **greater than**

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the appropriate *CMP User's Guide* for information on tiers.

Example

```
where the User's Tier downstream bandwidth limit is less than or equal to 25M
bps
```

where the User's Tier *upstream* bandwidth limit is between # bps and # bps

Mode

Cable, Wireless

Syntax

```
where the User's Tier qos-direction bandwidth limit is between bandwidth
bps and bandwidth bps
```

Parameters

qos-direction

One of the following:

- **upsteam** (default)
- **downsteam**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the appropriate *CMP User's Guide* for information on tiers.

Example

```
where the User's Tier downstream bandwidth limit is between 2M bps and 25M bps
```

Policy SDP Properties Conditions

Session Description Protocol (SDP) properties conditions identify any specific SDP attributes and evaluate their value. This includes setting proper bandwidth values on related PCC rules. The following conditions are available.

where the *local* codec data is an *offer*

Mode

Wireless

Syntax

`where the sdp_capabilities codec data is an codec-type`

Parameters

sdp_capabilities

Specifies where to search for the SDP property.

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

codec-type

Specifies the Codec type. The options are:

- **offer** (default)
- **answer**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Checks the Codec type (offer or answer) for a subscribers device (remote, local or both).

where the *local specified SDP property exists*

Mode

Wireless

Syntax

`where the sdp_capabilities SDP property accessibility`

Parameters

sdp_capabilities

Specifies where to search for the SDP property.

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

SDP property

A comma delimeted list of SDP properties. Specify the SDP properties using one of the following methods:

- Generic descriptor

  `sdp.[option]`

  Where:

  option Is any name (for example, i) or any keyword (for example, a=ptime)

  Examples using an SDP generic descriptor:

  - `where the common sdp.[a] exists`
  - `where the remote sdp.[a=ptime] exists`
  - `where the common sdp.[gd] exists`

- Media descriptor

  `sdp.[m.option]`

  Where:

  option
  - fmt
  - port
  - numberofports
  - media
  - proto

  Examples using an SDP media descriptor:

  - `where the local sdp.[m] exists`

- rtpmap

  `sdp.[codec-name(codec-name).rtpmap.OPTION]`

  Where:

  codec-name Specifies a codec name.

  option
  - payloadtype
  - clockrate
  - encodingparameters

  Examples using rtpmap:

  - `where the remote sdp.[ codec-name(AMR-WB).rtpmap] exists`

- fmtp

`sdp.[codec-name(codec-name).fmtp.OPTIONS]`

Where:

codec-name	Specifies a codec name.
option	• fmt • profile-level-id • mode-set • packetization-mode • Any other parameter to be conveyed

Examples using fmtp:

- `where the common sdp.[codec-name(AMR-WB).fmtp.fmt] exists`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Checks for the existence or non-existence of any SDP property.

where the *local specified SDP property* is numerically *equal to value*

Mode

Wireless

Syntax

`where the sdp_capabilities sdp_capabilities is numerically operator value`

Parameters

sdp_capabilities

Specifies where to search for the SDP property.

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

SDP property

A comma delimeted list of SDP properties. Specify the SDP properties using one of the following methods:

- **Generic descriptor**

Syntax: `sdp.[option]`

Where:

option	Is any name (for example, i) or any keyword (for example, a=ptime)

Examples using an SDP generic descriptor:

- `where the common sdp.[a=ptime] is numerically equal to 20`
- `where the common sdp.[f=hello] is numerically equal to 20`

- **Media descriptor**

  Syntax: `sdp.[m.option]`

  Where:

option	• fmt • port • numberofports • media • proto

  Example using an SDP media descriptor:

  - `where the local sdp.[m.numberofports] is numerically equal to 2`

- **rtpmap**

  Syntax: `sdp.[codec-name(codec-name).rtpmap.OPTION]`

  Where:

codec-name	Specifies a codec name.
option	• payloadtype • clockrate • encodingparameters

  Examples using rtpmap:

  - `where the local sdp.[codec-name(AMR-WB).rtpmap.clockrate] is numerically less than or equal to 16000`

- **fmtp**

  Syntax: `sdp.[codec-name(codec-name).fmtp.OPTIONS]`

  Where:

codec-name	Specifies a codec name.
option	• fmt • profile-level-id • mode-set • packetization-mode • Any other parameter to be conveyed

Example using fmtp:

- `where the local sdp.[codec-name(AMR-WB).fmtp.mode-set] is numerically less than or equal to 4`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

For this condition the default is **equal to**.

value

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Compares a numerical SDP property value against a specified number.

where the *local specified SDP property matches one of value(s)*

Mode

Wireless

Syntax

`where the` *`sdp_capabilities SDP property matches-op value-list`*

Parameters

sdp_capabilities

Specifies where to search for the SDP property.

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

SDP property

A comma delimeted list of SDP properties. Specify the SDP properties using one of the following methods:

- **Generic descriptor**

  Syntax: `sdp.[option]`

  Where:

option	Is any name (for example, i) or any keyword (for example, a=ptime)

  Examples using an SDP generic descriptor:

  - `where the local sdp.[i] matches one of *recvonly*`
  - `where the common sdp.[a=ptime] matches one of 20`
  - `where the common sdp.[a] matches one of ptime: 20`
  - `where the common sdp.[u] matches one of http://www.oracle.com:8080/hr/one.htm`
  - `where the common sdp.[u=http://www.oracle.com] matches one of 8080/hr/one.htm`
  - `where the common sdp.[u=http] matches one of //www.oracle.com:8080/hr/one.htm`
  - `where the remote sdp.[xy] matches one of z`
  - `where the remote sdp.[xy=z] matches one of 80`

- **Media descriptor**

  Syntax: `sdp.[m.option]`

  Where:

option	• fmt • port • numberofports • media • proto

  Examples using an SDP media descriptor:

  - `where the common sdp.[m.fmt] matches one of 102`
  - `where the common sdp.[m.port] does not match any of 41000,41002`
  - `where the remote sdp.[m.media] matches one of audio,video`
  - `where the local sdp.[m.proto] matches one of RTP/AVP`

- **rtpmap**

  Syntax: `sdp.[codec-name(codec-name).rtpmap.OPTION]`

  Where:

codec-name	Specifies a codec name.
option	• payloadtype • clockrate • encodingparameters

  Examples using rtpmap:

- `where the common sdp.[ codec-name(AMR-WB).rtpmap] matches one of 104 AMR-WB/160000`
- `where the common sdp.[ codec-name(AMR-WB).rtpmap.encodingparameters] matches one of 2`
- `where the common sdp.[ codec-name(AMR-WB).rtpmap.payloadtype] matches one of 104,102`

- **fmtp**

  Syntax: `sdp.[codec-name(`*`codec-name`*`).fmtp.`*`OPTIONS`*`]`

  Where:

codec-name	Specifies a codec name.
option	• fmt • profile-level-id • mode-set • packetization-mode • Any other parameter to be conveyed

  Examples using fmtp:

  - `where the common sdp.[codec-name(AMR-WB).fmtp.fmt] matches one of 104,102`
  - `where the common sdp.[codec-name(AMR-WB).fmtp.mode-set] matches one of 2,4`
  - `where the commonsdp.[codec-name(H264).fmtp.profile-level-id] matches one of42e00c`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Checks the Codec type (offer or answer) for a subscribers device (remote, local or both) for specific values.

State Variables Conditions

Note: State Variables replace User State Conditions. When upgrading from an earlier release that used State Variable, the properties for User State Conditions are automatically mapped to the corresponding State Variable values. Therefore, the **subscriber** property is mapped to the **subscriber remote** state variable and the **pool** property is mapped to the **pool** state variable.

State Variables are set within a policy action to be used at a later time during policy rule execution (in either conditions or actions). The names of these variables are not predefined and are determined at the time of creation. State variables have a scope which determines how long the value persists after it is set. The scopes are:

- **Subscriber Remote State Variable** — This state variable exists remotely in an SPR as long as the subscriber exists in the SPR. Using this variable requires that an SPR/HSS be configured that is capable of storing this variable.
- **Pool State Variable** — This variable is associated with a quota pool (of multiple subscribers). This variable is stored remotely in an SPR and exists as long as the pool exists in the SPR. Using this variable requires that an SPR/HSS be configured that is capable of storing this variable.
- **Subscriber Local State Variables**— This variable exists locally on the MPE and has a value as long as the associated subscriber has at least one session on that MPE. After the last session is terminated these variables no longer have value and will no longer be available for use in policies.
- **Session State Variables**— This variable has a value that is saved as long as the session the variable is associated with is still valid. After the session is terminated, this variable no longer has value and will no longer be available for use in policies.
- **Policy Evaluation State Variables**— This variable are available for the lifetime of a policy evaluation cycle (the process of evaluating all the policies for a single equest or context)

where the *scope* state variable *name + 0 days* rounded *up* with *same* granularity is *after now* using *configured local time*

Mode

Wireless

Syntax

```
where the scope state variable variable-name direction duration granularity1
rounded rounding with granularity2 granularity is datetime-compare datetime
using time-zone
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.

- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

direction

One of the following, indicating future or past:

- **+** (default)
- **-**

duration

Positive integer.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

granularity1

The offset is expressed in this granularity

- **days** (default)
- **months**
- **hours**
- **minutes**

rounding

One of the following, indicating rounding up or down:

- **up** (default)
- **down**

granularity2

The calculated date-time is expressed in this granularity:

- **same** (default) — Indicates that the value for *granularity1* is used.
- **months**
- **days**
- **hours**
- **minutes**

datetime-compare

One of the following:

- **after** (default)
- **before**
- **at or before**
- **at or after**

datetime

One of the following:

- The local date-time **now** (default)
- A policy variable
- A date-time in the format: `yyyy-mm-ddThh:mm:ss+UTCoffset`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is evaluated for a state variable based 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.

where the *scope* state variable *name exists*

Mode

Wireless

Syntax

`where the scope state variable variable-name accessibility`

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Triggers a policy based on whether or not the specified variable exists within the scope.

where the *scope* state variable *name* is *in* the current billing cycle using *configured local time*

Mode

Wireless

Syntax

```
where the scope state variable variable-name is comparison-op the current
billing cycle using time-zone
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

comparison-op

One of the following:

- **in** (default)
- **not in**
- **before**

- **after**

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is evaluated based on the comparison between the timestamp value of the specified state variable 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.

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.

where the *scope* state variable *name* is numerically *equal to value*

Mode

Wireless

Syntax

`where the` *`scope`* `state variable` *`variable-name`* `is numerically` *`operator value`*

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

For this condition the default is **equal to**.

value

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on a numerical comparison between the state variable value and a specified value.

where the *scope* state variable *name is* the current mobile country code

Mode

Wireless

Syntax

```
where the scope state variable variable-name operator-binary the current
mobile country code
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is evaluated based on the comparison between the value of the state variable and the current mobile country code.

where the *scope* state variable *name matches one of `value(s)`*

Mode

Wireless

Syntax

`where the scope state variable variable-name matches-op `match-list``

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the specified state variable value matches a list of specified values (based on matching wildcard patterns).

where the *scope* state variable *name* value *is* contained in Match Lists *selected lists*

Mode

Wireless

Syntax

`where the scope state variable variable-name value operator-binary contained in Match Lists match-list`

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the specified state variable value matches a list of specified values (based on matching wildcard patterns).

Policy Context Property Conditions

Policy Context Properties are user-defined name/value string pairs that can be created from policy actions and evaluated from policy conditions. By using policy context properties, one policy can influence the execution of other policies. Policy context properties exist across multiple policy executions on the same request, but are not persistent across requests.

where the policy context property *name exists*

Mode

Cable, Wireless, Wireline

Syntax

`where the policy context property` *`property-name accessibility`*

Parameters

property-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Triggers a policy based on whether or not the specified policy context property exists.

where the policy context property *name* is numerically *equal to value*

Mode

Cable, Wireless, Wireline

Syntax

```
where the policy context property property-name is numerically operator
value
```

Parameters

property-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

For this condition the default is **equal to**.

value

String.

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.

Example

The following policy will release the session if the DATA_LIM for the subscriber is changed from non-zero to zero:

```
where the reauth is triggered by subscriber profile update with
notification type SUBSCRIBER_POOL
And where at least one of pool fields DATA_LIM have been updated
And where the policy context property {Previous.Pool.DATA_LIM} is
numerically greater than 0
release the session
accept message
```

where the policy context property *name matches one of `value(s)`*

Mode

Cable, Wireless, Wireline

Syntax

`where the policy context property` *`property-name matches-op `match-list``*

Parameters

property-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the specified policy context property value matches a list of specified values (based on matching wildcard patterns).

where the policy context property *name1 matches one of name2*

Mode

Wireless

Syntax

`where the policy context property` *`property-name matches-op property-name`*

Parameters

property-name

String.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

Description

Triggers a policy based on whether a policy context property value matches one of a set of specified policy context property values.

Policy Method Conditions

Policy Method conditions are related to the methods used to process the policy.

where evaluate the customized method *specified name(s)*

Mode

Wireless

Syntax

`where evaluate the customized method specified name(s)`

Parameters

specified name(s)

The name of one or more policy methods.

Description

Uses customized policy methods to evaluate policies.

Time-of-Day Conditions

Time-of-Day conditions are related to the time at which the policy rules are being executed.

where the current time *is* between *start time* and *end time* using *configured local time*

Mode

Cable, Wireless, Wireline

Syntax

`where the current time operator-binary between time-of-day and time-of-day using time-zone`

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

time-of-day

A time, in the format of *hh*:*mm*, where *hh* is a number in the range from 0 to 23.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where the current time *is* within the *specified* time periods

Mode

Wireless

Syntax

`where the current time` *`operator-binary`* `within the` *`time-period`* `time periods`

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

time-period

Names of one or more time periods that are defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on the time period.

where today is a week day using *configured local time*

Mode

Cable, Wireless, Wireline

Syntax

`where today is a week day using` *`time-zone`*

Parameters

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where today is a weekend day using *configured local time*

Mode

Cable, Wireless

Syntax

`where today is a weekend day using` *`time-zone`*

Parameters

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

where today *is* the *specified numbers* th days of *Any Month* in*natural order* using *configured local time*

Mode

Wireless

Syntax

```
where today operator-binary the value-list th days of month in order using
time-zone
```

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

month

One or more of the following:

- **January**
- **February**
- **March**
- **April**
- **May**
- **June**
- **July**
- **August**
- **September**
- **October**
- **November**
- **December**

order

Specifies the order to evaluate the value list. The options are:

- **natural order**
- **reverse order**

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on a day in a month. 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

The following conditions, if evaluated as true, will trigger a policy:

```
   where today is the 1,2,3,4 th days of March,April,May in natural order
using USER LOCAL TIME
```

where today *is day* using *configured local time*

Mode

Cable, Wireless

Syntax

`where today` *`operator-binary day-of-week`* `using` *`time-zone`*

Parameters

operator-binary

One of the following:

- **is** (default)
- **is not**

day-of-week

One of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Policy Counter Conditions

Policy Counter conditions are related to policy counters stored in online charging servers (OCSs).

where a *current* status *exists* for Policy Counter IDs *select names*

Mode

Wireless

Syntax

`where a` *`status`* `status` *`accessibility`* `for Policy Counter IDs` *`counter -name`*

Parameters

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

accessibility

One of the following:

- **exists** (default)
- **does not exist**

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the specified policy counter ID property exists or does not exist in the selected counter ID status. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Filter-Ids for Policy Counter ID *select name current* status match one or more of *Filter-Ids to match*

Mode

Wireless

Syntax

`where the Filter-Ids for Policy Counter ID` *`counter -name status`* `status match one or more of` *`match-list`*

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the specified policy counter ID property matches the selected counter ID status and filter expression(s). See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Final-Unit-Action for Policy Counter IDs *select names current* status matches *Final-Unit-Action to match*

Mode

Wireless

Syntax

`where the Final-Unit-Action for Policy Counter IDs` *`counter -name status`*
`status matches` *`action`*

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

action

The action to match. One of the following:

- **ACTION_TERMINATE** (default)
- **ACTION_REDIRECT**
- **ACTION_RESTRICT_ACCESS**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Tests whether the Policy Counter ID contains a Final Unit Action (FUA) attribute-value pair (AVP) matching the specified FUA. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Final-Unit-Indication AVP for Policy Counter IDs *select names current* status *exists*

Mode

Wireless

Syntax

`where the Final-Unit-Indication AVP for Policy Counter IDs` *`counter -name status`* `status` *`accessibility`*

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.

- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Determines whether the Final-Unit-Indication AVP for the Policy Counter ID is accessible. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Policy Counter ID *select name current* status *is* contained in Match Lists *select lists*

Mode

Wireless

Syntax

```
where the Policy Counter ID counter -name status status operator-binary
contained in Match Lists match-list
```

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

operator-binary

One of the following:

- **is** (default)
- **is not**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Selects protocol messages based on whether the status of a policy counter ID matches, or does 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 Policy Counter Identifiers* for information on policy counter IDs. See *Managing Match Lists* for information about defining match lists.

where the Policy Counter ID *select name current* status is numerically *equal to value*

Mode

Wireless

Syntax

`where the policy context property` *`counter -name status`* `status is numerically` *`operator value`*

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**

- **not equal to**

For this condition the default is **equal to**.

value

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on a numerical comparison between the specified policy counter ID status value and a specified value. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Policy Counter ID *select name current* status *matches one of specified value(s)*

Mode

Wireless

Syntax

`where the Policy Counter ID counter -name status status matches-op value-list`

Parameters

counter -name

- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on whether the status of a specified policy counter ID value matches, or does not match, a list of specified values (based on matching wildcard patterns). See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Policy Counter ID *select name current* status *is* between *value* and *value*

Mode

Wireless

Syntax

`where the policy counter ID` *`counter -name status`*`status` *`operator-binary`* `between` *`value`* `and` *`value`*

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

status

One of the following:

- **pending** — Accesses the pending status closest to the current time.
- **current** — Accesses the current status (default).

operator-binary

One of the following:

- **is** (default)
- **is not**

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).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy based on a numerical comparison between the specified policy counter ID value and a pair of specified values, and whether the ID is or is not within the range defined by the two values. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Policy Counter IDs *select names exists*

Mode

Wireless

Syntax

`where the Policy Counter IDs counter -name accessibility`

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Triggers a policy based on whether or not the specified policy counter ID property exists or does not exist. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Policy Counter ID *select name* status *is* equal to default status

Mode

Wireless

Syntax

`where the Policy Counter ID counter -name status operator-binary equal to default status`

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

Description

Selects protocol messages based on whether the policy counter ID status is, or is not, equal to the default status defined for the policy counter ID. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

where the Sy Session *exists*

Mode

Wireless

Syntax

`where the Sy Session` *`accessibility`*

Parameters

accessibility

One of the following:

- **exists** (default)
- **does not exist**

Description

Determines whether the Sy Session is accessible. See *Managing Policy Counter Identifiers* for information on policy counter IDs.

Notification Conditions

Notification conditions are related to notifications from Sh and Sy data sources.

The mandatory action **reject message** is not applicable to policies that contain notification conditions. It does not reject the notification. Instead, use the mandatory action **accept message**.

The following optional actions are applicable to policies that contain notification conditions. Optional actions not listed here are not applicable to work with such policies.

Note: There is no validation done when other policy actions are added. During policy execution they will have no effect.

- clear alarm with severity `*severity level*`, id `*unique alarm identifier*` and message `*message text*`
- disable forwarding to next hop gateway
- disable VLAN tagging
- enable forwarding to next hop gateway with address *none*
- enable VLAN tagging with Id specified

- evaluate policy group *select policy group*
- evaluate policy *select policy*
- Re-authorize all credit control sessions associated with *select scope*
- Re-authorize all PCEF/TDF sessions associated with *select scope*
- Release all credit control sessions associated with *select scope*
- Release all PCEF/TDF sessions associated with *select scope*
- release the session
- remove all policy context properties
- remove all the *scope* state variables and save *always*
- remove policy context property *name*
- remove the *scope* state variable *name* and save *always*
- send http *POST* notification to *select notification destination* with headers *headers* and content *content*
- send http *POST* notification to url *URL* with headers *headers* and content *content*
- send notification to syslog with `*message text*` and severity `*severity level*`
- send notification to trace log with `*message text*` and severity `*severity level*`
- 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*`.
- 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*`.
- send SMS `*specified*` to user on their Billing Day. Request delivery receipt `*default*`.
- send SMS `*specified*` to user. Request delivery receipt `*default*`.
- send SMTP message with the following text/plain content.
- set alarm with severity `*severity level*`, id `*unique alarm identifier*` and message `*message text*`
- set policy context property name to *value*

where notification from Sh datasource is received for *User Profile*

Mode

Wireless

Syntax

```
where notification from Sh datasource is received for object-type
```

Parameters

object-type

One or more of the following:

- **User Profile**
- **Pool Profile**
- **Dynamic quota Profile**
- **Pool Dynamic quota Profile**
- **Quota Usage**
- **User state**
- **Pool Quota Usage**
- **Pool State**
- **Service**

- **User Session Policy**
- **User Location**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is only evaluated when notification is received from one of the specified object types in an Sh data source. The mandatory action **reject message** is not applicable to this condition.

Note: This condition generates an RAR/RAA message pair for each notification from each selected object type. Using this condition to generate an action for all object types can significantly impact performance. You should generally process only provisioning changes or quota resets.

Examples

The following example re-authorizes user sessions for all provisioning change notification and when quota usage is reset to zero:

```
where the user is using equal to 100 percent of total volume for plan1
quota
And where notification from Sh datasource is received for Quota Usage
Or where notification from Sh datasource is received for User Profile,Pool
 Profile,Dynamic quota Profile,Pool Dynamic quota Profile
re-authorize all PCEF/TDF sessions associated with User
continue processing message
```

If an MPE device is configured to process all notifications (see the *CMP Wireless User's Guide*), but you want to use the functions of a previous releases, you must write a policy rule similar to the following:

```
where notification from Sh datasource is received for User Profile,Pool
Profile,Dynamic quota Profile,Pool Dynamic quota Profile
re-authorize all PCEF/TDF sessions associated with User
continue processing message
```

The following example issues an updated RADIUS CoA message when a Profile Notification Request (PNR) message is received from an SPR system:

```
where notification from Sh datasource is received for Quota Usage
send CoA with CoA10-24
continue processing message
```

where notification from Sy datasource is received for Policy Counter IDs *select names*

Mode

Wireless

Syntax

```
where notification from Sy datasource is received for Policy Counter IDs
counter -name
```

Parameters
counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is evaluated when a notification for one or more policy counter IDs is received from an Sy data source.

Note: The mandatory action **reject message** is not applicable to this condition.

Example

```
And
    where notification from Sy datasource is received for Policy Counter
 IDs X,Y,Z
    where the Policy Counter ID select name status is modified from one
of specified values
    where the Policy Counter ID select name status matches one of specified
 values
Re-authorize all PCEF/TDF sessions associated with select scope
continue processing message
```

RADIUS Conditions

RADIUS conditions are related to RADIUS Change of Authorization (CoA) requests.

where the BNG COA destination port *is port number*

Mode

Wireless

Syntax

`where the BNG COA destination port` *`operator-binary port`*

Parameters
operator-binary

One of the following:

- **is** (default)
- **is not**

port

Enter a port number.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers a policy that is evaluated depending on the value of the destination port number of a broadband network gateway associated with the request.

where the RADIUS accounting request is *RADIUS Accounting-Start*

Mode

Wireless

Syntax

```
where the RADIUS accounting request is radius-request
```

Parameters

radius-request

One or more of the following:

- **Accounting-Start** (default) — RADIUS Accounting-Start message
- **Accounting-Stop** — RADIUS Accounting-Stop message
- **Interim-Update** — RADIUS Interim-Update message
- **Accounting-On** — RADIUS Accounting-On message
- **Accounting-Off** — RADIUS Accounting-Off message

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Evaluated as true when the RADIUS message has a code field value that matches one of the specified message types.

An Accounting-Start message is interpreted as a request to begin a session; an Accounting-Stop message is interpreted as a request to end a session. An Interim-Update message is interpreted as a keep-alive message. An Accounting-On message is interpreted as meaning the BNG device has restarted, while an Accounting-Off message is interpreted as meaning the BNG device is about to restart; in both cases the MPE device removes all the sessions' state information and any previously installed services, and marks the sessions as stale, to be removed during the next session cleanup cycle.

Example

```
where the RADIUS accounting request is Accounting-Start
send CoA with CoA Template
```

where the RADIUS request *contains* a TLV / VSA of *name or ID*

Mode

Wireless

Syntax

`where the RADIUS request containment a TLV / VSA of vsa`

Parameters

containment

One of the following:

- **contains one of** (default)
- **does not contain any of**

vsa

A VSA or TLV name, in the format *name:vendor_id* or *code*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Evaluates whether the RADIUS request message contains, or does not contain, the specified vendor-specific attribute (VSA) or type-length-value (TLV). You can specify either a standard TLV or VSA or a custom TLV or VSA number defined in the RADIUS dictionary.

where the RADIUS request contains TLV / VSA *name or ID* whose value *is* contained in Match List *List of TLV / VSA value as string*

Mode

Wireless

Syntax

```
where the RADIUS request contains TLV / VSA vsa whose value operator-binary
contained in Match List match-list
```

Parameters

vsa

A TLV or VSA name, in the format *name:vendor_id* or *code*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator-binary

One of the following:

- **is** (default)
- **is not**

match-list

A comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Evaluates whether the specified type-length-value (TLV) or vendor-specific attribute (VSA) in a RADIUS request message is contained, or is not contained, in a match list of values. The values are compared as strings. You can specify either a standard TLV or VSA or a custom TLV or VSA number defined in the RADIUS dictionary.

where the RADIUS request contains TLV / VSA *name or ID* whose value is numerically *equal to number*

Mode

Wireless

Syntax

`where the RADIUS request contains TLV / VSA` *`vsa`* `whose value is numerically` *`operator number`*

Parameters

vsa

A TLV or VSA name, in the format *name*:*vendor_id* or *code*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

operator

One of the following:

- **greater than or equal to**
- **greater than**
- **less than or equal to**
- **less than**
- **equal to**
- **not equal to**

For this condition the default is **equal to**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Compares the specified type-length-value (TLV) or vendor-specific attribute (VSA) in a RADIUS request message with a numeric value. The values are compared as numbers. You can specify either a standard TLV or VSA or a custom TLV or VSA number defined in the RADIUS dictionary.

where the RADIUS request contains TLV / VSA *name or ID* whose value *matches one of TLV / VSA value as string*

Mode

Wireless

Syntax

`where the RADIUS request contains TLV / VSA` *`vsa`* `whose value` *`matches-op value-list`*

Parameters

vsa

A TLV or VSA name, in the format *name*:*vendor_id* or *code*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

matches-op

One of the following:

- **matches one of** (default)
- **does not match any of**

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Evaluates whether the RADIUS request message contains, or does not contain, the specified type-length-value (TLV) or vendor-specific attribute (VSA) by comparing the name or ID against a list of values. The values are compared as strings. You can specify either a standard TLV or VSA or a custom TLV or VSA number defined in the RADIUS dictionary.

where the RADIUS request contains VSAs from *vendor*

Mode

Wireless

Syntax

`where the RADIUS request contains VSAs from` *`vendor-list`*

Parameters

vendor-list

One of the following:

- **IETF**
- **3GPP**
- **3GPP2**
- **Camiant**
- **Cisco**
- **Cisco-BBSM**
- **Cisco-VPN3000**
- **Cisco-VPN5000**
- **Juniper**
- **Juniper-M-Series**
- Any defined custom vendors appear at the end of the list; for more information see *Managing Custom Vendors*

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Evaluates as true if the RADIUS request message contains a type-length-value (TLV) or vendor-specific attribute (VSA) from the specified vendor. The vendor value can be either a standard or custom value defined in the RADIUS dictionary.

Note: The base RADIUS TLVs are considered as being from IETF.

Actions 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 policy-processing actions:

Mandatory actions	This action defines what happens 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	These are actions executed when the conditions in the policy rule have been met. When you are creating a policy rule in the policy wizard, this is a list of actions that you can add to your policy rule. You can select none, one, several, or up to 40 of these optional actions per rule. However, each action is limited, so that it can be executed only once per policy rule.

In the same way that you can customize conditions by editing parameter values, many of these actions can be customized by specifying parameter values as well.

Actions are listed in alphabetical order. Actions also are affected by the current mode. Therefore, some of the actions documented 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.

accept message

Mode

Cable, Wireless, Wireline

Syntax

```
accept message
```

Parameters

None

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.

break from policy level

Mode

Cable, Wireless

Syntax

```
break from policy level
```

Parameters

None

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.

continue processing message

Mode

Cable, Wireless, Wireline

Syntax

```
continue processing message
```

Parameters

None

Description

After executing the current policy rule, the Policy Engine continues with the next policy rule.

reject message

Mode

Cable, Wireless, Wireline

Syntax

```
reject message
```

Parameters

None

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.

reject message with Experimental-Result-Code `*number*` and Vendor-ID `*number*`

Mode

Wireless

Syntax

`reject message with Experimental-Result-Code` `*number*` `and Vendor-ID` `*number*`

Parameters

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

After executing the current policy rule, the message is rejected, including the specified experimental result code and vendor ID AVPs in the AAA message and the trace log. This action supports sponsored data connectivity.

Example

The following conditions, if evaluated as true, accept sponsored data connectivity, but otherwise reject the message with Experimental-Result-Code 5067 (“UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY”) and Vendor-ID 10415 (3GPP):

```
Or
    where the Sponsor-Identity matches one of nba
    And where the Application-Service-Provider-Identity matches one of
netmovies
    And where the AF-Application-ID matches one of streaming,voip
    And where the application is one of af-10.24
    continue processing message

reject message with Experimental-Result-Code `5067` and Vendor-ID `10415`
```

reject message with code `*number*`

Mode

Wireless

Syntax

`reject message with code` `*number*`

Parameters

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

After executing the current policy rule, the MPE device terminates all policy-rule processing and rejects the current protocol message with a specified error code. If the input number is an invalid error code, then the message returns DIAMETER_AUTHORIZATION_REJECTED(5003).

reject message with code `*number*`

Mode

Wireline

Syntax

```
reject message with code `number`
```

Parameters

number
qos-direction

A numeric value.

This value is an integer from 1–2000000000.

Description

After executing the current policy rule, the generated code is propagated back to the VoD server.

skip to next device

Mode

Cable, Wireless

Syntax

```
skip to next device
```

Parameters

None

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.

skip to next flow

Mode

Cable, Wireless

Syntax

```
skip to next flow
```

Parameters

None

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 Policy-Processing Actions

The following optional policy-processing actions are available.

accumulate reported quota usage of *selected* to *selected*

Mode

Wireless

Syntax

`accumulate reported quota usage of` *`select-quota1`* `to` *`select-qutota2`*

Parameters

select-quota1

Name of a quota.

select-quota2

Name of a different quota.

Description

Transfers the quota usage report for the quota to the specified quota. See *Managing Quotas* for information on quotas.

add custom grouped AVP *name* and send *always*

Mode

Wireless

Syntax

`add custom grouped AVP` *`name`* `and send` *`send-mode`*

Parameters

name

Select an existing grouped third-party AVP Name and Vender ID, or an AVP name from an existing policy table.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

send-mode

One of the following:

- **always** (default)
- **unless rejected**
- **if rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

add the APP Detection Flow *select scope* to *specified* PCC rules

Mode

Wireless

Syntax

`add the APP Detection Flow flow-type to value-list PCC rules`

Parameters

flow-type

Select one of the following options:

- **Flow-information** (default)
- **TDF-Application-Instance-Identifier**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This action binds the specified TDF-Application-Identifier and TDF-Application-Instance-Identifier information of the current application detection flow to the Policy and Charging Control (PCC) rules, so that the MPE device can find the mapping. The specified PCC rules must be installed in this Credit Control Answer (CCA), or the PCC rules are ignored and not installed.

When **Flow-Information** is specified, the TDF-Application-Identifier and TDF-Application-Instance-Identifier information of the current application detection flow is recorded in the MPE device that is associated with the PCC rules. During this process, the MPE device removes related rules while reporting Application-Detection-Information with TDF-Application-Identifier and TDF-Application-Instance-Identifier for an application stop . The Flow-Information is added to the specified PCC rules if select scope is Flow-Information. And do not add duplicated Flow.

When **TDF-Application-Instance-Identifier** is specified, the TDF-Application-Identifier and TDF-Application-Instance-Identifier information of the current application detection flow is recorded

in the MPEdevice that is associated with the PCC rules. During this process, the MPE device removes related rules while reporting Application-Detection-Information with TDF-Application-Identifier and TDF-Application-Instance-Identifier for an application stop.

Advanced: set values for QoS and Charging parameters to *specified value*

Mode

Cable, Wireless

Syntax

`Advanced: set values for QoS and Charging parameters to` *`profile-param`*

Parameters

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 policy wizard includes a customized dialog to help you in the selection of parameters and valid values for them. For the specific meaning of the fields it may be necessary to consult protocol specifications.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

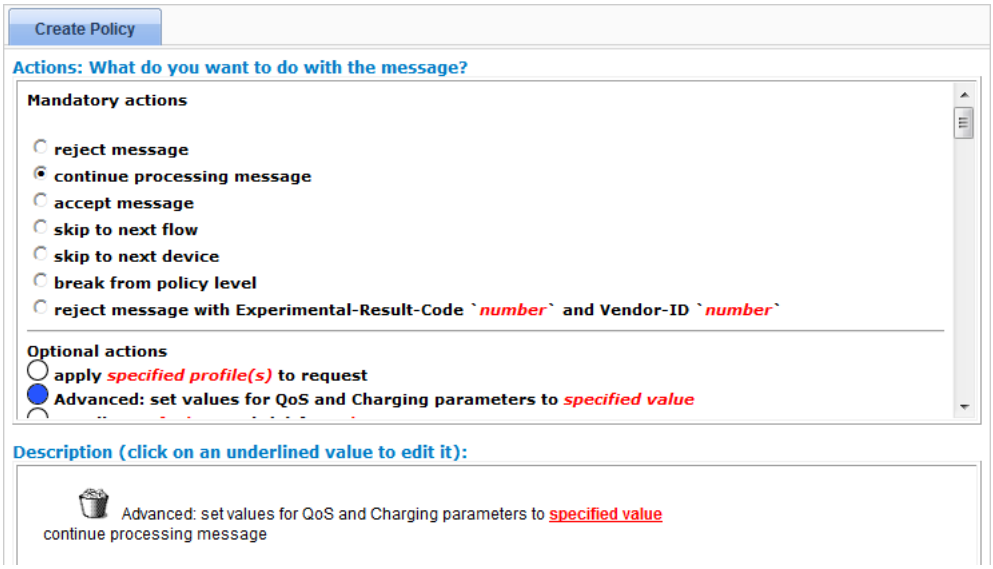
Overwrites the corresponding settings in the current protocol message. If you specify settings that are not relevant in the current protocol message, they are ignored.

Example

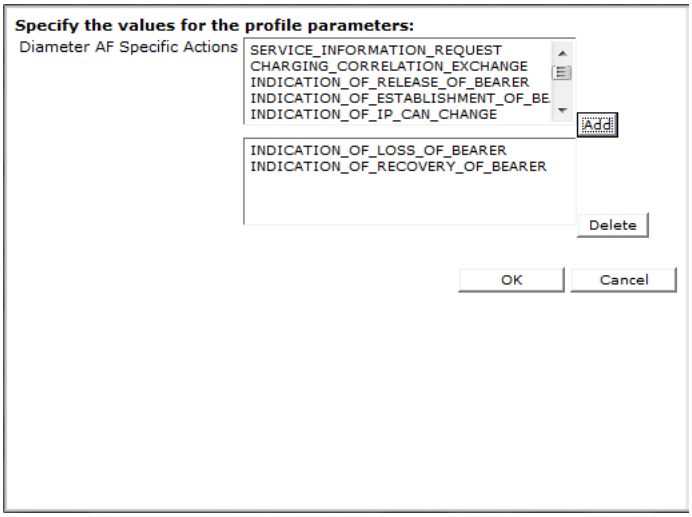
This is the sequence of steps within the policy wizard needed to specify the following action:

```
Advanced: set values for QoS and Charging Parameters to Diameter AF Specific
ActionsINDICATION_OF_LOSS OF BEARER,INDICATION_OF_RECOVERY OF BEARER
```

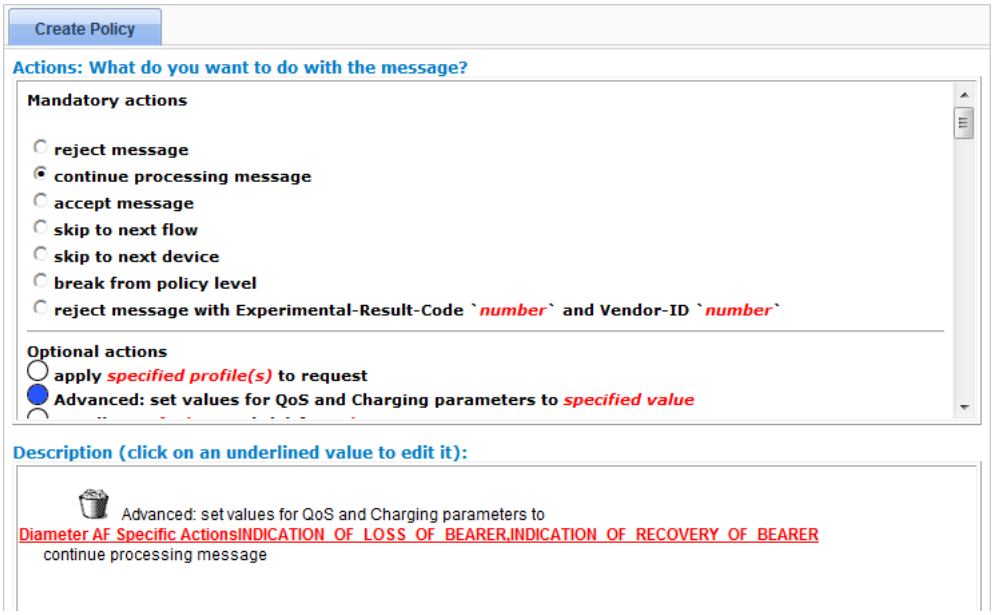
1. In the Actions step, select the optional action **Advanced: set values for QoS and Charging Parameters to** *specified value*. The action is displayed in the Description section of the page.



2. In the Description section of the page, click on *specified value*. The **Profile Parameter** window opens.
3. In the **Profile Parameter** window, select **Diameter AF Specific Actions**, and click **OK**. You are prompted, `Specify the values for the profile parameters:`.
4. Use Shift-click or Ctrl-click to select **INDICATION_OF_LOSS_OF_BEARER** and **INDICATION_OF_RECOVERY_OF_BEARER**, and click **Add** to move the values to the list of selected values.



5. Click **OK**. The action is defined.



apply Roaming Profile *name*

Mode

Wireless

Syntax

`apply Roaming Profile` *`roaming-profile`*

Parameters

roaming-profile

The name of the Roaming Profile. For more information on roaming profiles, see *Managing Roaming Profiles*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This parameter allows you to apply a specific roaming profile.

apply *specified profile(s)* to all flows in the request

Mode

Cable, Wireless

Syntax

`apply` *`traffic-profile`* `to all flows in the request`

Parameters

traffic-profile

One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This parameter allows you to choose different traffic profiles to apply to different types of calls.

apply *specified profiles* to flows whose media type matches one of *specified types*

Mode

Wireless

Syntax

`apply` *`traffic-profile`* `to flows whose media type matches one of` *`media-type`*

Parameters

traffic-profile

One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

media-type

One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**
- **Message**
- **Other**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Applies one or more traffic profiles to one or more flows of the specified types. Overwrites the corresponding settings in the protocol messages of the specified flows. If multiple traffic profiles are selected they are applied in the order in which they are specified. If a traffic profile contains settings that are not relevant in the current protocol message, they are ignored. The second parameter lets you apply different traffic profiles to flows of different types.

apply *specified profile(s)* to request

Mode

Cable, Wireless

Syntax

`apply` *`traffic-profile`* `to request`

Parameters

traffic-profile

One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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, they are ignored.

apply *specified profiles* to selected *specified types* flows in the request

Mode

Cable, Wireless

Syntax

apply *traffic-profile* to selected *media-type* flows in the request

Parameters

traffic-profile

One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

media-type

One or more of the following, used to determine the type of media:

- **Audio**
- **Video**
- **Data**
- **Application**
- **Control**
- **Text**

- **Message**
- **Other**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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, they are ignored. The second parameter lets you choose different traffic profiles to apply to different types of calls.

clear alarm with severity `*severity level*`, id `*unique alarm identifier*` and message `*message text*`

Mode

Cable, Wireless

Syntax

```
clear alarm with severity `level`, id `alarm-id` and message `message`
```

Parameters

level

One of the following, used to determine which alarm ID is cleared:

- **Critical** (ID 74000)
- **Major** (ID 74001)
- **Minor** (ID 74002)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the appropriate *CMP User's Guide*.

disable forwarding to next hop gateway

Mode

Wireless

Syntax

disable forwarding to next hop gateway

Parameters

None.

Description

Disables forwarding to the next hop gateway.

disable *monitoring key*

Mode

Wireless

Syntax

disable *mon-key*

Parameters

mon-key

Name(s) of a monitoring key in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

discard next quota usage report in grace period of *select-quota*

Mode

Wireless

Syntax

`discard next quota usage report in grace period of quota-name`

Parameters

quota-name

Name(s) of quota defined in the CMP database.

Description

Discards the next quota usage report for the specified quota. See *Managing Quotas* for information on quotas.

Example

```
where the policy context property ICHGFLAG matches one of 'TYPE:3'
 And where the session granted quota using INT is valid
 discard next quota usage report in grace period of DATA_Plan_NEVER_RESET
break from policy level
```

discard next quota usage report in grace period of *select-quota* using *monitoring-key*

Mode

Wireless

Syntax

`discard next quota usage report in grace period of quota-name using mon-key`

Parameters

quota-name

Name(s) of quota defined in the CMP database.

mon-key

Name(s) of a monitoring key in the CMP database.

Description

Discards the next quota usage report for the specified quota that has the specified monitoring key. See *Managing Quotas* for information on quotas.

Example

```
where the policy context property ICHGFLAG matches one of 'TYPE:3'
 And where the session granted quota using INT is valid
 discard next quota usage report in grace period of DATA_Plan_NEVER_RESET
 using INT
break from policy level
```

enable/disable PRA subscription

Mode

Wireless mode with the 3GPP mode enabled.

Syntax

status `PRA subscription`

Parameters

status

One of the following:

- **enable**
- **disable**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This action enables or disables PRA subscription.

enable event messaging for this request

Mode

Cable

Syntax

`enable event messaging for this request`

Parameters

None

Description

Enables event messaging for the current message, using the default Event Messaging parameters for this MPE device. If there is no EventGenerationInfo object in the current message, a new one is added.

enable subscription for notification of user profile changes

Mode

Wireless

Syntax

```
enable subscription for notification of user profile changes
```

Parameters

None

Description

Causes the MPE device to subscribe to an SPR system for notification of user profile changes.

Note: Within the same MPE device, if subscription to profile updates (that is, Sh:Notify) has occurred (for example, as a result of a policy action), then the MPE device will not resubscribe to update notifications on subsequent triggers (that is, it will not send additional SNR messages to the SPR system).

enable subtracting usage from *select quota* for *monitoring key*

Mode

Wireless

Syntax

enable/disable subtracting usage from *quota-name* for *mon-key*

Parameters

enable/disable

Select one of the following:

- **enable** (default)
- **disable**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

mon-key

Name(s) of a monitoring key in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Allows or disallows subtraction of the usage reported by the specified monitoring key(s) from the specified quota(s). 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
```

establish traffic detection session using the IP-CAN TDF information

Mode

Wireless

Syntax

```
establish traffic detection session using the IP-CAN TDF information
```

Parameters

None

Description

Use this action to establish an Sd session specified in a Gx CCR request with a single TDF device. On 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.

Example

```
where the request is creating a new session
And where the session is an enforcement session
And where the enforcement session is an IP-CAN session
establish traffic detection session using the IP-CAN TDF information
continue processing message
```

establish traffic detection session with *select network element identity*

Mode

Wireless

Syntax

`establish traffic detection session with tdf`

Parameters

tdf

One or more TDF network elements defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

On a IP-CAN session establishment, the policy action will trigger a TSR command that is sent to the selected TDF device(s) to establish an Sd session.

Example

```
where the request is creating a new session
And where the session is an enforcement session
And where the enforcement session is an IP-CAN session
establish traffic detection session with
tdf1.GalacTel.com,tdf2.GalacTel.com
continue processing message
```

evaluate policy group *select policy group*

Mode

Cable, Wireless

Syntax

`evaluate policy group group-name`

Parameters

group-name

Name of a policy group defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

If the conditions evaluates to true, evaluate the rules in a policy group. When you click the **select policy group** parameter, a pop-up window opens so you can select an existing policy group.

evaluate policy *select policy*

Mode

Cable, Wireless

Syntax
evaluate policy *policy-name*

Parameters
policy-name

Name of a policy defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

If the conditions evaluate to true, evaluate a policy. When you click 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.

evaluate the schedule task on *Service*

Mode

Wireless

Syntax
evaluate the schedule task on *Service*

Parameters
service

- **Service** (default)
- **User Session Policy**
- **Billing Day**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

If the conditions evaluate to true, evaluate the task.

Example

```
where notification from Sh datasource is received for Service
And where the user Service 210125012345678901234567890123 01
ServiceStartDateTime prior to notification does not match any of previous
 value
evaluate the schedule task on Service
accept message
```

fetch Policy Counters *default* from OCS

Mode

Wireless

Syntax

`fetch Policy Counters counter-name from OCS`

Parameters

counter-name

Select one or more policy counter IDs defined in the CMP database; or enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Fetches one or more policy counters, by ID, from an online charging server.

grant # bytes for quota

Mode

Wireless

Syntax

`grant number bytes for quota`

Parameters

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Grants a user the specified number of bytes for the requested service. See *Managing Quotas* for information on quotas.

grant # of *select units* for *select quota*

Mode

Wireless

Syntax

```
grant number of unit for quota-name
```

Parameters

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

unit

One of the following:

- **Seconds**
- **Bytes**
- **Service Specific**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the usage threshold to the specified number of units for the selected quota profile(s). See *Managing Quotas* for information on quotas.

Example

```
grant 40000000 of Bytes for DailyVol,MonthlyVol
```

grant # percent in service-specific units for quota

Mode

Wireless

Syntax

```
grant extended-percent percent in service-specific units for quota
```

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Grants a user the specified percentage of the service-specific unit limit for the requested service.

grant # percent in time for quota

Mode

Wireless

Syntax

`grant` *`extended-percent`* `percent in time for quota`

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Grants a user the specified percentage of the initial time limit (in seconds) for the requested service.

grant # percent in volume for quota

Mode

Wireless

Syntax

`grant` *`extended-percent`* `percent in volume for quota`

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Grants a user the specified percentage of the user's volume limit (in bytes) for the requested service.

grant # percent of *select type* for BEST OF *select quota*

Mode

Wireless

Syntax

```
grant extended-percent percent of service-type for BEST OF quota-name
```

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

service-type

One of the following:

- **Time** (Gx only)
- **Volume**
- **Service Specific**
- **Uplink Volume**
- **Downlink Volume**
- **All Volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the usage threshold to the highest available percentage of time, volume, or service-specific quantity of the selected quota profiles. See *Managing Quotas* for information on quotas. The best quota is determined using the following rules:

1. Passes are always better than plans
2. Between two passes, the one with the higher priority is better
3. Between two passes with equal priorities, the one with the earlier expiration date is better
4. Between two passes with equal priorities and expiration dates, the one with the earlier purchase date is better

Example

```
grant 100 percent of remaining on Volume for BEST OF
GoldDailyVol,GoldWeeklyVol,GoldMonthlyVol
```

grant # percent of *select type* for *select quota*

Mode

Wireless

Syntax
grant *extended-percent* percent of *type* for *quota-name*

Parameters
extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

type

One of the following:

- **Time**
- **Volume**
- **Service Specific**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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
```

grant # seconds for quota

Mode

Wireless

Syntax
`grant number seconds for quota`

Parameters
number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Grants a user the specified amount of time (in seconds) for the requested service. See *Managing Quotas* for information on quotas.

grant # service-specific units for quota

Mode

Wireless

Syntax

`grant number service-specific units for quota`

Parameters

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Grants a user the specified service-specific units for the requested service. See *Managing Quotas* for information on quotas.

grant session time limit to # percent of *select quota*

Mode

Wireless

Syntax

`grant session time limit to extended-percent percent of quota-name`

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the session time limit based on a percentage of the time limit, retrieved from up to five named quota profiles. See *Managing Quotas* for information on quotas.

grant *total* volume to # bytes of *select quota*

Mode

Wireless

Syntax

`grant number units of service-unit for quota-name`

Parameters

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the session volume limit in bytes or seconds for the named quota profile. See *Managing Quotas* for information on quotas.

grant *total* volume to # bytes of *select quota* using *monitoring key*

Mode

Wireless

Syntax

`grant number units of service-unit for quota-type using mon-key`

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

number

A numeric value.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-type

One of the following:

- **used** (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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

mon-key

Name(s) of a monitoring key in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 50 000 units of total volume (bytes) for used using key1

continue processing message
```

grant *total* volume to # percent *used* for BEST OF *select quota*

Mode

Wireless

Syntax

`grant` *`service-type`* `to` *`extended-percent`* `percent` *`quota-type`* `for BEST OF` *`quota-name`*

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**

- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-type

One of the following:

- **used** (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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the usage threshold to the highest available percentage volume or time of the selected quota profiles. See *Managing Quotas* for information on quotas. The best quota is determined using the following rules:

1. Passes are always better than plans
2. Between two passes, the one with the higher priority is better
3. Between two passes with equal priorities, the one with the earlier expiration date is better
4. Between two passes with equal priorities and expiration dates, the one with the earlier purchase date is better

Example

```
where the request is creating a new session
grant total volume to 100 percent used for BEST OF Monthly1,Daily1

continue processing message
```

grant *total* volume to # percent *used* for BEST OF *select quota* using *monitoring key*

Mode

Wireless

Syntax

```
grant service-type to extended-percent percent quota-type for BEST OF
quota-name using mon-key
```

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-type

One of the following:

- **used** (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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

mon-key

Name(s) of a monitoring key in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. The best quota is determined using the following rules:

1. Passes are always better than plans

2. Between two passes, the one with the higher priority is better
3. Between two passes with equal priorities, the one with the earlier expiration date is better
4. Between two passes with equal priorities and expiration dates, the one with the earlier purchase date is better

Example

```
where the request is creating a new session
grant total volume to 100 percent used for BEST OF Monthly1,Daily1 using
 key1

continue processing message
```

grant *total* volume to # percent *used* for *select quota*

Mode

Wireless

Syntax

`grant service-type to extended-percent percent quota-type for quota-name`

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-type

One of the following:

- **used** (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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

grant *total* volume to # percent *used* for *select quota* using *monitoring key*

Mode

Wireless

Syntax

```
grant service-type to extended-percent percent quota-type for quota-name
using mon-key
```

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-type

One of the following:

- **used** (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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

mon-key

Name(s) of a monitoring key in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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
```

grant *total* volume to *Min* of # bytes and # percent *used* for *select quota*

Mode

Wireless

Syntax

```
grant volume-type volume to extrema of number bytes and percent percent
quota-type for quota-name
```

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

extrema

One of the following:

- **Min** (default) — Specifies that the calculation sets the minimum level for the quota.
- **Max** — Specifies that the calculation sets the maximum level for the quota.

number

A numeric value.

quota-type

One of the following:

- **used** (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.

quota-name

Name(s) of quota defined in the CMP database.

Description

Grants a user the specified service-specific units for the requested service. See *Managing Quotas* for information on quotas.

Example

```
where the user is using less than 100 percent of total volume for DATA_Plan
 quota
grant total volume to Min of 20M bytes and 100 percent used for DATA_Plan
continue processing message
```

grant *total* volume to *Min* of # bytes and # percent *used* for *select quota* using *monitoring key*

Syntax

`grant volume-type volume to extrema of number bytes and percent percent for quota-type using mon-key`

Parameters

volume-type

One of the following:

- **total** (default)
- **uplink**
- **downlink**

extrema

One of the following:

- **Min** (default) — Specifies that the calculation sets the minimum level for the quota.
- **Max** — Specifies that the calculation sets the maximum level for the quota.

number

A numeric value.

percent

An integer value between 0 and 100.

quota-type

One of the following:

- **used** (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.

quota-name

Name(s) of quota defined in the CMP database.

mon-key

Name(s) of a monitoring key in the CMP database.

Description

Grants a user the specified service-specific units for the requested service. See *Managing Quotas* for information on quotas.

Example

```
where the user is using less than 100 percent of total volume for DATA_Plan
 quota
grant total volume to Min of 20M bytes and 100 percent used for DATA_Plan
 using SESS
continue processing message
```

install *specified* ADC rules for *select scope*

Mode

Wireless

Syntax

`install adc-rule ADC rules for adc-rule-scope-install`

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified ADC rule is installed for the session, using the values specified in the associated traffic profile. See *Managing Traffic Profiles* for information on traffic profiles.

Example

```
where the enforcement session is a DPI enforcement session
install ADC1,ADC5,ADC6 ADC rules for session
continue processing message
```

install *specified* ADC rules for *select scope* active between *start time and end time*

Mode

Wireless

Syntax

`install` *`adc-rule`* `ADC rules for` *`adc-rule-scope-install`* `active between` *`start-and-end-time`*

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

start-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:

- **None**— 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.
- **Specific Time** — Specifies the time and date to start/end in the form *YYYY-MM-dd*T*HH*:*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 — select to start/end now.
  - Time only — select to use the time only.
- **Policy Counter ID** — Select one or more policy counter IDs defined in the CMP database; or enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified ADC rule is installed for the session, using the values specified in the associated traffic profile, and is active between the specified start and end times. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* ADC rules for *select scope* active within *Time Period*

Mode

Wireless

Syntax

`install` *`adc-rule`* `ADC rules for` *`adc-rule-scope-install`* `active within` *`time-period`*

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-period

Select a predefiend time period.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified ADC rule is installed for the session, using the values specified in the associated traffic profile, and the rule is active for the specified time period. When a time period is used in a policy, you cannot delete that time period from the CMP database. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* ADC rules for *select scope* for *specified retry profile* active between *start time and end time*

Mode

Wireless

Syntax

install *adc-rule* ADC rules for *adc-rule-scope-install* for *retry-profile* active between *start-end-time*

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Name of a retry profile that is defined in the CMP database. (See *Managing Retry Profiles* for more information.)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

start-end-time

Specifies the start and end time for rule to be active. If a start time is not specified, the rule becomes active immediately. If an end time is not specified, the rule never deactivates. Select either absolute time or relative time for both the start time and the 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-dd*T*HH*:*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.
  - none — ignore time.
  - Now — select to start/end now.
  - Time only — select to use the time only.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified ADC rule is installed for the session, using the values specified in the associated traffic profile and the associated retry profile, and the rule is active for the specified time period. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* ADC rules for *select scope* for *specified retry profile* active within *Time Period*

Mode

Wireless

Syntax

```
install adc-rule ADC rules for adc-rule-scope-install for retry-profile
active within time-period
```

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Name of a retry profile that is defined in the CMP database. (See *Managing Retry Profiles* for more information.)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified ADC rule is installed for the session, using the values specified in the associated traffic profile and the associated retry profile, and the rule is active for the specified time period. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* ADC rules for *select scope* with *specified retry profile*

Mode

Wireless

Syntax

`install` *`adc-rule`* `ADC rules for` *`adc-rule-scope-install`* `with` *`retry-profile`*

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Name of a retry profile that is defined in the CMP database. (See *Managing Retry Profiles* for more information.)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified ADC rule is installed for the session, using the values specified in the associated traffic profile and the associated retry profile. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* PCC rules for *select scope*

Mode

Wireless

Syntax

`install` *`pcc-rule`* `PCC rules for` *`pcc-rule-scope-install`*

Parameters

pcc-rule

Names of policy and charging control traffic profiles that are defined in the CMP database. The PCC profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

The specified PCC rule is installed for either the session or flow, using the values specified in the associated traffic profile. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* PCC rules for *select scope* active between *start time and end time*

Mode

Wireless

Syntax

`install` *`pcc-rule`* `PCC rules for` *`pcc-rule-scope-install`* `active between` *`start-and-end-time`*

Parameters

pcc-rule

Names of policy and charging control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

start-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:

- **None**— 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.
- **Specific Time** — Specifies the time and date to start/end in the form *YYYY-MM-dd*T*HH*:*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 — select to start/end now
  - Time only — select to use the time only

- **Policy Counter Id** — Select one or more policy counter IDs defined in the CMP database; or enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* PCC rules for *select scope* active within *Time Period*

Mode

Wireless

Syntax

`install` *`pcc-rule`* `PCC rules for` *`pcc-rule-scope-install`* `active within` *`time-period`*

Parameters

pcc-rule

Names of policy and charging control profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. When a time period is used in a policy, you cannot delete that time period from the CMP database. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* PCC rules for *select scope* for *specified retry profile* active between *start time and end time*

Mode

Wireless

Syntax

`install` *`pcc-rule`* `PCC rules for` *`pcc-rule-scope-install`* `for` *`retry-profile`*
`active between` *`start-end-time`*

Parameters

pcc-rule

Names of policy and charging control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Name of a retry profile that is defined in the CMP database. (See *Managing Retry Profiles* for more information.)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

start-end-time

Specifies the start and end time for rule to be active. If a start time is not specified, the rule becomes active immediately. If an end time is not specified, the rule never deactivates. Select either absolute time or relative time for both the start time and the 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-dd*T*HH*:*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 — select to start/end now.
  - Time only — select to use the time only.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* PCC rules for *select scope* for *specified retry profile* active within *Time Period*

Mode

Wireless

Syntax

install *pcc-rule* PCC rules for *pcc-rule-scope-install* for *retry-profile* active within *time-period*

Parameters

pcc-rule

Names of policy and charging control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Name of a retry profile that is defined in the CMP database. (See *Managing Retry Profiles* for more information.)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See *Managing Traffic Profiles* for information on traffic profiles.

install *specified* PCC rules for *select scope* with *specified retry profile*

Mode

Wireless

Syntax

`install` *`pcc-rule`* `PCC rules for` *`pcc-rule-scope-install`* `with` *`retry-profile`*

Parameters

pcc-rule

Names of policy and charging control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Name of a retry profile that is defined in the CMP database. (See *Managing Retry Profiles* for more information.)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. See *Managing Traffic Profiles* for information on traffic profiles.

mark request AVP *name* as failed if exists and send *always*

Mode

Wireless

Syntax

`mark request AVP name as failed if exists and send send-mode`

Parameters

name

String representing existing AVP name, entered in the format *AVPname*:*VendorID* or, for nested AVP names in an AVP group, entered in the format [*AVPname1*]:*VendorID*.[*AVPname2*]:*VendorID* ... for the members of the grouped AVPs. There is also the option to evaluate as an expression (click to select check box).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

send-mode

One of the following:

- **always** (default)
- **unless rejected**
- **if rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

overwrite DSCP/TOS field with

Mode

Cable

Syntax

```
overwrite DSCP/TOS field with dscp
```

Parameters

dscp

A numeric representation of DSCP bits to be inserted into the message.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Overwrites the DSCP/TOS field with a value. Although this is a number, the policy wizard includes a customized dialog to help you construct the value.

overwrite SessionClassId with

Mode

Cable

Syntax

```
overwrite SessionClassId with number
```

Parameters

number

A numeric value.

Valid range is 0–2000000000.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Overwrites the *SessionClassId* field in the message with the specified value.

re-authorize all credit control sessions associated with User

Mode

Wireless

Syntax

```
re-authorize all credit control sessions associated with User
```

Parameters

None

Description

Triggers reauthorization for PCEF sessions for all the user's sessions.

re-authorize all PCEF/TDF sessions associated with *select scope*

Mode

Wireless

Syntax

```
re-authorize all PCEF/TDF sessions associated with pcef-scope-install
```

Parameters

pcef-scope-install

One of the following:

- **IP-CAN session**
- **user**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers reauthorization for PCEF or TDF 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.

release all credit control sessions associated with User

Mode

Wireless

Syntax

```
release all credit control sessions associated with User
```

Parameters

None

Description

Triggers release of credit control sessions for all the sessions for the user.

release all PCEF/TDF sessions associated with *select scope*

Mode

Wireless

Syntax

`release all PCEF/TDF sessions associated with` *`pcef-scope-install`*

Parameters

pcef-scope-install

One of the following:

- **IP-CAN session**
- **user**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Triggers release of PCEF or TDF 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).

release the session

Mode

Wireless

Syntax

`release the session`

Parameters

None

Description

Releases the session.

release the session with cause `*ReleaseCause*`

Mode

Wireless

Syntax

`release the session with cause` *`release_cause`*

Parameters

release_cause

One of the following:

- **UNSPECIFIED_REASON**
- **UE_SUBSCRIPTION_REASON**
- **INSUFFICIENT_SERVER_RESOURCES**
- **IP_CAN_SESSION_TERMINATION**

Description

Releases the session and provides the cause.

remove ADC rule types *select types of rules* for *select scope*

Mode

Wireless

Syntax

`remove ADC rule types` *`adc-rule-type`* `for` *`adc-rule-scope-install`*

Parameters

adc-rule-type

One or more of the following:

- **none**
- **predefined**
- **predefined base**
- **dynamically provisioned**
- **all**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

adc-rule-scope-install

One of the following:

- **session**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Removes the application detection control rules from the current session based on their type. See *Managing Traffic Profiles* for information on ADC traffic profiles.

remove all policy context properties

Mode

Cable, Wireless, Wireline

Syntax

```
remove all policy context properties
```

Parameters

None

Description

In Wireless mode, removes all subscriber properties in the SPR.

In Cable mode, removes all policy context properties.

In Wireline mode, removes all policy context properties.

Removes all policy context properties.

remove all the *scope* state variables and save *always*

Mode

Wireless

Syntax

remove all the *scope* state variables and save *save-mode*

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Note: *save-mode* is not applicable with the **policy_evaluation** scope since this variable only exists in the policy.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Deletes all the state variable for a scope. You can specify that the properties are not deleted if the policy rejects the message.

remove custom AVP *name* from reply *always*

Mode

Wireless

Syntax

`remove custom AVP name from reply send-mode`

Parameters

name

An existing AVP name and Vender ID, or an AVP name from an existing Policy Table.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

send-mode

One of the following:

- **always** (default)
- **unless rejected**
- **if rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Removes the custom AVP name previously set from the reply message.

remove *default* PCC rules of *default* TDF application IDs for APPLICATION_STOP

Mode

Wireless

Syntax

remove *traffic-profile* PCC /ADCrules of *value-list* TDF application IDs for APPLICATION_STOP

Parameters

traffic-profile

One or more traffic profiles. For more information on traffic profiles, see *Managing Traffic Profiles*.

If **default** (default) is specified, all associated PCCrules according to Application-Detection-Information AVP in this report are removed. If specific PCC rules are specified, the associated PCC rules that should be removed must also in specified PCC rules.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value-list

A comma-delimited list of values to compare against.

If **default** (default) is specified, all PCC rules according to Application-Detection-Information AVP in this report are removed. If specific TDF-Application-Identifiers are specified, the associated PCC rules that should be removed must also in specified PCC rules.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

This action removes PCC rules when the PCEF reports an application stop.

The TDF-Application-Identifier and TDF-Application-Instance-Identifier must be bound to the PCC rules before the application start.

If there is not a TDF-Application-Instance-Identifier in the Application-Detection-Information AVP, but PCC rules contain binding info to that a TDF-Application-Identifier is installed, the MPE device logs the following warning in the trace log and continues with the session processing.

```
Policy Trace policy name: Could not execute 'remove PCC rules of TDF application

ids for APPLICATION_STOP' because there is no TDF-Application-Instance-Identifier
 in
Application-Detection-Information AVP
```

If the PCC rules that are associated with the TDF-Application-Identifier and TDF-Application-Instance-Identifier info is not found, then MPE device logs the following warning in the trace log and continues with the session processing.

```
Policy Trace policy name: Could not execute 'remove PCC rules of TDF application

ids for APPLICATION_STOP ' because can not find related PCC rule to remove,
TDF-Application-Identifier:TDFID,
TDF-Application-Instance-Identifier:InstanceID
```

remove PCC rule for the flow

Mode

Wireless

Syntax

```
remove PCC rule for the flow
```

Parameters

None

Description

Removes the policy and charging control rule from the current flow. See *Managing Traffic Profiles* for information on PCC traffic profiles.

remove PCC rule types *select types of rules* for *select scope*

Mode

Wireless

Syntax

`remove PCC rule types` *`pcc-rule-type`* `for` *`pcc-rule-scope-install`*

Parameters

pcc-rule-type

One or more of the following:

- **none**
- **predefined**
- **predefined base**
- **dynamically provisioned**
- **all**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

pcc-rule-scope-install

One of the following:

- **flow**
- **session**
- **all**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Removes the policy and charging control rules from the current flow/session based on their type. See *Managing Traffic Profiles* for information on PCC traffic profiles.

remove policy context property *name*

Mode

Cable, Wireless, Wireline

Syntax

`remove policy context property` *`property-name`*

Parameters

property-name

String. May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Removes a policy context property (in Cable mode and Wireline mode) or a subscriber property in the SPR (in Wireless mode).

Removes a policy context property.

remove *specified* ADC rules

Mode

Wireless

Syntax

`remove` *`adc-rule`* `ADC rules`

Parameters

adc-rule

Names of application detection control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **ADC Rule**
- **Predefined ADC Rule**
- **Predefined ADC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Removes the ADC rules from the current session.

remove *specified* PCC rules

Mode

Wireless

Syntax

`remove pcc-rule PCC rules`

Parameters

pcc-rule

Names of policy and charging control traffic profiles that are defined in the CMP database. The traffic profiles must be one of the following types:

- **PCC Rule**
- **Predefined PCC Rule**
- **Predefined PCC Rule Base**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Removes the PCC rules from the current flow/session. See *Managing Traffic Profiles* for information on traffic profiles.

remove the *scope* state variable *name* and save *always*

Mode

Wireless

Syntax

`remove the scope state variable variable-name and save save-mode`

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Note: *save-mode* is not applicable with the **policy_evaluation** scope since this variable only exists in the policy.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Deletes a state variable. You can specify that the variable is not deleted if the policy rejects the message.

request usage report for *monitoring key*

Mode

Wireless

Syntax

`request usage report for mon-key`

Parameters

mon-key

Name(s) of a monitoring key in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

reset all plan usage

Mode

Wireless

Syntax

`reset all plan usage`

Parameters

None

Description

Resets all plans for the subscriber.

reset all plan usage with reset type of `select reset type`

Mode

Wireless

Syntax

`reset all plan usage with reset type of` *`reset_type`*

Parameters

reset_type

One of the following:

- **Usage**
- **Rollover**
- **Billing Cycle**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Resets all plan usage for the selected reset type. See *Managing Quotas* for information on quotas.

reset all subscriber data

Mode

Wireless

Syntax

`reset all subscriber data`

Parameters

None

Description

Resets all data for the subscriber.

reset *select quota* reset type of *select reset type*

Mode

Wireless

Syntax

`reset` *`quota-name`* `reset type of` *`reset-type`*

Parameters

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

reset-type

One of the following:

- **Usage**
- **Rollover**
- **Billing Cycle**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Resets the selected quota with the selected reset type. See *Managing Quotas* for information on quotas.

reset usage for *select quota*

Mode

Wireless

Syntax

`reset usage for` *`quota-name`*

Parameters

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Resets the selected quota. See *Managing Quotas* for information on quotas.

revalidate the session at *datetime* using `configured local time`

Mode

Wireless

Syntax

`revalidate the session at` *`datetime`* `using` *`time-zone`*

Parameters

datetime

One of the following:

- The local date-time **now** (default)
- A policy variable
- A date-time in the format: *`yyyy-mm-dd`*`T`*`hh`*`:`*`mm`*`:`*`ss+UTCoffset`*

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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
```

schedule next RAR for resetting usage for *select quota*

Mode

Wireless

Syntax

`creates the next RAR task to reset usage for` *`quota-name`*

Parameters

quota-name

Name(s) of quota defined in the CMP database.

Description

Causes the next RAR that is sent to reset usage for a selected quota.

send CoA with *COA Template*

Mode

Wireless

Syntax

`send CoA with coa`

Parameters

coa

Select a RADIUS CoA template from the list.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Send a RADIUS change of authorization (CoA) message, constructed using the specified CoA template, to the broadband network gateway that sent the RADIUS request that caused the policy to be triggered. To send multiple CoA messages, include this action multiple times in the policy.

Example

The following example issues an updated RADIUS CoA message when a Profile Notification Request (PNR) message is received from an SPR system:

```
where notification from Sh datasource is received for Quota Usage
send CoA with CoA10-24
continue processing message
```

send http *action* notification to *select notification destination* with headers *headers* and content *content*

Mode

Wireless mode with the SMS:SMPP or SMS:XML function enabled.

Syntax

`send http http_method notification to server with headers headers and content content`

Parameters

http_method

String. The HTTP method for the request message. Supported methods are:

- **POST** — (default) a method for sending data for processing by the application specified by URL
- **GET** — a method for requesting the retrieval of data located at the specified URL
- **PUT** — a method for requesting the storage of the data at the specified URL
- **DELETE** — a method for deleting the data located at the specified URL

server

A list of the defined notification servers. Select the notification server from the list. See *Managing Notification Servers* for information about adding a notification server.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

headers

String. One or more HTTP message headers (up to a maximum of 20 headers) using the format: *field-name:field-value*. For example, *Content-Type:text/xml*, *Content-Type:application/json*, and *Content-Type:text/plain*. Refer to the HTTP standard at *http://www.ietf.org* for details on valid message header fields and values. This field cannot be empty.

Note: MPE does not validate whether the field-value corresponds to the field-name.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

content

String. The message body content that supports any type of notification like JSON/XML/Text message. The content can use policy variable substitution and can contain up to 4000 characters.

Note: MPE does not validate whether the message headers correspond to particular content.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Enables PCRF to send a configurable HTTP request message using the Web services interface. These notification messages are sent to pre-configured destinations. After a notification message is sent, PCRF receives the response from the specified URL. In the event of a failure, PCRF does not attempt to re-send the message.

Examples

XML POST

```
send http POST  notification to NS1 with headers
Content-Type:text/xml;charset=UTF-8 and content <?xml version="1.0"
encoding="UTF-8"?> <subscriber> <msisdn>{User.MSISDN}</msisdn>
<quota>{User.Quota.Foo.volume}</quota> </subscriber>
```

JSON POST

```
send http POST notification to NS2 with
headers Content-Type: application/json and content
{"class":"Subscriber","entitlement":"Extended
Service`,`msisdn`:`{User.MSISDN}`,`name`:`{User.name}`}`
```

HTTP GET with query parameters

```
send http GET notification to
NS3 with headers Content-Type:text/plain and content ``
```

send http *action* notification to url *URL* with headers *headers* and content *content*

Mode

Wireless mode with the SMS:SMPP or SMS:XML function enabled.

Syntax

`send http` *`http_method`* `notification to url` *`URL`* `with headers` *`headers`* `and content` *`content`*

Parameters

http_method

String. The HTTP method for the request message. Supported methods are:

- **POST** — (default) a method for sending data for processing by the application specified by URL
- **GET** — a method for requesting the retrieval of data located at the specified URL
- **PUT** — a method for requesting the storage of the data at the specified URL
- **DELETE** — a method for deleting the data located at the specified URL

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

URL

String. The dynamic URL for the server that is the destination for the HTTP request message. This URL can use policy variable substitution, for example, *http://10.15.20.190:80/rs/quota/notify/{User.MSISDN}*.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

headers

(Required) String. One or more HTTP message headers (up to a maximum of 20 headers) using the format: *field-name :field-value*. For example:

- `Content-Type:text/xml`
- `Content-Type:application/json`
- `Content-Type:text/plain`

Refer to the HTTP standard at *http://www.ietf.org* for details on valid message header fields and values. This field cannot be empty.

Note: MPE does not validate whether the field-value corresponds to the field-name.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

content

String. The message body content that supports any type of notification like JSON/XML/Text message. The content can use policy variable substitution and can contain a maximum of 4000 characters.

Note: MPE does not validate whether the message headers correspond to particular content.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Enables PCRF to send a configurable HTTP request message using the web services interface. These notification messages are sent to either servers configured in CMP or to servers using a dynamic URL. After a notification message is sent, PCRF receives the response from the specified URL. In the event of a failure, PCRF does not attempt to resend the message.

Examples

XML POST

```
send http POST notification to url
http://10.15.20.190:80/rs/quota/xmlnotify with
headers Content-Type:text/xml;charset=UTF-8 and
content <?xml version="1.0" encoding="UTF-8"?> <subscriber>
<msisdn>{User.MSISDN}</msisdn> <quota>{User.Quota.Foo.volume}</quota>
</subscriber>`
```

JSON POST

```
send http POST notification to url
http://10.15.20.190:80/rs/quota/jsonnotify/{User.MSISDN} with
headers Content-Type: application/json and content
{"class":"Subscriber","entitlement":"Extended
Service`,`msisdn`:`{User.MSISDN}`,`name`:`{User.name}`}`
```

HTTP GET with query parameters

```
send http GET notification to url
http://10.15.20.190:80/rs/quota/notify?msisdn={User.MSISDN}&quota={User.Quota.Foo.volume}
 with
headers Content-Type:text/plain and content ``
```

send notification to syslog with `*message text*` and severity `*severity level*`

Mode

Cable, Wireless, Wireline

Syntax

`send notification to syslog with` `` `*message*` `` `and severity` `` `*level*` ``

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

level

The sevlog severity. One of the following:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info**
- **Debug**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends a message to the syslog service containing the specified message text and at the specified 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, which sends a notification to the syslog instead of an alarm to the CMP system.

send notification to trace log with `*message text*` and severity `*severity level*`

Mode

Cable, Wireless

Syntax

`send notification to trace log with` `` `*message*` `` `and severity` `` `*level*` ``

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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` are converted to use this action, with the severity of Info.

send SMS Alert `*specified*` to user

Mode

Wireless mode with the SMS:XML function enabled.

Syntax

`send SMS Alert` `message` `to user`

Parameters

message

String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends an SMS alert message, with specified text, to the subscriber associated with the message.

Example

```
send SMS alert `you have reached 80%% of your quota {User.MSISDN}` to user
```

send SMS `*specified*` to `*default*` destination address, `*default*` TON and `*default*` NPI from `*default*` source address, `*default*` TON and `*default*` NPI on `*Billing Day*`. Request delivery receipt `*default*`.

Mode

Wireless mode the SMS:SMPP function enabled:

Syntax

```
send SMS `message` to `dest_address` destination address, `ton` TON and
`npi` NPI from `source_address` source address, `ton` TON and `npi` NPI
`delivery-day`. Request delivery receipt `receipt`.
```

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

ton

If not the default, this overrides the configured Type of Number. One of the following:

- **default** (default)
- **UNKNOWN**
- **INTERNATIONAL**
- **NATIONAL**
- **NETWORK SPECIFIC**
- **SUBSCRIBER NUMBER**
- **ALPHANUMERIC**
- **ABBREVIATED**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

npi

If not the default, this overrides the configured Number Plan Indicator. One of the following:

- **default** (default)
- **UNKNOWN**
- **ISDN (E163/E164)**
- **DATA (X.121)**
- **TELEX (F.69)**
- **LAND MOBILE (E.212)**
- **NATIONAL**
- **PRIVATE**
- **ERMES**
- **INTERNET (IP)**
- **WAP CLIENT ID**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

source_address

String. If not the default, this overrides the configured address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

delivery-day

String. Enter a value in one of the following formats:

- **`Billing Day`** (default) — Keep the default value **`Billing Day`** to deliver the SMS on the user's billing day. If the policy is triggered on the user's billing day, the SMS will be delivered on the current billing day.
- **day** — Enter an integer between 1 and 31 to deliver the SMS on the specified day of the month. If the specified day of the month has passed for the current month, the SMS will be delivered on that day in the following month. If the specified day of the month does not exist in the current month, the SMS will be delivered on the last day of the month. Any value less than 1 or greater than 31 is invalid.
- **smart string** — Enable the **Evaluate as Expression** checkbox. In the **Value** field, enter an arithmetic expression containing one of the following policy parameters:
  - **`{User.BillingDay}`** — The billing day for the subscriber profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.`*`custom_field`*`}`**, where *custom_field* is a configured custom subscriber profile field, may also be used if the custom field resolves to an integer value.
  - **`{User.Pool.BillingDay}`** — The billing day for the subscriber's pool profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.Pool.`*`custom_field`*`}`**, where *custom_field* is a configured custom pool profile field, may also be used if the custom field resolves to an integer value.

  The arithmetic expression supports addition and subtraction and must not contain the default value **`Billing Day`**. The result will be evaluated with consideration to the number of days in the current month. For example, the expression **`{User.BillingDay}-4`** would deliver the SMS four days before the user's billing

day. If the expression would result in the SMS being sent in the past, the SMS will not be sent.

Note: Scheduled SMS delivery is only available when the user's billing type is monthly.

receipt

One of the following:

- **default** (default) — Use global default configured for this MPE device.
- **No Delivery Receipt**
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends an SMS text message, with specified text, to the subscriber associated with the message on the billing day for the subscriber.

In SMPP mode, messages can be up to 254 characters long. If SMPP long message support is configured, SMS messages longer than 160 characters are split into segments and reassembled by the receiving device; messages of up to 1000 characters are supported. See the appropriate *CMP User's Guide* for information on configuring SMPP long message support.

Note: Messages over 1000 characters are truncated.

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 MSISDN for the subscriber. If the MSISDN for the subscriber cannot be determined, then an SMS message is not 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 in either case. See the *CMP Wireless User's Guide* for information on configuring delivery receipt default actions.

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 Billing Day.
Request delivery receipt `Default`.
```

send SMS `*specified*` to `*default*` destination address, `*default*` TON and `*default*` NPI from `*default*` source address, `*default*` TON and `*default*` NPI on `*now*`. Request delivery receipt `*default*`.

Mode

Wireless mode the SMS:SMPP function enabled:

Syntax

`send SMS` `` `*message*` `` `to` `` `*dest_address*` `` `destination address,` `` `*ton*` `` `TON and` `` `*npi*` `` `NPI from` `` `*source_address*` `` `source address,` `` `*ton*` `` `TON and` `` `*npi*` `` `NPI on` `*delivery-day*`. `Request delivery receipt` `` `*receipt*` `.

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

ton

If not the default, this overrides the configured Type of Number. One of the following:

- **default** (default)
- **UNKNOWN**
- **INTERNATIONAL**
- **NATIONAL**
- **NETWORK SPECIFIC**
- **SUBSCRIBER NUMBER**
- **ALPHANUMERIC**
- **ABBREVIATED**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

npi

If not the default, this overrides the configured Number Plan Indicator. One of the following:

- **default** (default)
- **UNKNOWN**
- **ISDN (E163/E164)**
- **DATA (X.121)**
- **TELEX (F.69)**
- **LAND MOBILE (E.212)**

- **NATIONAL**
- **PRIVATE**
- **ERMES**
- **INTERNET (IP)**
- **WAP CLIENT ID**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

source_address

String. If not the default, this overrides the configured address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

delivery-day

String. Enter a value in one of the following formats:

- **`now`** (default) — Keep the default value **`now`** to deliver the SMS immediately when the policy is triggered.
- **day** — Enter an integer between 1 and 31 to deliver the SMS on the specified day of the month. If the specified day of the month has passed for the current month, the SMS will be delivered on that day in the following month. If the specified day of the month does not exist in the current month, the SMS will be delivered on the last day of the month. Any value less than 1 or greater than 31 is invalid.
- **smart string** — Enable the **Evaluate as Expression** checkbox. In the **Value** field, enter an arithmetic expression containing one of the following policy parameters:
  - **`{User.BillingDay}`** — The billing day for the subscriber profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.`*`custom_field`*`}`**, where *custom_field* is a configured custom subscriber profile field, may also be used if the custom field resolves to an integer value.
  - **`{User.Pool.BillingDay}`** — The billing day for the subscriber's pool profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.Pool.`*`custom_field`*`}`**, where *custom_field* is a configured custom pool profile field, may also be used if the custom field resolves to an integer value.

  The arithmetic expression supports addition and subtraction and must not contain the default value **`now`**. The result will be evaluated with consideration to the number of days in the current month. For example, the expression **`{User.BillingDay}-4`** would deliver the SMS four days before the user's billing day. If the expression would result in the SMS being sent in the past, the SMS will not be sent.

Note: Scheduled SMS delivery is only available when the user's billing type is monthly.

receipt

One of the following:

- **default** (default) — Use global default configured for this MPE device.
- **No Delivery Receipt**
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. If SMPP long message support is configured, SMS messages longer than 160 characters are split into segments and reassembled by the receiving device; messages of up to 1000 characters are supported. See the appropriate *CMP User's Guide* for information on configuring SMPP long message support.

Note: Messages over 1000 characters are truncated.

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 in either case. See the *CMP Wireless User's Guide* for information on configuring delivery receipt default actions.

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 `now`. Request delivery receipt `default`.
```

send SMS `*specified*` to `*default*` destination address, from `*default*` source address. Request delivery receipt `*default*`.

Mode

Wireless mode With at least one of the following functions enabled:

- SMS:SMPP
- SMS:XML

Syntax

```
send SMS `message` to `dest_address` destination address, from
`source_address` source address. Request delivery receipt `receipt`.
```

Parameters

message

String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

source_address

String. If not the default, this overrides the configured address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

receipt

One of the following:

- **default** (default) — The Registered Delivery value is used. See the appropriate CMP user's guide.
- **No Delivery Receipt**
- **Delivery Receipt**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends an SMS CMPP text message, with specified text, to the subscriber associated with the message.

The default source and destination address 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. 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.

Example

The following example uses a custom field named "Custom7" in the User.Pool object, defined in an SPR, of comma-separated MSISDN values to send a notification message to all members of a subscriber pool:

```
send SMS `1 GB of data has been granted to your subscriber pool.` to
`{User.Pool.Custom7}` destination
address, from `default` source address. Request delivery receipt `default`.
```

Because a custom field is limited to 255 characters, the list of MSISDNs in a large subscriber pool may require multiple variables. The following example uses a series of custom fields in the User.Pool object, defined in an SPR, each containing comma-separated MSISDN values, to send a message to all members of a large subscriber pool:

```
send SMS `1 GB of data has been granted to your subscriber pool.` to
`{User.Pool.Custom7},{User.Pool.Custom8},{User.Pool.Custom9}` destination

address, from `default` source address. Request delivery receipt `default`.
```

send SMS `*specified*` to `*default*` destination address, ' from `*default*` source address on user billing day. Request delivery receipt `*default*`.

Mode

Wireless mode With at least one of the following functions enabled:

- SMS:SMPP
- SMS:XML

Syntax

```
send SMS `message` to `dest_address` destination address, from
`source_address` source address. Request delivery receipt `receipt`.
```

Parameters

message

String. This text may contain policy parameters (described later in this section) to perform parameter substitution within the message text.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

source_address

String. If not the default, this overrides the configured address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

receipt

One of the following:

- **default** (default) — The Registered Delivery value is used. See the appropriate CMP user's guide.
- **No Delivery Receipt**
- **Delivery Receipt**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends an SMS CMPP text message, with specified text, to the subscriber associated with the message on the user billing day.

The default source and destination address 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. 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.

send SMS `*specified*` to user on `*Billing Day*`. Request delivery receipt `*default*`.

Mode

Wireless mode with at least one of the following functions enabled:

- SMS:SMPP
- SMS:XML

Syntax

```
send SMS `message` to user on `delivery-day`. Request delivery receipt
`receipt`.
```

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

delivery-day

String. Enter a value in one of the following formats:

- **`Billing Day`** (default) — Keep the default value **`Billing Day`** to deliver the SMS on the user's billing day. If the policy is triggered on the user's billing day, the SMS will be delivered on the current billing day.
- **day** — Enter an integer between 1 and 31 to deliver the SMS on the specified day of the month. If the specified day of the month has passed for the current month, the SMS will be delivered on that day in the following month. If the specified day of the month does not exist in the current month, the SMS will be delivered on the last day of the month. Any value less than 1 or greater than 31 is invalid.
- **smart string** — Enable the **Evaluate as Expression** checkbox. In the **Value** field, enter an arithmetic expression containing one of the following policy parameters:
  - **`{User.BillingDay}`** — The billing day for the subscriber profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.`*`custom_field`*`}`**, where *custom_field* is a configured custom subscriber profile field, may also be used if the custom field resolves to an integer value.
  - **`{User.Pool.BillingDay}`** — The billing day for the subscriber's pool profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.Pool.`*`custom_field`*`}`**, where *custom_field* is a configured custom pool profile field, may also be used if the custom field resolves to an integer value.

  The arithmetic expression supports addition and subtraction and must not contain the default value **`Billing Day`**. The result will be evaluated with consideration to the number of days in the current month. For example, the expression **`{User.BillingDay}-4`** would deliver the SMS four days before the user's billing day. If the expression would result in the SMS being sent in the past, the SMS will not be sent.

Note: Scheduled SMS delivery is only available when the user's billing type is monthly.

receipt

One of the following:

- **default** (default) — Use global default configured for this MPE device.
- **No Delivery Receipt**
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends an SMS text message, with specified text, to the subscriber associated with the message on the billing day for the subscriber.

In SMPP mode, messages can be up to 254 characters long. If SMPP long message support is configured, SMS messages longer than 160 characters are split into segments and reassembled by the receiving

device; messages of up to 1000 characters are supported. See the appropriate *CMP User's Guide* for information on configuring SMPP long message support.

Note: Messages over 1000 characters are truncated.

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 in either case. See the *CMP Wireless User's Guide* for information on configuring delivery receipt default functions.

Example

```
send SMS `you have reached 80%% of your quota` to user on `Billing Day`.
 Request delivery receipt `Default`.
```

send SMS `*specified*` to user on `*now*`. Request delivery receipt `*default*`.

Mode

Wireless mode with at least one of the following functions enabled:

- SMS:SMPP
- SMS:XML

Syntax

```
send SMS `message` to user on `delivery-day`. Request delivery receipt
`receipt`.
```

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

delivery-day

String. Enter a value in one of the following formats:

- **`now`** (default) — Keep the default value **`now`** to deliver the SMS immediately when the policy is triggered.
- **day** — Enter an integer between 1 and 31 to deliver the SMS on the specified day of the month. If the specified day of the month has passed for the current month, the SMS will be delivered on that day in the following month. If the specified day of the month does not exist in the current month, the SMS will be delivered on the last day of the month. Any value less than 1 or greater than 31 is invalid.
- **smart string** — Enable the **Evaluate as Expression** checkbox. In the **Value** field, enter an arithmetic expression containing one of the following policy parameters:
  - **`{User.BillingDay}`** — The billing day for the subscriber profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter

`{User.`*`custom_field`*`}`, where *custom_field* is a configured custom subscriber profile field, may also be used if the custom field resolves to an integer value.

- **`{User.Pool.BillingDay}`** — The billing day for the subscriber's pool profile. Resolves to an integer between 1 and 31. If this parameter is used, the parameter **`{User.Pool.`*`custom_field`*`}`**, where *custom_field* is a configured custom pool profile field, may also be used if the custom field resolves to an integer value.

The arithmetic expression supports addition and subtraction and must not contain the default value **`now`**. The result will be evaluated with consideration to the number of days in the current month. For example, the expression **`{User.BillingDay}-4`** would deliver the SMS four days before the user's billing day. If the expression would result in the SMS being sent in the past, the SMS will not be sent.

Note: Scheduled SMS delivery is only available when the user's billing type is monthly.

receipt

One of the following:

- **default** (default) — Use global default configured for this MPE device.
- **No Delivery Receipt**
- **Delivery Receipt on success and failure**
- **Delivery Receipt on failure**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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. If SMPP long message support is configured, SMS messages longer than 160 characters are split into segments and reassembled by the receiving device; messages of up to 1000 characters are supported. See the appropriate *CMP User's Guide* for information on configuring SMPP long message support.

Note: Messages over 1000 characters are truncated.

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 in either case. See the *CMP Wireless User's Guide* for information on configuring delivery receipt default functions.

Example

```
send SMS `you have reached 80%% of your quota` to user on
`{User.BillingDay}-4`. Request delivery receipt `Default`.
```

send SMS `*specified*` to user from `*default*` source address if exceed `*number*` `*days*` for `*Identity*`. Request delivery receipt `*default*`.

Mode

Wireless mode With at least one of the following functions enabled:

- SMS:XML

Syntax

```
send SMS `message` to user from `source_address` source address, if exceed
`number' `days` for `identity`. Request delivery receipt `receipt`.
```

Parameters

message

String. This text can contain policy parameters (described later in this section) to perform parameter substitution within the message text.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

source_address

String. If not the default, this overrides the configured address. To specify the the default, enter **`deafault`**. The default uses the value of the smpp.protocol.srcId attribute configured in the SMPP.properties.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

number

Positive integer.

days

The calculated datetime is expressed in this granularity:

- **days** (default)
- **hours**

Identity

String. Identifies different types of SMS messages. Must be less than 20 characters.

receipt

One of the following:

- **default** (default)—Uses global default configured for this MPE device. Uses the Registered Delivery global default which is configured in SMS profile section of the **Policy Server** tab.
- **No Delivery Receipt**—Doe not request a delivery receipt when sending an SMS message.
- **Delivery Receipt**—Requests a delivery receipt when sending an SMS message.

Description

Sends an SMS text message to an end user once during the configured interval.

You can request a receipt from the SMSC server, which will be logged in the file CMPP.log, when the message is delivered to the subscriber. You can also request a receipt. See the CMP user's guide for information on configuring delivery receipt default functions.

The last delivery time for each type of SMS message (specified in the *Identity* variable) is listed on the **State** tab of the **Profile Data** in the **SPR** section of the navigation pane.

send SMS `*specified*` to user. Request delivery receipt `*default*`.

Syntax

`send SMS` `*message*` `to user. Request delivery receipt` `*receipt*`.

Mode

Wireless mode With at least one of the following functions enabled:

- SMS:SMPP
- SMS:XML

Parameters

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

receipt

One of the following:

- **default** (default) — The value in the Registered Delivery field configured in the protocol options is used. See the appropriate CMP user's guide for information on configuring protocol options.
- **No Delivery Receipt**
- **Delivery Receipt**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends a CMPP message, with specified text, to the subscriber associated with the message.

Example

```
send SMS `you have reached 80%% of your quota` to user. Request delivery
 receipt `Default`.
```

send SMTP message with the following *text/plain* content:

Mode

Wireless mode with SMS:SMPP or SMS:XML function enabled.

Syntax

```
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
```

Parameters

format

One of the following:

- **text/plain** (default) — The email is in plain-text format.
- **text/html** — The email includes HTML formatting.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

reply_address

String. If not the default, this overrides the configured address.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

subject

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

message

String. Body of the message.

signature

String. If not `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 *bcc_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 the *CMP Wieless User's Guide* for information on configuring SMTP default values.

set alarm with severity `*severity level*`, id `*unique alarm identifier*` and message `*message text*`

Mode

Cable, Wireless

Syntax

```
set alarm with severity `level`, id `alarm-id` and message `message`
```

Parameters

level

One of the following:

- **Critical** (ID 74000)
- **Major** (ID 74001)
- **Minor** (ID 74002)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sends an alarm to the CMP system 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 the appropriate *CMP User's Guide*.

set authorization validity time to # seconds

Mode

Wireless

Syntax

`set authorization validity time to` *`seconds`* `seconds`

Parameters

seconds

A numeric value that specifies time in units of seconds.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set authorization validity time to *datetime*

Mode

Wireless

Syntax

`set authorization validity time to` *`datetime`*

Parameters

datetime

One of the following:

- The local date-time **now** (default)
- A policy variable
- A date-time in the format: `yyyy-mm-ddThh:mm:ss+UTCoffset`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set authorization validity time to *time* on *day* using *configured local time*

Mode

Wireless

Syntax

```
set authorization validity time to time on day-of-week using time-zone
```

Parameters

time

A time, in the format *hh*:*mm* (limited to 15-minute intervals).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

day-of-week

One of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set charging server(s) for the IP-CAN session to *specified values*

Mode

Wireless

Syntax

`set charging server(s) for the IP-CAN session to` *`charging-server-name`*

Parameters

charging-server-name

Names of charging servers that are defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets the charging servers, as specified. To define a charging server, see the *CMP Wireless User's Guide*.

set CSG reporting info to *select value*

Mode

Wireless

Syntax

`set CSG reporting info to` *`info-type`*

Parameters

info-type

- **CHANGE_CSG_CELL** — Indicates that the PCEF reports the user CSG information change to the charging domain when the UE enters/leaves/accesses via a CSG cell.
- **CHANGE_CSG_SUBSCRIBED_HIBRID_CELL** — Indicates that the PCEF reports the user CSG information change to the charging domain when the UE enters/leaves/accesses via a hybrid cell in which the subscriber is a CSG member
- **CHANGE_CSG_UNSUBSCRIBED_HIBRID_CELL** — Indicates that the PCEF reports the user CSG information change to the charging domain when the UE

enters/leaves/accesses via a hybrid cell in which the subscriber is not a CSG member.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sent from the MPE device to the PCEF to request the PCEF to report the user CSG information change to the charging domain.

set custom AVP *name* value to the policy context property *name*

Mode

Wireless

Syntax

`set custom AVP avp-name value to the policy context property property-name`

Parameters

avp-name

An existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

property-name

String that represents the policy context property.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Makes the AVP value accessible throughout the policy context so other policies can access this AVP value as a context property. The context property variable will be set only if this AVP exists in the request and its value is not null.

set custom AVP *name* value to the user property *name* and save *always*

Mode

Wireless

Syntax

`set custom AVP avp-name value to the user property property-name and save save-mode`

Parameters

avp-name

An existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

property-name

String.

Up to 255 characters that represents a user property.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets an AVP value as a User object property to persist between sessions.

set *external field* to # percent of *select type* for *selected* quota

Mode

Cable, Wireless

Syntax

`set` *`field`* `to` *`value`* `percent of` *`type`* `for` *`quota-name`* `quota`

Parameters

field

String name of field in external database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value

New string name of field in external database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

type

One of the following:

- **service-specific**
- **time**
- **total volume**
- **uplink volume**

- **downlink volume**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 the appropriate *CMP User's Guide*. See *Managing Quotas* for information on quotas.

set *external field* to `*value*`

Mode

Cable, Wireless

Syntax

```
set field to `value`
```

Parameters

field

String name of field in external database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value

String.

Value specifies a field in the external database. If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets the value of a field in an external database. This can be an LDAP server or, in wireless mode, 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 the appropriate *CMP User's Guide*.

Examples (Wireless Mode)

```
set Quota Volume to `{User.Quota.Gold.volume}`
```

```
set Last Session to `{Date(2012-10-24 19:54:01)}`
```

set NoOptimization to request

Mode

Wireless

Syntax

```
set NoOptimization to request
```

Parameters

None

Description

Prevents the RAR optimization mechanism from being applied to a request. This functionality allows an RAR request to be sent to the MPE device without being impacted by optimization priorities.

set policy context property *name* to *value*

Mode

Cable, Wireless, Wireline

Syntax

```
set policy context property property-name to value
```

Parameters

property-name

String.

May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set policy context property *name* to the instance name of dynamic quota of *selected*being used

Mode

Wireless

Syntax

`set the policy context` *`property-name`* `to the instance name of dynamic` *`quota-name`* `being used`

Parameters

property-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

quota-name

Name(s) of quota defined in the CMP database.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets the instance ID of the dynamic quota being used for the specified quota profile into a policy context property. See *Managing Quotas* for information on quotas.

set Quota Exhaustion Action to *specified*

Mode

Wireless

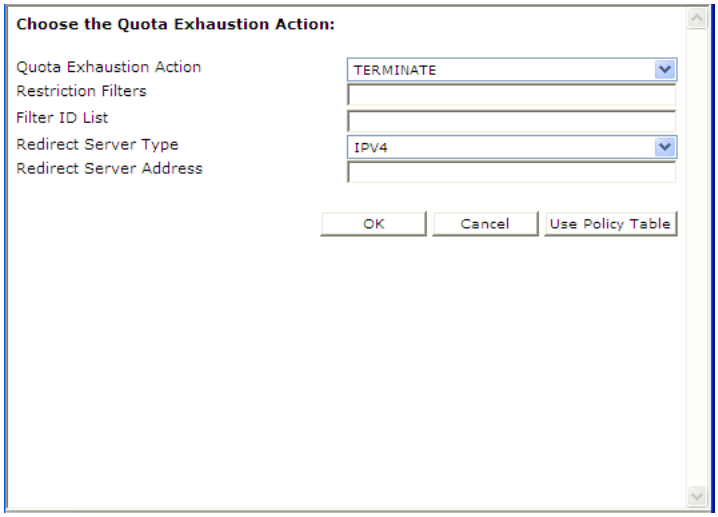
Syntax

`set Quota Exhaustion Action to` *`action`*

Parameters

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** (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** (default), **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

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets the action to take if the subscriber's quota is exhausted. See *Managing Quotas* for information on quotas.

set session revalidation time to # seconds

Mode

Wireless

Syntax

`set session revalidation time to` *`seconds`* `seconds`

Parameters

seconds

A numeric value that specifies time in units of seconds.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the session revalidation time to the number of seconds from when the policy executes.

set session revalidation time to Policy Counter IDs *select names*

Mode

Wireless

Syntax

`session revalidation time to Policy Counter IDs` *`counter -name`*

Parameters

counter -name

- Select **Policy Counter Id** to select one or more policy counter ID defined in the CMP database.
- Select **Policy Counter ID(s)(CSV)** to enter a comma-separated string of policy counter IDs.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Provisions the session revalidation time to the value in the specified policy counter ID or IDs.

set session revalidation time to *time* on *day* using *configured local time*

Mode

Wireless

Syntax

`set session revalidation time to` *`time`* `on` *`day-of-week`* `using` *`time-zone`*

Parameters

time

A time, in the format *hh*:*mm* (limited to 15-minute intervals).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

day-of-week

One of the following:

- **Sunday**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set the *scope* state variable *name* to *now + 0 days* rounded *up* with *same* granularity using *configured local time* and save *always*

Mode

Wireless

Syntax

```
set the scope state variable variable-name to datetime direction duration
granularity1 rounded rounding with granularity2 granularity using time-zone
and save save-mode
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.

- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Note: Any string up to 32 ASCII characters in length if the scope is **subscriber_local** or **session**.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

datetime

One of the following:

- The local date-time **now** (default)
- A policy variable
- A date-time in the format: `yyyy-mm-ddThh:mm:ss+UTCoffset`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

direction

One of the following, indicating future or past:

- **+** (default)
- **-**

duration

Positive integer.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

granularity1

The offset is expressed in this granularity:

- **days** (default)
- **months**
- **hours**
- **minutes**

rounding

One of the following, indicating rounding up or down:

- **up** (default)
- **down**

granularity2

The calculated date-time is expressed in this granularity:

- **same** (default)

- **months**
- **days**
- **hours**
- **minutes**

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets and saves a state date-time variable 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 location of the user equipment. You can specify that the variable is not saved if the policy rejects the message.

set the *scope* state variable *name* to *now* using *configured local time* and save *always*

Mode

Wireless

Syntax

`set the scope state variable variable-name to datetime using time-zone and save save-mode`

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.

- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

datetime

One of the following:

- The local date-time **now** (default)
- A policy variable
- A date-time in the format: `yyyy-mm-ddThh:mm:ss+UTCoffset`

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

time-zone

One of the following:

- **CONFIGURED LOCAL TIME** (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 configured for the user equipment's location

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets and saves a state variable timestamp 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 variable is not saved if the policy rejects the message.

set the *scope* state variable *name* to property *name + multiple of 0 days* rounded *up* with *same* granularity and save *always*

Mode

Wireless

Syntax

```
set the scope state variable variable-name to property property-name
direction multiplier duration granularity rounded rounding withgranularity2
granularity and save save-mode
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

property-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

direction

One of the following, indicating future or past:

- **+** (default)
- **-**

multiplier

One of the following:

- **multiple of** (default) — the duration is added repeatedly until the result is in the future
- **exactly** — the duration is added once

duration

Positive integer.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

granularity

The offset is expressed in this granularity:

- **days** (default)
- **months**

- **hours**
- **minutes**

rounding

One of the following, indicating rounding up or down:

- **up** (default)
- **down**

granularity2

The calculated date-time is expressed in this granularity:

- **same** (default)
- **months**
- **days**
- **hours**
- **minutes**

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Offsets a scope date-time variable, 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 variable is in the future, either the exact offset, or one unit of the offset, is added.
- If the value of the first variable 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 variable is null then the action is ignored.

set the *scope* state variable *name* to `*value*` and save *always*

Mode

Wireless

Syntax

```
set the scope state variable variable-name to `value` and save save-mode
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

value

String.

If you select **Evaluate as expression**, the text in the field is evaluated as an arithmetic expression, and the result is used.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets and saves a state variable. You can specify that the variable is not saved if the policy rejects the message.

set the *scope* state variable *name* to select traffic profile *name* and save *always*

Mode

Wireless

Syntax

```
set the scope state variable variable-name to select traffic profile
retry-profile and save save-mode
```

Parameters

scope

One of the following:

- **subscriber_remote** — Subscribers in the remote SPR.
- **pool** — Subscriber pool defined on the SPR
- **subscriber_local**—Subscribers on the local MPE.
- **session**—Session variables that have a value as long as the session they are associated with is open.
- **policy_evaluation**—Policy evaluation variables that last only for the duration of the policy evaluation cycle.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

variable-name

String.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

retry-profile

Select a profile.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

save-mode

One of the following:

- **always** (default)
- **unless rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets and saves a scope state variable to the specified traffic profile. You can specify that the variable is not saved if the policy rejects the message.

set the user property *name* to *Existing or New* custom AVP *name* and send *always*

Mode

Wireless

Syntax

```
set the user property property-name to property-type custom AVP avp-name
and send send-mode
```

Parameters

property-name

String.

May contain policy rule variables (see *Policy Rule Variables*) to perform parameter substitution within the property name.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

property-type

One of the following:

- **Existing or New** (default)
- **New**

avp-name

Select an existing AVP Name and Vender ID, or an AVP name from an existing Policy Table.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

send-mode

One of the following:

- **always** (default)
- **unless rejected**
- **if rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set threshold to # percent of *granted* quota for service-specific units

Mode

Wireless

Syntax

```
set threshold to extended-percent percent of provided-quota quota for
service-specific units
```

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

provided-quota

One of the following:

- **initial**

- **granted** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set threshold to # percent of *granted* quota for time

Mode

Wireless

Syntax

`set threshold to` *`extended-percent`* `percent of` *`provided-quota`* `quota for time`

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

provided-quota

One of the following:

- **initial**
- **granted** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Sets a threshold, based on a percentage of the time (in seconds) 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.

set threshold to # percent of *granted* quota for volume

Mode

Wireless

Syntax

`set threshold to` *`extended-percent`* `percent of` *`provided-quota`* `quota for volume`

Parameters

extended-percent

An extended, non-integer percentage that can exceed 100 (for example, 102.4%).

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

provided-quota

One of the following:

- **initial**
- **granted** (default)

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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.

set time limit to # seconds

Mode

Cable

Syntax

`set time limit to` *`seconds`* `seconds`

Parameters

seconds

A numeric value that specifies time in units of seconds.

Valid range is 0–1000000000.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Overwrites the time limit in the current message. If there is no TimeLimit object in the current message, a new one is added with the specified value.

set *value* to *Existing or New* custom AVP *name* and send *always*

Mode

Wireless

Syntax

`set value to avp-type custom AVP avp-name and send send-mode`

Parameters

value

String.

This string represents a third-party non-grouped AVP. Check **Evaluate as expression** to evaluate this value as an expression.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

avp-type

Select type of AVP name:

- **Existing** (default)
- **New**

avp-name

An existing AVP Name and Vender ID.

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

send-mode

One of the following:

- **always** (default)
- **unless rejected**
- **if rejected**

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

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 present in the message.

set volume limit to # kilobytes

Mode

Cable

Syntax

`set volume limit to bandwidth kilobytes`

Parameters

bandwidth

A numeric value that specifies bandwidth in bits per second (bps). You can also specify the type to change the rate per second by specifying one of the following:

k	kilobits per second
K	kilobits per second
m	megabits per second
M	megabits per second
g	gigabits per second
G	gigabits per second

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Overwrites the volume limit in the current message. If there is no VolumeLimit object in the current message, a new one is added with the specified value.

subscribe PRA change for *PRA area*

Mode

Wireless mode with the 3GPP mode enabled.

Syntax

`subscribe PRA change for` *`pra`*

Parameters

pra

One of the following:

- **predefined PRA list** — select a defined PRA list
- **manual input** — enter the identifier for the PRA in hexadecimal format or a custom PRA from a subscriber profile in the format *{User.CustomField}*. For information on creating custom fields in subscriber profiles, see your CMP User's Guide.
- **default area** — the last PRA to which the user equipment was subscribed

Click **OK**. If you are using a policy table for this parameter, click **Use Policy Table**, choose the field (column) representing the parameter, and click **OK**.

Description

Subscribes the user equipment to PRA changes in the specified PRA. If **default area** is selected as the definition for the parameter *pra*, subscribes the user equipment to PRA changes in the last subscribed PRA.

unsubscribe PRA change

Mode

Wireless mode with the 3GPP mode enabled.

Syntax

```
unsubscribe PRA change
```

Parameters

None

Description

Unsubscribes from PRA changes.

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.

About Policy Rule Variables

One use of policy rule variables is in an action to perform substitution of textual information into a text message that is being used for some type of logging. The variable is inserted 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 following 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}
```

About Basic Policy Rule Variables

Under certain circumstances an 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 carrier network environment (wireless, cable, or wireline) in which the MPE device is executing
- Whether the information is provisioned on the MPE device or, if present, a Subscriber Profile Repository (SPR) database
- 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)

A number of policy rule variables can provide information about the device for which a policy rule is being executed. Some of these variables are only meaningful in certain modes, while others are available in all modes. Likewise, some of these variables are only available for certain device types, while others are available for all devices.

Basic Policy Rule Variables displays some of the basic policy rule variables that are available.

Basic Policy Rule Variables

Variable Name	**Modes, Protocols, Device Type, and Description**
{***Policy***}	Any mode The name of the policy rule that is being executed.
{***Date***}	Any mode The date when the policy rule is executed, in the following format: ***MMM*[*mm*]*/dd* [*/yyyy*]** where: • *MMM* – Specifies the month. For example: **Feb** • *mm* – Specifies the month numerically. For example: **02** • *dd* – Specifies the day of the month. For example: **09** • *yyyy* – Specifies the year. For example **2017**
{***Time***}	Any mode The time when the policy rule is executed, in the following format: *hh*:*mm*:*ss*.*SSS* where:

Variable Name	Modes, Protocols, Device Type, and Description
	• *hh* – Specifies the hour in 24-hour time. • *mm* – Specifies the minutes. • *ss* – Specifies the seconds. • *SSS* – Specifies the fractional seconds.
{***Conditions***}	Any mode 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 following format: ***variable=value***
{***Device***}	Any mode The name of the device for which the policy rule is being evaluated.
{***DeviceId***}	Any mode The ID of the device for which the policy rule is being evaluated.
{***QosDir***}	Any mode The direction of the flow for which the policy rule is being evaluated, either *Up* (uplink) or *Down* (downlink).
{***Bandwidth***}	Any mode The DOCSIS type of the flow for which the policy rule is being evaluated: • BES • NRTP • RTP • UGS • UGSAD
{***Account.AccountId***}	Wireless The account ID of the account associated with the request.
{***Account.DownstreamLimit***}	Wireless The downstream bandwidth limit of the account associated with the request.
{***Account.EndpointId***}	Wireless The Endpoint ID of the account associated with the request.
{***Account.Entitlements***}	Wireless
{***Account.StaticIpAddresses***}	Wireless
{***Account.Tier.DownstreamLimit***} | {***AccountTier.DownstreamLimit***}	Wireless The downstream bandwidth limit of the tier of the account associated with the request.

Variable Name	**Modes, Protocols, Device Type, and Description**
{***AccountTier.Entitlements***}	Wireless
{***Account.Tier.Name***} | {***AccountTier.Name***}	Wireless The name of the tier of the account associated with the request.
{***Account.Tier.UpstreamLimit***} | {***AccountTier.UpstreamLimit***}	Wireless The upstream bandwidth limit if the tier of the account associated with the request.
{***Account.UpstreamLimit***}	Wireless The upstream bandwidth limit of the account associated with the request.
{***Application.AmIds***}	Wireless
{***Application.EnforcementPt***}	Wireless
{***Application.HDThreshold***}	Wireless
{***Application.Hostnames***}	Wireless
{***Application.IpAddresses***}	Wireless
{***Application.LatencySensitivity***}	Wireless
{***Application.Name***}	Wireless The name of the application associated with the request.
{***Application.SessionClassIds***}	Wireless
{***Device.DownstreamCapacity***}	Any device The downstream bandwidth capacity of the device.
{***Device.FlowCount***}	Any device The number of active flows for the device.
{***Device.Name***}	Any device The name (as defined in the CMP database) of the device.
{***Device.UpstreamCapacity***}	Any device The upstream bandwidth capacity of the device.
{***Element.BackupHostname***}	Any device The host name (or IP address) of the backup 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.
{Element.CapabilitiesSet}	Wireless
{***Element.DiameterIdentities***}	Wireless

Variable Name	**Modes, Protocols, Device Type, and Description**
{***Element.DiameterRealm***}	Wireless
{***Element.DownstreamCapacity***}	Any device 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.
{***Element.UpstreamCapacity***}	Any device The upstream bandwidth capacity of the network element associated {*Element.UpstreamCapacity*} 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.
{***Element.Hostname***}	Any device The host name (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.
{Element.Name}	Any device The name (as defined in the CMP database) 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.
{***Element.NasIdentifiers***}	Wireless
{***Element.OfflineCharging***}	Wireless
{***Element.OnlineCharging***}	Wireless
{***Element.PrimaryOfflineChargingServer***}	Wireless
{***Element.PrimaryOnlineChargingServer***}	Wireless
{***Element.SecondaryOfflineChargingServer***}	Wireless
{***Element.SecondaryOnlineChargingServer***}	Wireless
{***Element.Subtype***}	Wireless
{***Element.UpstreamCapacity***}	Any device

Variable Name	Modes, Protocols, Device Type, and Description
	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.
{***Flow.CurrentOriginalFlowInfo***}	Wireless
{***Flow.OriginalFlowInfo***}	Wireless
{***Flow.TranslatedFlowInfo***}	Wireless
{***Flow.Usage***}	Wireless
{***Quota.Limit.quota_name.ServiceSpecific***}	Wireless
{***Quota.Limit.quota_name.Time***}	Wireless
{***Quota.Limit.quota_name.Volume***}	Wireless
{***Request.AdaptorContext***}	Wireless
{***Request.AppId***}	Wireless
{***Request.CreateTimestamp***}	Wireless
{***Request.CustomAvpValues***}	Wireless
{***Request.DestinationHost***}	Wireless
{***Request.DestinationRealm***}	Wireless
{***Request.EndpointIp***}	Wireless
{***Request.EndTimestamp***}	Wireless
{***Request.ExplictRoute***}	Wireless
{***Request.HandlerKey***}	Wireless
{***Request.MsgType***}	Wireless
{***Request.MSTimeZone***}	Wireless
{***Request.OriginalEvent***}	Wireless
{***Request.PeerIdentity***}	Wireless
{***Request.PolicyOutputResourceEvents***}	Wireless
{***Request.Primary***}	Wireless
{***Request.Reason***}	Wireless
{***Request.ResourceChanges***}	Wireless
{***Request.ServerAction***}	Wireless
{***Request.SessionId***}	Wireless
{***Request.SubscriptionsEnabled***}	Wireless

Variable Name	**Modes, Protocols, Device Type, and Description**
{***Request.Tasks***}	Wireless
{***Request.TriggeredByReAuthPolicyAction***}	Wireless
{***Request.UserIds***}	Wireless
{***Session.CreatedTimestamp***}	Wireless
{***Session.EndpointIp***}	Wireless
{***Session.IMEI***}	Any device This variable expands to the IMEI of the phone for the subscriber or for the equipment associated with the request.
{***Session.IMEISV***}	Any device This variable expands to the IMEISV of the subscriber's phone or equipment associated with the request.
{***Session.LastAcceptedTransactionTime***}	Wireless
{***Session.MSTimeZone***}	Wireless
{***Session.NextBillingDate***}	Wireless 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*.
{***Session.PRASubscriptionInfo***}	Wireless The PRA subscription information associated with the request. It is available when PRA change is subscribed for the current IP-CAN session.
{***Session.PRASubscriptionInfo.PRAIdentifier***}	Wireless The PRA Identifier of the currently subscribed PRA associated with the request. It is available when PRA change is subscribed for the current IP-CAN session.
{***Session.PRASubscriptionInfo.PRAStatus***}	Wireless The PRA status associated with the request. It is available when PRA change is subscribed for the current IP-CAN session. Values accepted are 0 and 1, where 0 indicates that the user equipment is inside the PRA and 1 indicates that the user equipment is outside the PRA.
{Session.Resources}	Wireless
{***Session.Secondary***}	Wireless
{***Session.ServingMcc***}	Wireless The serving Mobile Country Code associated with the request.

Variable Name	Modes, Protocols, Device Type, and Description
{*Session.SessionId*}	Wireless
{*Session.SubscriberPool*}	Wireless
{*Session.UsePoolQuota*}	Wireless
{*Session.UserLocation.CellIdentifier*}	Wireless The Cell Identifier for the subscriber.
{*Session.UserLocation.EUTRANCellIdentifier*}	Wireless The E-UTRAN Cell Identifier for the subscriber.
{*Session.UserLocation.RoutingAreaIdentifier*}	Wireless The Routing Area Identifier for the subscriber.
{*Session.UserLocation.ServiceAreaCode*}	Wireless The Service Area Code for the subscriber.
{*Session.UserLocation.TrackingAreaCode*}	Wireless The Tracking Area Code for the subscriber.
{*Session.UserLocationInfo. GeographicLocationField.LAC*}	Wireless The Location Area Code for the subscriber.
{*Session.UserLocationInfo. GeographicLocationField.RAC*}	Wireless The Routing Area Code for the subscriber.
{*User.AccountId*}	Wireless The account ID of the subscriber associated with the request.
{*User.BillingDay*}	Wireless The Billing Day value of the subscriber associated with the request.
{*User.BillingType*}	Wireless The Billing Type value of the subscriber associated with the request.
{*User.Custom*}	Wireless
{*User.CustomEntity.Pre.ServiceCodes*}	Wireless The value of the Service Code for the current subscriber before Profile Change Notification (PNR).
{*User.CustomEntity.Pre.UsrLocationCodes*}	Wireless The value of the User Location Code value for the current subscriber before Profile Change Notification (PNR).
{*User.CustomEntity.Pre. UsrSessionPolicyCodes*}	Wireless The value of the Session Policy Code for the current subscriber before Profile Change Notification (PNR).
{*User.CustomEntity.ServiceCodes*}	Wireless

Variable Name	Modes, Protocols, Device Type, and Description
	The Service Code value for the current subscriber. If there are multiple codes separate the values with a comma.
{*User.CustomEntity.UsrLocationCodes*}	Wireless The User Location Code value for the current subscriber. If there are multiple codes, separate the values with a comma.
{*User.CustomEntity.UsrSessionPolicyCodes*}	Wireless The Session Policy Code value for the current subscriber. If there are multiple codes, separate the values with a comma.
{*User.customfield*}	Wireless 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.
{*User.DownstreamGuaranteed*}	Wireless
{*User.DownstreamLimit*}	Wireless
{*User.E164*}	Wireless The E.164 phone number of the subscriber associated with the request.
{*User.Entitlement*}	Wireless The Entitlement value of the subscriber associated with the request.
{*User.EquipmentIds*}	Wireless
{*User.IMSI*}	Wireless The IMSI of the subscriber associated with the request.
{*User.IP*}	Wireless The IP address of the subscriber associated with the request.
{*User.IsUnknown*}	Wireless
{*User.MSISDN*}	Wireless The mobile subscriber ISDN of the subscriber associated with the request.
{*User.Pool*} | {*User.Pool.PoolId*}	Wireless The ID of the pool for the subscriber.
{*User.Pool.BillingDay*}	Wireless The pool profile billing day for the subscriber.
{*User.Pool.Entitlement*}	Wireless The pool profile entitlement the subscriber.

Variable Name	**Modes, Protocols, Device Type, and Description**
{***User.Pool.Tier***}	Wireless The pool profile tier for the subscriber pool.
{***User.Pool.custom***}	Wireless A pool profile custom field for the subscriber.
{***User.Pool.State.prop***}	Wireless A pool state property for the subscriber.
{***User.Quota.name.ServiceSpecific***}	Wireless The total initial service-specific events for the subscriber in the quota *name*. This variable applies to subscriber-level and pool-level quota defined on the MPE device.
{***User.Quota.name.Time***}	Wireless The total initial time in seconds for the subscriber in the quota *name*. This variable applies to subscriber-level and pool-level quota defined on the device.
{***User.Quota.name.Volume***}	Wireless The total initial volume (in bytes) for the subscriber in the quota *name*. This variable applies to subscriber-level and pool-level quota defined on the device.
{***User.SIP***}	Wireless The SIP URI of the subscriber associated with the request.
{***User.State.Deltas***}	Wireless
{***User.State.EntityStateType***}	Wireless
{***User.State.New***}	Wireless
{***User.State.prop***}	Wireless The value of a subscriber property, obtained from the SPR database, where *prop* is the property name.
{***User.State.SequenceNumber***}	Wireless
{***User.State.StateMap***}	Wireless
{***User.State.UpdateMode***}	Wireless
{***User.State.Variables***}	Wireless
{***User.Tier***}	Wireless The Tier value of the subscriber associated with the request.
{***User.UpstreamGuaranteed***}	Wireless
{***User.UpstreamLimit***}	Wireless

Variable Name	Modes, Protocols, Device Type, and Description
{User.UserIds}	Wireless

Policy Rule Variables for Quotas and Quota Conventions

The format of a policy rule variable when used with a quota or quota convention is as follows:

object[.*scope*].*attribute*[.*subAttribute*[.*divisor*]]where:

object An object in *Quota Objects*

scope **(optional)** Used to narrow or expand the object. Possible values are:

- **lookupname** — The next value is the name of the pass or plan to look up.
- **lookupgroup** — The next value is the group of the pass (groups are not defined for plans).
- **best** — Selects only the current pass or top-up (if available).
- **next** — Selects only the next pass or top-up after the best.

attribute **(required)** Possible values are:

- **name** — Returns the current plan or pass name.
- **group** — Returns the current pass group (groups are not defined for plans).
- **expirationtime** — Returns any defined expiration time for the best pass unless a scope value of `next` has been used.
- **purchasetime** — Returns any defined purchase time for the best pass (unless a scope value of `next` has been used).
- **activationtime** — Returns any defined activation time for the best pass (unless a scope value of `next` has been used).
- **count** — Returns the number of passes or top-ups in the current selection scope.
- **time** — Returns the sum of the time attribute for the current passes or top-ups scope. This value can have a sub-attribute.
- **volume** — Returns the sum of the volume attribute for the current passes or top-ups scope. This value can have a sub-attribute.
- **upvolume** — Returns the sum of the input-volume (uplink-volume) attribute for the current passes or top-ups scope. This value can have a sub-attribute.
- **downvolume** — Returns the sum of the output-volume (downlink-volume) attribute for the current passes or top-ups scope. This value can have a sub-attribute.
- **servicespecific** — Returns the sum of the service specific attribute for the current passes or top-ups scope. This value can have a sub-attribute.

subAttribute **(required)** Allows limits/used/available to be specified for a counter. If a sub-attribute is defined, a *divisor* may also be defined. Possible values are:

- **limits** — Returns the sum of all unit limits for all passes or top-ups in the current scop.
- **used** — Returns the units used for the ACTIVE pass or top-up.
- **available** — Returns the sum of all units available for all passes or top-ups in the current scope.

divisor A number that tells the system to divide a result by a specified number. Allows values to be specified in higher-division units (days instead of seconds and megabytes instead of bytes).

Policy Variables for Quotas and Quota Conventions defines policy rule variables that can be used with quotas and quota conventions (passes, rollovers, and topups).

Quota Objects defines quota objects that can be used when creating policies that involve quotas and quota conventions.

Policy Variables for Quotas and Quota Conventions

Variable Name	Description
{***allpasses***}	All passes associated with a user.
{***currentPass***}	The current set of passes selected by policy. The default is all passes.
{***currentTopup***}	The current set of top-ups for a user.
{***passes***}	All passes associated with a user.
{***topups***}	All top-ups associated with a user.

Quota Objects

Quota Object	Description
timelimit	The number of seconds with which a pass, plan or top-up started.
totalVolumeLimit	The number of bytes of total volume with which a pass, plan or top-up started.
inputVolumeLimit	The number of bytes of input volume with which a pass, plan or top-up started.
outputVolumeLimit	The number of bytes of output volume with which a pass, plan or top-up started.
serviceSpecificLimit	The number of service-specific events with which a pass, plan or top-up started.
timeConsumed	The number of seconds currently consumed.
totalVolumeConsumed	The number of bytes of total volume currently consumed.
inputVolumeConsumed	The number of bytes of input volume currently consumed.
outputVolumeConsumed	The number of bytes of output volume currently consumed.
serviceSpecificConsumed	The number of service specific units currently consumed.
activationTime	The date-time when the object became active. For plans, the value is null. For roll-overs, the value is the time of the rollover calculation.
expirationTime	The date-time when the MPE device will expire the object.
purchaseTime	The date-time when the object was purchased. For plans and roll-overs, the value is null.

Quota Object	Description
resetTime	The next time the plan has a billing cycle reset. For passes, top-ups and rollovers, the value is null.
name	The name of the pass or plan. For rollovers and top-ups, the name of the associated plan.
field[*name*]	Passes support custom or unknown fields delivered by the SPR. This allows those fields to be accessed and used.
parent	For passes, all the passes that share the same name as the instance. For top-ups, all the top-ups associated with the plan with which that the top-up is associated.
next	The pass or top-up that will be used after the current pass or top-up is exhausted or expired.
best	The best pass/top-up. See *About Quota Conventions* and *About Quotas* for more information.
count	The number of passes or top-ups in the defined collection that are in the Active or Current state.
lookupName	Returns a collection of passes/top-ups for the name of that pass or plan.
lookupGroup	Returns a collection of passes/top-ups for the group of that pass or plan.

Policy Rule Variables for RADIUS

Policy conditions and policy actions can access RADIUS TLVs or VSAs as strings.

The syntax of a TLV variable is as follows:

RADIUS.REQUEST.TLV.*tlv_name_or_id*[.*subfield*]

The syntax of a VSA variable is as follows:

RADIUS.REQUEST.vsa.*vendor_name_or_id*.*vendor_attribute_name_or_id*[.*subfield*]

Where:

- *tlv_name_or_id* — A TLV name (as defined in the RADIUS dictionary) or the unique TLV identifier from the RADIUS standards.
- *vendor_name_or_id* — A vendor's name (as defined in the RADIUS dictionary) or the unique vendor identifier (an integer).
- *vendor_attribute_name_or_id* — A VSA name (as defined in the RADIUS dictionary) or the unique VSA identifier defined by the vendor.
- *subfield* — Either the *n*th field (in order) of the data, or a field name (if the compound structure consists of name-value pairs).

The RADIUS standard does not define a way to support data structures in VSAs, but several vendors have overloaded string definitions to implement CSVs or name-value pairs. (This is sometimes referred to as compound types.) You can use the subfield identifier to parse values out of compound types.

For example, consider the following compound structure from Vendor ID 9, attribute 33:

```
agordon;Pssw3RD!?;GoldPlan
```

The variable `RADIUS.REQUEST.vsa.9.33.2` returns the string `Pssw3RD!?` because `Pssw3RD!?` is the second field in the compound structure.

If the compound structure is defined as follows:

```
user=agordon,passwd=Pssw3RD!?,access=GoldPlan
```

The variable `RADIUS.REQUEST.vsa.9.33.user` returns the string `agordon` because `agordon` is associated with the field name.

See *RADIUS Policy Rule TLV Variables* for a list of the RADIUS policy rule variables that are available when correlating a RADIUS session with a Gx Plus or Gx-Lite session.

RADIUS Policy Rule TLV Variables

Variable Name	**Description**
{***RADIUS.REQUEST.TLV.User-Name***}	The name of the user account. A string value in UTF-8 format.
{***RADIUS.REQUEST.TLV. NAS-Port-Type***}	The port type used by the GGSN. An integer value greater than 0.
{***RADIUS.REQUEST.TLV. NAS-Identifier***}	The unique identifier of the NAS that originated the request. A byte value.
{***RADIUS.REQUEST.TLV. NAS-IP-Address***}	The IP address of the GGSN that is communicating with the MPE device. A valid address in IPv4 format.
{***RADIUS.REQUEST.TLV. Framed-IP-Address***}	Mandatory field. The IP address of the user account. A valid address in IPv4 format.
{***RADIUS.REQUEST.TLV. Acct-Session-Id***}	Mandatory field. The unique Accounting ID to make it easy to match start and stop record in a log file. The start and stop records for a given session must have the same Acct-Session-Id. An Accounting-Request packet must have an Acct-Session-Id. A string value in UTF-8 format.
{***RADIUS.REQUEST.TLV. Called-Station-Id***}	The identifier for the target network (the APN). A byte value.
{***RADIUS.REQUEST.TLV. Calling-Station-Id***}	The identifier for the MS (the MSISDN). A byte value.
{***RADIUS.REQUEST.TLV.3GPP-IMSI***}	The IMSI for this user. A 15-byte value.
{***RADIUS.REQUEST.TLV. 3GPP-IMEISV***}	The International Mobile Equipment ID (IMEI) and software version.
{***RADIUS.REQUEST.TLV. 3GPP-IMSI-MCC-MNC***}	The Mobile Country Code (MCC) and Mobile Network Code (MNC) parsed from the user IMSI. A two- and three-byte value.
{***RADIUS.REQUEST.TLV. 3GPP-SGSN-Address***}	The SGSN IP address. A valid address in IPv4 format.

Variable Name	Description
{*RADIUS.REQUEST.TLV. 3GPP-SGSN-MCC-MNC*}	The MCC and MNC parsed from the location information of the SGSN. A two- and three-byte value.
{*RADIUS.REQUEST.TLV. 3GPP-GGSN-Address*}	The GGSN IP address. A valid address in IPv4 format.
{*RADIUS.REQUEST.TLV. 3GPP-GGSN-MCC-MNC*}	The MCC and MNC parsed from the location information of the GGSN. A two- and three-byte value.
{*RADIUS.REQUEST.TLV. 3GPP-CG-Address*}	The associated charging gateway (CG) IP address. A valid address in IPv4 format.
{*RADIUS.REQUEST.TLV. 3GPP-User-Location-Info*}	The location information of the user equipment. A byte value.
{*RADIUS.REQUEST.TLV. 3GPP-GPRS-Negotiated-QOS-Profile*}	The QoS profile negotiated by the GGSN. A string value in UTF-8 format.
{*RADIUS.REQUEST.TLV. 3GPP-Charging-Characteristics*}	For a GGSN, the charging characteristics for this PDP context received in the Create PDP Context Request Message (in R99 and later releases). A two-character value in UTF-8 format.
{*RADIUS.REQUEST.TLV. 3GPP-Charging-Id*}	For a GGSN, the charging ID for this PDP context. This, together with the GGSN IP address, constitutes a unique identifier for the PDP context. An unsigned integer value.
{*RADIUS.REQUEST.TLV. 3GPP-PDP-Type*}	For a GGSN, the type of PDP context (IP or PPP). An unsigned integer value.
{*RADIUS.REQUEST.TLV. 3GPP-RAT-Type*}	Indicates with Radio Access Technology (RAT) type is currently serving the user equipment (UE). A byte value.
{*RADIUS.REQUEST.TLV.3GPP-NSAPI*}	For a GGSN, the particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion. A character value in UTF-8 format.
{*RADIUS.REQUEST.TLV. 3GPP-Selection-Mode*}	For a GGSN, the selection mode for this PDP context received in the Create PDP Context Request message. A character value in UTF-8 format.
{*RADIUS.REQUEST.TLV. 3GPP-MS-Timezone*}	The offset between universal time and local time, in 15-minute increments, of where the MS/UE currently resides.

Chapter 24

Managing Policy Rules

Topics:

- *Displaying a Policy.....506*
- *Deploying Policy Rules.....506*
- *Modifying and Deleting a Policy.....509*
- *Policy Templates.....510*
- *Managing a Policy Group.....512*
- *Importing and Exporting Policies, Policy Groups, and Templates.....518*

Policy rules are created and saved within the CMP database and then deployed to MPE devices. The CMP system lets you create and modify the details within policy rules, 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*. This chapter 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 navigation pane, select **Policy Library**.
   The content tree displays a list of policy library groups; the initial group is **ALL**. If a policy references another policy or policy group, a gear icon (⚙) appears next to the policy name in the content tree.
2. From the content tree, select the policy.
   The policy is displayed. *Figure 5: Sample Policy Description* shows an example.

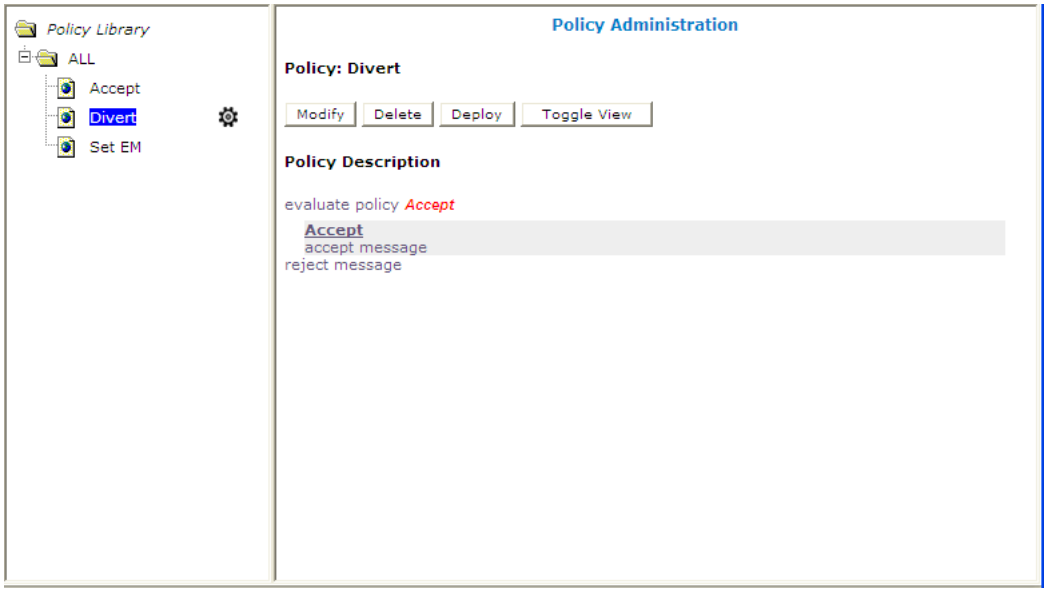


Figure 5: Sample Policy Description

You can choose from two logical views of policy conditions:

- A tree format (shown)
- A Boolean expression format similar to SQL

To switch between one views, click **Toggle View**.

If the policy evaluates a policy group, the policies in the group (which are referenced policies) are displayed. Click a policy name to see details of that policy. If a referenced policy 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 policy database to an MPE device. After a policy is deployed, the rules defined within the policy or policy group are used as decision-making criteria by the MPE device.

Figure 6: Policy Deployment shows how policies P1 through P7 are created in the CMP database 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.

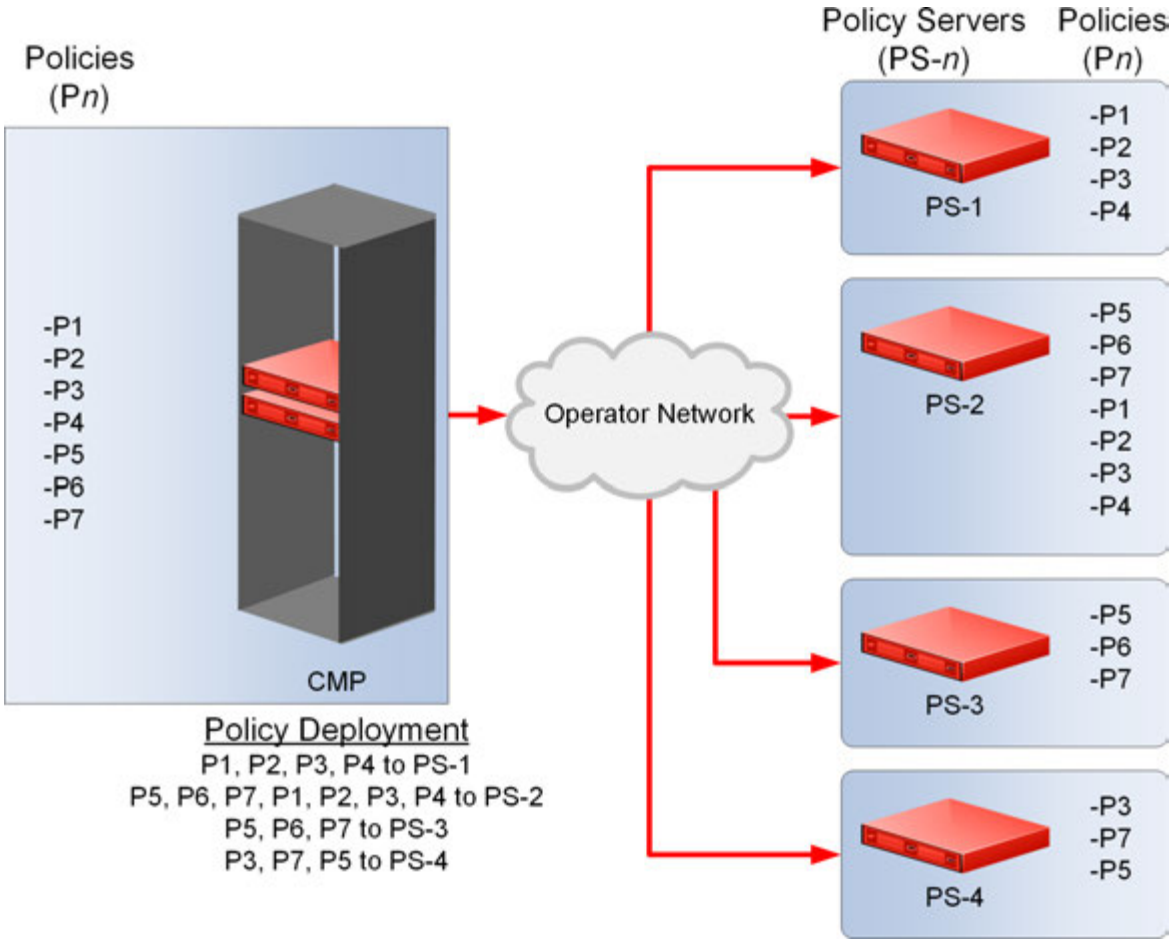


Figure 6: Policy Deployment

Figure 7: 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.

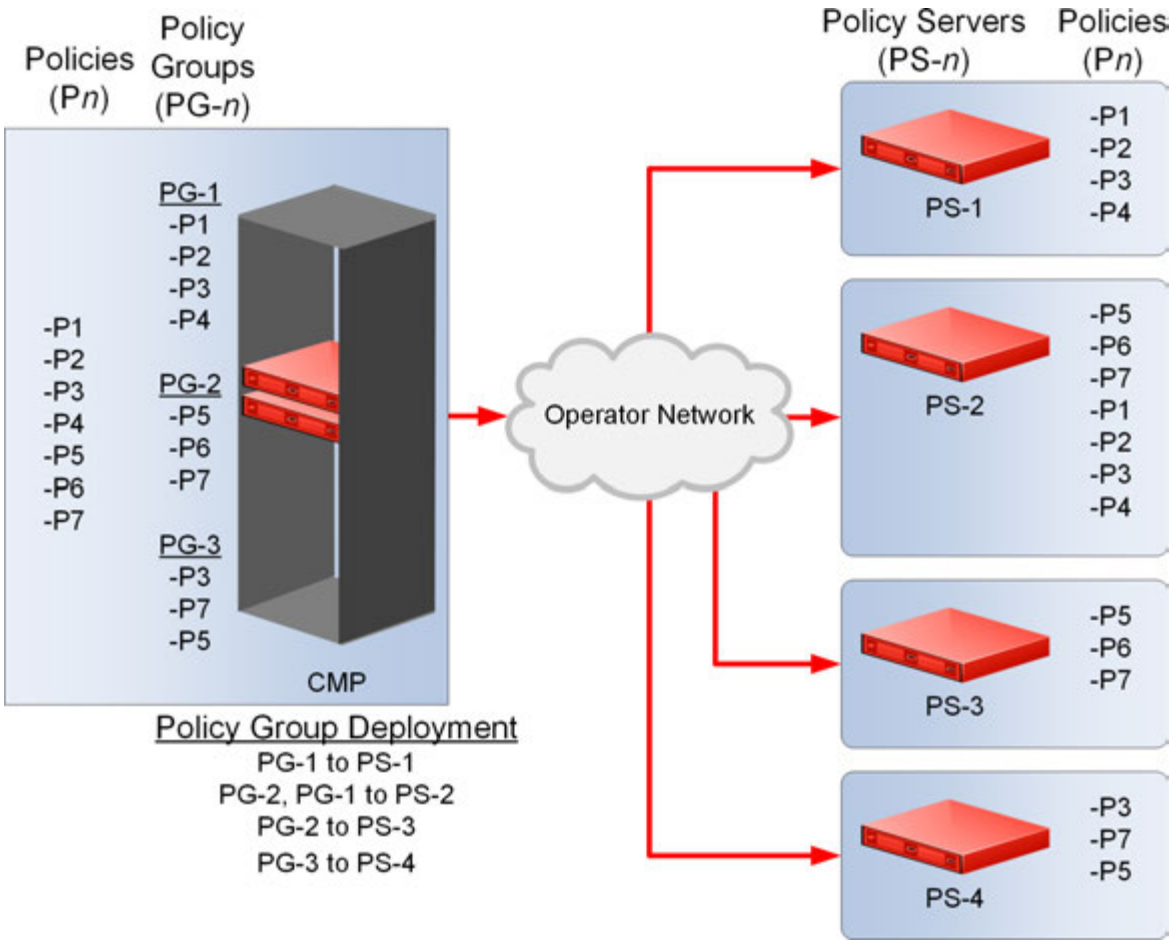


Figure 7: Policy Group Deployment

When you first create a policy rule, that rule exists only within the CMP database. After 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 8: Policy Redeployment shows that when a policy (P3) is modified, its associated groups (PG-1 and PG-3) are redeployed automatically.

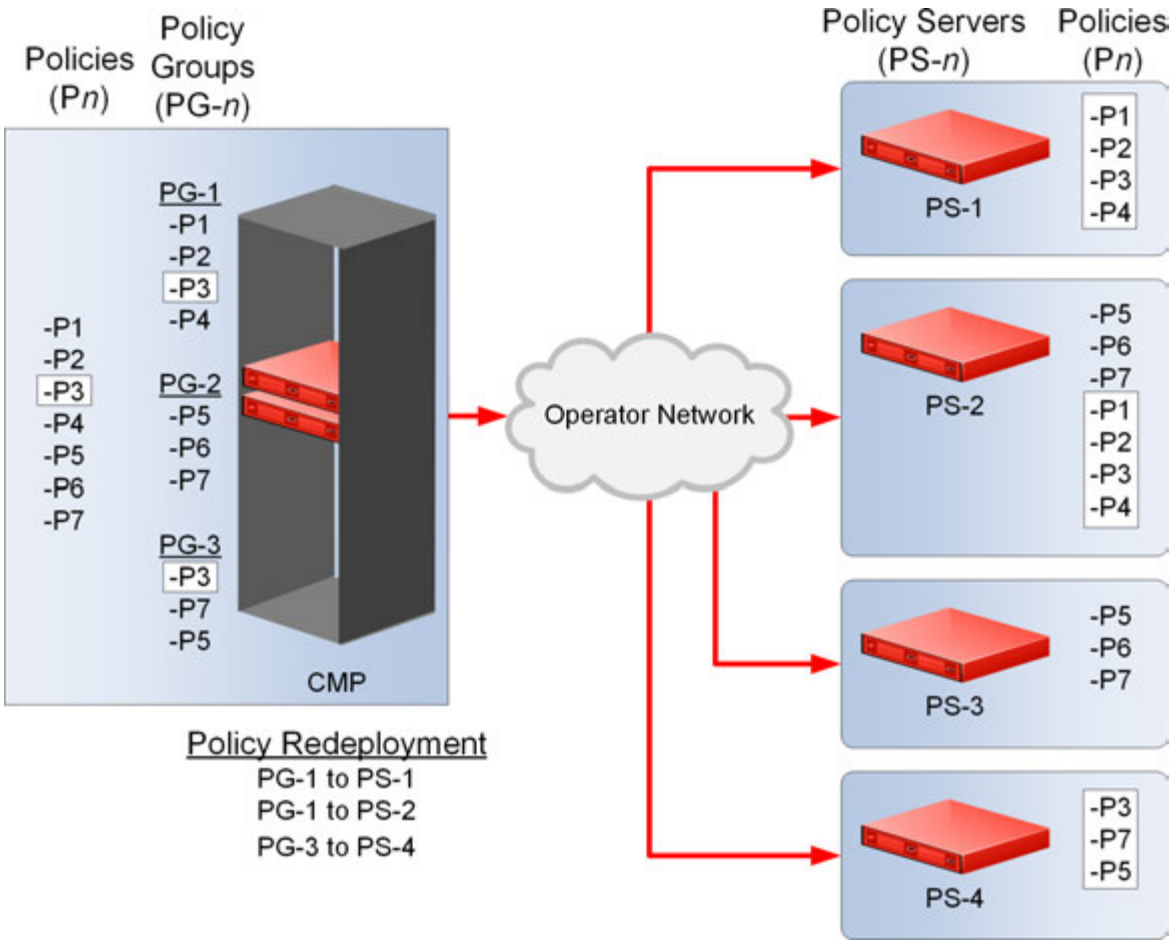


Figure 8: Policy Redeployment

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 a 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 policy information.

   See *Creating a Policy* for details on the fields within the policy wizard.
6. Click **Finish**.

The policy is modified. The modified policy is now ready to be added to a policy group (see *Adding a Policy or a Policy Group 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 in the CMP database, it can be redeployed at a later date if needed. If a policy is no longer needed, it can be deleted from the CMP database as well.

Note: Deleting a policy from the CMP database 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**.

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

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 system 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 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. Click **Create Template**.
   The **Create New Policy Template** window opens.
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, then save the policy as a policy template.
5. Edit the policy information from one or more of the policy wizard pages.
   See *Creating a Policy* for details on the fields within the policy wizard.
6. Click **Finish**.

The policy template is created.

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 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 showing the last step of the template creation process.
5. Click **Back** to return to the page you want to edit and modify the information.
6. Click **Finish** to save the modified template.

The template is modified.

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**.

   A confirmation message displays.
3. Click **OK** to delete the policy template.

The policy template is deleted.

Managing a Policy Group

The CMP system lets you create policy groups. Policy groups are an organizational aid that provide for flexible policy management, deployment, and execution. You save policies to a group in the order in which you want an MPE device to apply 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. You can also group, or nest, policy groups.

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. Click **Create Group**.
   The group naming field opens in the work area.
4. Enter the name to assign to the new group.

   The name can be up to 64 characters long and must not contain quotation marks (") or commas (,).
5. Click **Save**.

The new group information is saved to the CMP database and displayed in the content tree.

Adding a Policy or a Policy Group to a Policy Group

After you create a policy group, you can add policies to the group. You can also add policy groups to a policy group.

Note: It is recommended that you only nest policy groups two levels deep.

To add one or more policies or policy groups 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 or policy group.
   The **Policy Administration** page opens in the work area, listing the policies and policy groups currently in the group.
3. Click **Modify**.
   The **Policy Administration** page opens in the work area.
4. Click **Add**.
   A window opens, displaying the policies and policy groups available.
5. You can optionally filter the list by policies or policy groups. From the list, select **Policy** to display policies, **Group** to display policy groups, or **All** (default) to list both policies and policy groups.
6. Select the policy or group to add to this group and click **Add**. Use Shift/click to select multiple policies or policy groups. By default policies and policy groups are added after the first item in the group; to change the insert position, change the value in the **Location** field.
   The policies or policy groups are added to the policy group in the specified location and the window closes.

   Note: Policies or policy groups are applied to messages in the order in which they appear in the policy group. You can change the sequential order (see *Changing the Sequence of Deployed Policies or Policy Groups*).

7. Click **Save**.

The added policies and policy groups are displayed in the policy group tree. 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 synchronized with the CMP database.

Managing Analytics Data Stream Generation for a Policy Group

You can enable or disable generation of an analytics data stream (ADS) for all policies in a group. See the *Analytics Data Stream Reference* for more information on the Oracle Communications Policy Management Analytics product.

To enable ADS generation for all policies in a group:

1. Enable the ADS feature by configuring the **Manage Analytic Data** management option. See the appropriate *CMP User's Guide* for more information.
2. 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**.
3. From the content tree, select the group of interest.
   The **Policy Administration** page opens in the work area, listing available policies.

4. On the **Policy Administration** page, click **Enable Analytics**.
   ADS generation is configured for all policies in the group.

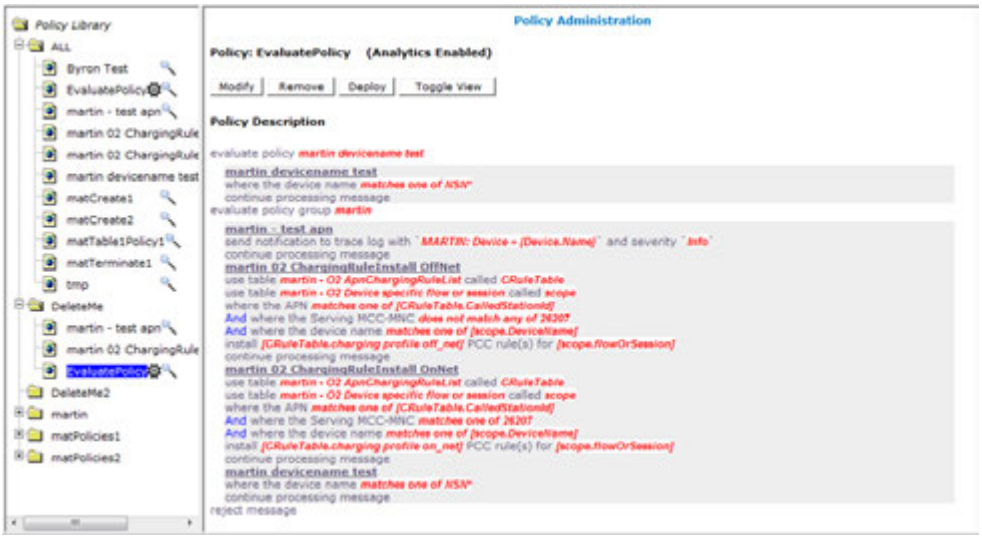
   Note: To disable ADS generation for a group, select the group and click **Disable Analytics** from the **Policy Administration** page. ADS generation is disabled for all policies in the group.

Removing a Policy from a Policy Group

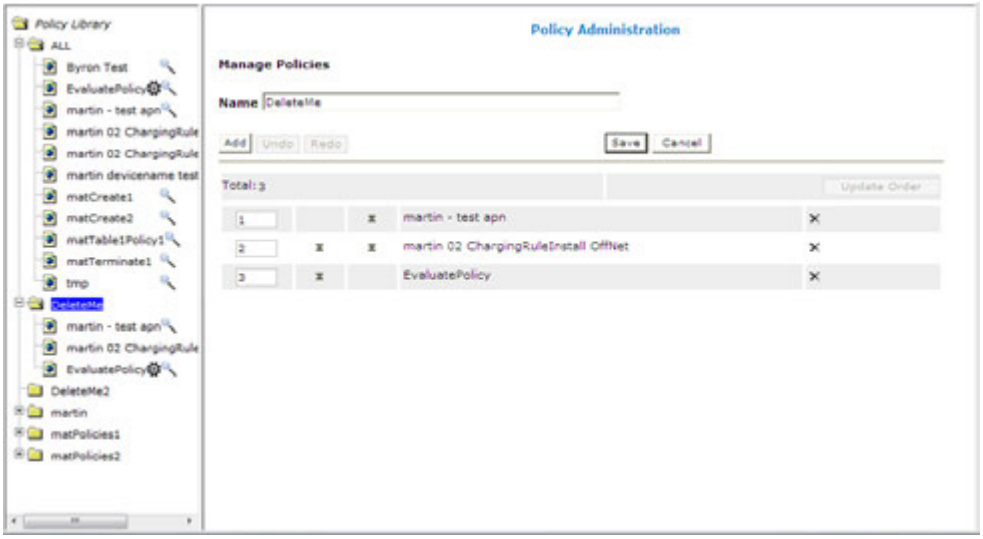
Removing a policy from a policy group that has been saved to the CMP database only removes the policy from the selected policy group. The policy remains in the **ALL** group, as well as any other group to which it had been added. (To remove a policy from all groups in the Policy Library, see *Removing 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 policy group.
   The **Policy Administration** page opens in the work area, listing the policies it contains.
3. Remove the policy using one of the following methods:
   - From the content tree, select the policy within the policy group; the profile information for the policy is displayed. Click **Remove**.



   - From the content tree, select the policy group and click **Modify**. Select the remove icon, located to the right of the policy you want to remove.



The modified policy group is redeployed, ensuring that the MPE devices are resynchronized with the CMP database.

Note: If the policy group has never been deployed, you can now deploy it to MPE devices (see *Deploying a Policy or Policy Group to MPE Devices*).

Removing a Policy Group

Removing a policy group removes the policy group from all policy groups to which it has been added.

To remove 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.
   The **Policy Administration** page opens in the work area, listing policies and policy groups.
3. From the content tree, select the policy group; the profile information for the group is displayed. Click **Delete**.
   A confirmation message displays.
4. Click **OK** to delete the policy group.

The policy group is removed from the CMP database. Any policy groups that contained the deleted policy group are redeployed, ensuring that the MPE devices are synchronized with the CMP database.

Changing the Sequence of Policies or Policy Groups Within a Policy Group

The order in which policies or policy groups 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 or policy groups, both inside and outside of a policy group.

To change the order of the policies or policy groups 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 policy group.
   The **Policy Administration** page opens in the work area, displaying policies or policy groups in their current sequential order.
3. Click **Modify**.
   The **Manage Policies** page opens.
4. Use any of the following options to change the sequence of policies or policy groups within the group:
   - Use the (top) and (bottom) icons, located to the left of policies or policy groups. The (top) icon moves the item it to the top of the list. The (bottom) icon moves the item it to the bottom of the list.
   - Drag and drop policies or policy groups to a different position in the sequence.
   - Change the sequence numbers, located to the left of policies or policy groups. Click **Update Order** to refresh the display.
   - Optionally, you can click **Undo** or **Redo** to step back and forth through your changes.
5. Click **Save**.

The modified policy group is redeployed, ensuring that the MPE devices are resynchronized with the CMP database.

Note: If the policy group has never been deployed, you can now deploy it to MPE devices (see *Deploying a Policy or Policy Group to MPE Devices*).

Displaying Details of All Policies in a Policy Group

To display the details of all policies in 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.
   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. Click **Cancel**.

The details of all policies in the group displays.

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 or policy group to deploy.
   The **Policy Administration** page opens in the work area, listing the policies it contains.
3. 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 target MPE devices or policy server groups.

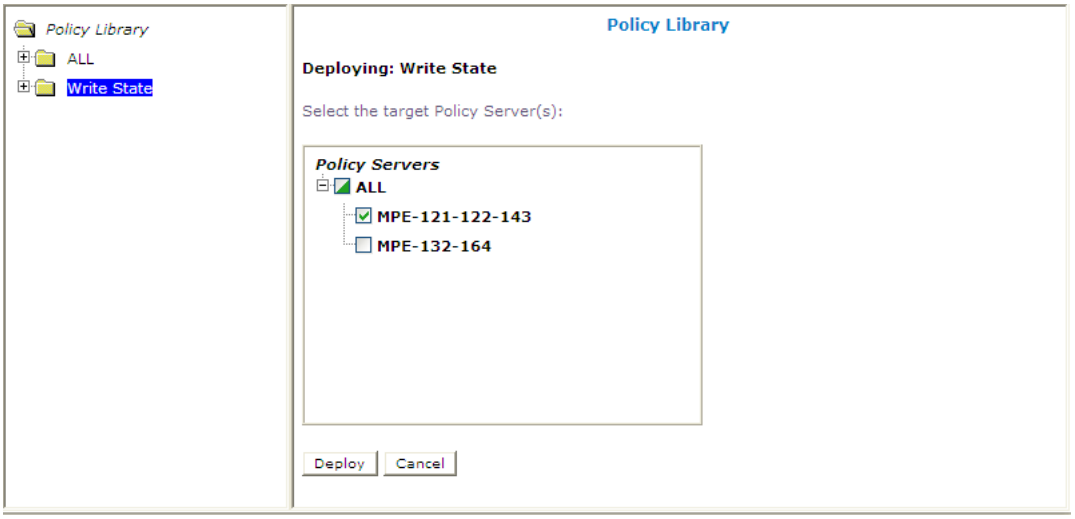


Figure 9: Policy server selection window

An icon indicates whether you have selected some (◢) or all (☑) MPE devices to which to deploy the policy or policy group.

5. Click **Deploy**.
   A confirmation message displays followed by a list of MPE devices to which the policy or policy group was deployed.

The policy information is saved to each selected MPE device.

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 or 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. Select the **Policies** tab.
4. Click **Modify**.
   The **Manage Policies** page opens.
5. Click (scissors) located to the right of the policy or policy group that you want to remove.
   The policy or policy group is removed from the list.
6. Repeat step 5 as required.
7. click **Save**.
   A confirmation message displays.

The policy or policy group is removed from the MPE device. The policy or policy group is redeployed to the MPE device, minus the removed policy or policy group.

Changing the Sequence of Deployed Policies or Policy Groups

Changing the sequential order of deployed policies or policy groups is performed directly on an MPE device using the **Policy Server Administration** page.

To change the sequential order of policies or 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. Select the **Policies** tab.
4. Click **Modify**.
   The **Manage Policies** page opens in the work area.
5. Use any of the following options to change the sequential positioning of the policies or policy groups:
   - Use the (top) and (bottom) icons, located to the left of policies or policy groups. The (top) icon moves the item it to the top of the list. The (bottom) icon moves the item it to the bottom of the list.
   - Drag and drop policies or policy groups to a different position in the sequence.
   - Change the sequence numbers, located to the left of policies or policy groups. Click **Update Order** to refresh the display.
   - Optionally, you can click **Undo** or **Redo** to step back and forth through your changes.
6. Click **Save**.

The policies or 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 database for inspection or backup purposes. For mor information about importing and exporting, see the *CMP User's Guide*.

Chapter 25

Managing Policy Tables

Topics:

- *About Policy Tables.....520*
- *About Data Matching.....521*
- *Policy Table Case Study.....523*
- *Creating Policy Tables.....528*
- *Viewing Policy Tables.....530*
- *Associating Policy Tables with a Policy Rule...530*
- *Associating a Parameter with a Policy Table Column.....531*
- *Modifying Policy Tables.....531*
- *Deleting Policy Tables.....532*

This chapter describes how to create, modify, delete, and view policy tables, which are independent objects that you can use to capture differences in policy structures.

You can manage multiple policies with small differences by abstracting the differences into tables. The process of modifying the policies, or creating new, similar policies then becomes a matter of modifying the policy table, which is simpler and less prone to error.

About Policy Tables

In practical use, many policies are very similar, having only small differences between them. Policy tables are an available option in the policy wizard. A policy table abstracts the differences between related policies.

Using a policy table instead of creating many similar policies makes the tasks of adding new policies, modifying existing sets of policies, and checking consistency among related policies simpler and less prone to error.

Policy tables resemble database tables, and contain the following elements:

- Table name
- Table description
- Column definitions

  Every column has a definition that contains a name, data type, and indication if the column is a key column. Every entry in the column must have the same data type. Any data associated with a message, including fields (such as a quota or RAT type) and sub-fields (such as a user account ID or tier name), can be used as a key.

- Policy variable (for key columns only)

  Used to obtain the value from the policy context when using the policy table to look up a row.

- Data

  The contents of the table cells. (Blank cells are not allowed in a policy table.)

Each row in a policy table can be thought of as a scenario, and each row can replace a policy. Substitutions in policy condition and action parameters can include the values in a specified policy table.

Table 3: Example of a Policy Table shows an example of a simple policy table. The first column lists one or more access point names (APN), and is the key column. The second column contains a PCC rule that will be installed as part of the execution of a policy. The third column contains one or more PCC rules that will be removed as part of the execution of a policy. The second and third columns must contain names of PCC rules defined as traffic profiles in the CMP database.

Table 3: Example of a Policy Table

APN	Install	Remove
apn1.com	pcc_rule_1	pcc_default_1, pcc_basic
apn2.com	pcc_rule_2	pcc_default_2, pcc_basic
apn3.com, apn4.com	pcc_rule_1	pcc_default_1
apn5.com, apn6.com	pcc_rule_2	pcc_default_2

Each policy can have zero or more policy tables. To support the use of multiple policy tables, policies refer to a policy table using an alias. Each policy can use a different alias for the same policy table. For example, a policy table named **PCC rules to install and remove, based on APN** can be referred to in a policy as `pcc_rules`. Policies can use table cells addressed as *table_name.column_name*.

The following policy rule uses the defined policy table. The italicized text represent substitutions. The table references begin with pcc_rules.

```
use table ‘PCC rules to install and remove, based on APN‘ called ‘pcc_rules‘
where the request is modifying an existing session
     and where the session is a credit control session
     and where the requested quota is one of Bucket Exceeded,OS_no_TV_volume
     and where the quota usage reporting reason is one of validity time expired
     and where the APN matches one of pcc_rules.apn
     and where the user Custom1 matches one of 101
install pcc_rules.install PCC rules for flow
remove pcc_rules.remove PCC rules
send notification to syslog with
`100;{User.MSISDN};{User.AccountId};{User.IMSI};{Session.IMEI};{Date} {Time};
Info GalacTel : You have a new 500 minutes to enjoy your mobile Internet offer.
 Beyond that the flow will be reduced.; {Date} {Time};{Date}
{Time};{User.Custom1};{User.BillingDay}` and severity `Emergency`

accept message
```

The use of policy tables is not required. The decision to use a policy table may arise after you have created a series of production policy rules, if you notice that the policies differ only in a few small ways.

About Data Matching

When policy tables are evaluated, values in key column fields are evaluated against information parsed out of messages or retrieved from external data sources and stored in the policy context. For example, fields such as entitlements or multivalued custom fields can be retrieved from a subscriber profile stored in an SPR system. By default, values are evaluated as single entities, and matches must be exact. However, you can optionally specify that values be treated as a set of delimited values and evaluated as multi-value fields, and accept as a match a complete or subset match of the values within the key column field. The first row with a successful match is used. You can define up to 50 values within one field.

Using multi-value keys makes a policy table more flexible and reduces the number of rows needed.

Policy Matching Operations shows the available matching operations between policy context data and key column cell values. Data matching is case insensitive.

Note: If no delimiter is defined, the data in the key column cell is used as is and not parsed.

Example of Data Matching provides a simple example of data matching and compares the results from each matching operation.

Policy Matching Operations

Operation	Description and Example
Wildcard	One or more wildcarded values in the key column cell are compared to the values in the policy context data. If there is any match, the row is matched. The asterisk (*) character represents any number of characters, and the period (.) character represents any single character.

Operation	Description and Example
	`child*,student*,family..`
Policy Context Set Contains All Multiple Valued Key Column	A multivalued key column cell is compared to multivalued policy context data. If the policy context data is a subset of the key column cell data, the row is matched. `gold|silver|bronze`
Multiple Key Column Set Contains Single Value Context	A multivalued key column cell is compared to single-value policy context data. If the policy context data is a subset of the key column cell data, the row is matched. (The policy context data is evaluated as a string, and must be included in the key column cell data.) `weekday|weekend`
Multiple Policy Context Set Contains Single Value Key Column	A single-value key column cell is compared to multivalued policy context data. If the key column cell data is a subset of the policy context data, the row is matched. (The key column cell data is evaluated as a string, and must be included in the policy context data.) `gold`
Key Column Value Set Contains Any Multiple Valued Context	A multivalued key column cell is compared to multivalued policy context data. If any values within the key column cell data match any values of the policy context data, the row is matched. `GalacTel,GalacTel Plus,GalacTel Premium,GalacTel Business`
Equivalence	A multivalued key column cell is compared to multivalued policy context data. If the key column cell data matches the policy context data, the row is matched. (The order does not matter.) `Gold!EU`
Key Column Set Contains All Multiple Valued Policy Context	A multivalued key column cell is compared to multivalued policy context data. If the key column cell data is a subset of the policy context data, the row is matched. `Gold!EU!Weekend`

Example of Data Matching

As an example of how matching operations work, consider a Policy Table with the following multirow key column:

Data.UserLevel
Gold,Silver
Bronze
Gold,Silver,Bronze
GO*,SILVE.

If the delimiter is turned off (not selected), then any matching algorithm will simply compare the policy context value to the entire key column cell. For example, the first row of the column is evaluated as the string `Gold,Silver` and not as two values. If the policy context has a UserLevel of `Bronze` then the second row will match. However, the third row would not match as it would be seen as `Gold,Silver,Bronze` and compared to `Bronze` not an exact match.

Key Column Set Contains All Multiple Valued Policy Context will only return true if the key column cell contains all of the policy context information. For example, if the policy context has a UserLevel of `Silver,Bronze` then the first row of the column will not match, but the third row will.

Policy Context Set Contains All Multiple Valued Key Column is the opposite of the previous matching operation: The policy context information must contain all of the key column cell values. For example, if the policy context has a UserLevel of `Silver,Bronze` then only the second row of the column will match.

Key Column Value Set Contains Any Multiple Valued Context means that if any values in the key column cell and the policy context information are the same, then the match is true. For example, if the policy context has a UserLevel of `Silver,Bronze` then every row of the column will match, as each row contains the same information as the Policy Context. (The policy will use the first row matched.)

Equivalence means that all values must be exact. The order does not matter; that is, `Silver,Gold` and `Gold,Silver` are the same. However, all set information must be in both values. For example, if the policy context has a UserLevel of `Silver,Bronze` then it does not match any row in the table as the two sets are never exact. However, if the policy context has a UserLevel of `Silver,Gold,Bronze` then the third row of the column will match, since the order does not matter. (If the delimiter were turned off then the operation would perform a string comparison of `Silver,Gold,Bronze` with `Gold,Silver,Bronze` which is not a match.)

Multiple Key Column Set Contains Single Value Context will give the same results as **Key Column Set Contains All Multiple Valued Policy Context**. However, the policy context is not separated into delimited values.

Multiple Policy Context Set Contains Single Value Key Column will give the same results as **Policy Context Set Contains All Multiple Valued Key Column**. However, the key column cell values are not separated into delimited values, only the policy context (if possible).

Wildcard is the intersection of the policy context with the key column call values, taking into account wildcards. For example, if the policy context has a UserLevel of `Gold` then the first and fourth row of the column will match. The same is true if the policy context has a UserLevel of `Silver` instead. However, if the policy context has a UserLevel of `GOLDEN` then only the fourth row will match.

Policy Table Case Study

The following case study is derived and simplified from actual carrier policies, and illustrates how a large set of policies can be consolidated using a policy table.

A wireless carrier named Example Inc. offers three monthly data usage plans for its subscribers. The monthly quota levels are 100 MB, 2 GB, and 150 GB. Seven policies are used to capture the business logic for each usage plan, as follows:

- When subscribers near their monthly quota limit, the carrier (1) sends an SMS notification.

- When subscribers reach their monthly quota limit, the carrier (2) sends an SMS notification, (3) sets an additional quota (at an additional price), (4) sets a new warning threshold, and (5) sets a new limit threshold.
- When subscribers reach the additional limit, the carrier (6) sends an SMS notification and (7) throttles additional usage to 64 kbps.

The rules for each usage plan are collected in a policy group, so to support the three plans there are three policy groups. Finally, triggering policies determine which policy group to execute based on the entitlement of the subscriber.

The names the carrier uses for the groups, and the names of the policies each contains, are as follows. The groups are named for the data plans (100 MB, 2 GB, and 100 GB), and the policies are named for the data plans and the actions each policy performs.

Group Name	Policy Name
Quota 100 MB	Quota 100 MB send 70 percent SMS
	Quota 100 MB send 100 percent SMS
	Quota 100 MB additional quota send 100 percent SMS
	Quota 100 MB set 70 percent volume threshold
	Quota 100 MB set 100 percent volume threshold
	Quota 100 MB additional quota set 100 percent volume threshold
	Throttle 64 kbps 100 MB
Quota 2 GB	Quota 2 GB send 90 percent SMS
	Quota 2 GB send 100 percent SMS
	Quota 2 GB additional quota send 100 percent SMS
	Quota 2 GB set 90 percent volume threshold
	Quota 2 GB set 100 percent volume threshold
	Quota 2 GB additional quota set 100 percent volume threshold
	Throttle 64 kbps 2GB
Quota 100 GB	Quota 100 GB send 90 percent SMS
	Quota 100 GB send 100 percent SMS
	Quota 100 GB additional quota send 100 percent SMS
	Quota 100 GB set 90 percent volume threshold
	Quota 100 GB set 100 percent volume threshold
	Quota 100 GB additional quota set 100 percent volume threshold
	Throttle 64 kbps 100 GB

Comparing the triggering policies shows that they differ only in the name of the entitlement to match and the policy group to execute:

- Trigger Policy: Evaluate 3G Volume Quota Group 100 MB

```
where the ENTITLEMENTS is contained in Match Lists Ent 100MB Quota

evaluate policy group Quota 100MB
```

- Trigger Policy: Evaluate 3G Volume Quota Group 2 GB

```
where the ENTITLEMENTS is contained in Match Lists Ent 2GB Quota

evaluate policy group Quota 2GB
```

- Trigger Policy: Evaluate 3G Volume Quota Group 100 GB

```
where the ENTITLEMENTS is contained in Match Lists Ent 100GB Quota

evaluate policy group Quota 100GB
```

Similarly, comparing the corresponding policies in different groups shows that they are mostly the same, with only a few isolated differences:

- Group: Quota *100MB*; Policy: Quota *100MB* send *70* percent SMS

```
where the user is using greater than or equal to 70 percent and less than 100
percent of volume for DP_QUOTA.100MB quota
And where the event trigger is one of USAGE_THRESHOLD_REACHED
send SMS `You have consumed 70 % of your total quota allotted on Example Inc.`
to user. Request delivery receipt `default`.
send notification to syslog with `SMS
70%;{User.E164};{User.Custom5};{User.Custom6};GOLD;{User.Entitlement};You have
consumed 70 % of your total quota allotted on Example Inc.` and severity `Info`
Advanced: set values for QoS and Charging parameters to
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

continue processing message
```

- Group: Quota *2GB*; Policy: Quota *2GB* send *90* percent SMS

```
where the user is using greater than or equal to 90 percent and less than 100
percent of volume for DP_QUOTA.2GB quota
And where the event trigger is one of USAGE_THRESHOLD_REACHED
send SMS `You have consumed 90 % of your total quota allotted on Example Inc.`
to user. Request delivery receipt `default`.
send notification to syslog with `SMS
90%;{User.E164};{User.Custom5};{User.Custom6};GOLD;{User.Entitlement};You have
consumed 90 % of your total quota allotted on Example Inc.` and severity `Info`
Advanced: set values for QoS and Charging parameters to
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

continue processing message
```

- Group: Quota *100GB*; Policy: Quota *100GB* send *90* percent SMS

```
where the user is using greater than or equal to 90 percent and less than 100
percent of volume for DP_QUOTA.100GB quota
And where the event trigger is one of USAGE_THRESHOLD_REACHED
send SMS `You have consumed 90 % of your total quota allotted on Example Inc.`
to user. Request delivery receipt `default`.
send notification to syslog with `SMS
```

```
90%;{User.E164};{User.Custom5};{User.Custom6};GOLD;{User.Entitlement};You have
consumed 90 % of your total quota allotted on Example Inc.` and severity `Info`
Advanced: set values for QoS and Charging parameters to
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

continue processing message
```

- Group: Quota *100MB*; Policy: Quota *100MB* additional quota set 100 percent volume threshold

```
where the user is using greater than or equal to 100 percent of total volume for
 DP_QUOTA.100MB quota
And where the user is using less than 100 percent of total volume for
DP_QUOTA_ADDL.3GB quota
remove PCC rule types all for all
install 16Mbps_DL_5.76Mbps_UL PCC rules for flow
grant total volume to 100 percent used for DP_QUOTA_ADDL.3GB
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers  REVALIDATION_TIMEOUT,
USAGE_THRESHOLD_REACHED
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

accept message
```

- Group: Quota *2GB*; Policy: Quota *2GB* additional quota set 100 percent volume threshold

```
where the user is using greater than or equal to 100 percent of total volume for
 DP_QUOTA.2GB quota
And where the user is using less than 100 percent of total volume for
DP_QUOTA_ADDL.4GB quota
remove PCC rule types all for all
install 16Mbps_DL_5.76Mbps_UL PCC rules for flow
grant total volume to 100 percent used for DP_QUOTA_ADDL.4GB
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers  REVALIDATION_TIMEOUT,
USAGE_THRESHOLD_REACHED
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

accept message
```

- Group: Quota *100GB*; Policy: Quota *100GB* additional quota set 100 percent volume threshold

```
where the user is using greater than or equal to 100 percent of total volume for
 DP_QUOTA.100GB quota
And where the user is using less than 100 percent of total volume for
DP_QUOTA_ADDL.5GB quota
remove PCC rule types all for all
install 16Mbps_DL_5.76Mbps_UL PCC rules for flow
grant total volume to 100 percent used for DP_QUOTA_ADDL.5GB
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers  REVALIDATION_TIMEOUT,
USAGE_THRESHOLD_REACHED
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

accept message
```

All the differences in the seven policies for the three groups can be tabulated using only six columns and three rows, as follows. Because of the similarities from group to group, these policies are good candidates for using a policy table. These three groups can be replaced by one set of policies using variables for differences and one policy table with three rows. The table's key column, representing

the scenarios, is a policy context property. The table column headings become the names of the other variables used in the policies.

Policy Variable scenario	Base Quota	Additional Quota	Percent Limit	Additional Limit	Grant Quota
100 MB	DP_QUOTA.100MB	DP_QUOTA_ADDL.3GB	70	3 GB	DP_QUOTA_ADDL.3GB
2 GB	DP_QUOTA.2GB	DP_QUOTA_ADDL.4GB	90	4 GB	DP_QUOTA_ADDL.4GB
100 GB	DP_QUOTA.100GB	DP_QUOTA_ADDL.5GB	90	5 GB	DP_QUOTA_ADDL.5GB

The triggering policies are now rewritten to use the policy table and a single policy group, which in this case study is named `QUOTA`. A policy context property is used as the key to locate the row in the table to use.

- Table-Driven Trigger Policy: Evaluate 3G Volume Quota Group 100 MB

```
where the ENTITLEMENTS is contained in Match Lists Ent 100MB Quota
set policy context property scenario to 100MB
evaluate policy group QUOTA
```

- Table-Driven Trigger Policy: Evaluate 3G Volume Quota Group 2 GB

```
where the ENTITLEMENTS is contained in Match Lists Ent 2GB Quota
set policy context property scenario to 2GB
evaluate policy group QUOTA
```

- Table-Driven Trigger Policy: Evaluate 3G Volume Quota Group 100 GB

```
where the ENTITLEMENTS is contained in Match Lists Ent 100GB Quota
set policy context property scenario to 100GB
evaluate policy group QUOTA
```

The policies in the QUOTA group are now rewritten to use the policy table, which in this case study is named `Quota_table`, and variables. The sample policies shown previously are rewritten as follows:

- Group: QUOTA; Policy: Quota send Warning percent SMS

```
use table Quota_table called table
where the user is using greater than or equal to table.PctLmt percent and less
than 100 percent of volume for table.BaseQuota quota
And where the event trigger is one of USAGE_THRESHOLD_REACHED
send SMS `You have consumed table.PctLmt % of your total quota allotted on Example
 Inc.` to user. Request delivery receipt `default`.
send notification to syslog with `SMS
table.PctLmt%;{User.E164};{User.Custom5};{User.Custom6};GOLD;{User.Entitlement};You
 have consumed table.PctLmt % of your total quota allotted on Example Inc.` and
 severity `Info`
Advanced: set values for QoS and Charging parameters to
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

continue processing message
```

Group: QUOTA; Policy: Quota additional quota set 100 percent volume threshold

```
use table Quota_table called table
where the user is using greater than or equal to 100 percent of total volume for
 table.BaseQuota quota
And where the user is using less than 100 percent of total volume for
table.AddlLmt quota
remove PCC rule types all for all
install 16Mbps_DL_5.76Mbps_UL PCC rules for flow
grant total volume to 100 percent used for table.AddlQuota
Advanced: set values for QoS and Charging parameters to
Diameter Enforcement Session Event Triggers  REVALIDATION_TIMEOUT,
USAGE_THRESHOLD_REACHED
Diameter IP-CAN Session Usage Monitoring  USAGE_MONITORING_ENABLED

accept message
```

Creating Policy Tables

When you define a policy table, it must contain at least one key column and one row, and you must populate every cell in the table.

To create a policy table:

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. Click **Create Policy Table**.
   The **Policy Table Administration** page opens.
4. Enter information as appropriate:
   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) — You must define at least one key column.
   If you click **Add Column**, a **Policy Table Column** window opens. Enter the following information:
   - **Column Name** (required) — The name you assign to the column. Policies use this name as part of the address of cells in this column.
   - **Column Type** (required) — The data type of cells in the column. Click the folder icon; a selection window opens, displaying the Policy Wizard actions and conditions. Locate the condition or action you want to abstract and select the variable to use (displayed in red text); the data type is taken from the variable.
   - **Key** — The policy variable used as a key. If this is a key column, select the check box and either select a policy variable from the list or type the name of the variable you want to use. The policy variable is used to obtain the value from the policy context when using the table to look up a row.

- **Delimiter** — The character that separates values within a cell. For fields that accept multiple values, specify the delimiter between values. Enter any single ASCII character. The default is a comma (,). If you enter no value, the field is evaluated as a single value.
- **Matching Operation** — If this is a key column and no delimiter is defined, the default matching operation is **Equivalence**. If a delimiter is defined, select the matching operation:
  - **Wildcard**
  - **Policy Context Set Contains All Multiple Valued Key Column**
  - **Multiple Key Column Set Contains Single Value Context** (default)
  - **Multiple Policy Context Set Contains Single Value Key Column**
  - **Key Column Value Set Contains Any Multiple Valued Context**
  - **Equivalence**
  - **Key Column Set Contains All Multiple Valued Policy Context**

  For information on matching operations see *About Data Matching*.
- click **Save**.

To add a row:

a) Click **Add Row**. A row is added below the current row in the table.
b) Select a cell in the row. A window opens so you can enter the value for that cell. The data in the cell must match the data type of the column.
c) Enter the value and click **OK**. You can also enter a comma-separated list of values.

The column or row is displayed.

6. To manage a row or column, select it and click **Operations**, then select an operation from the 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**.

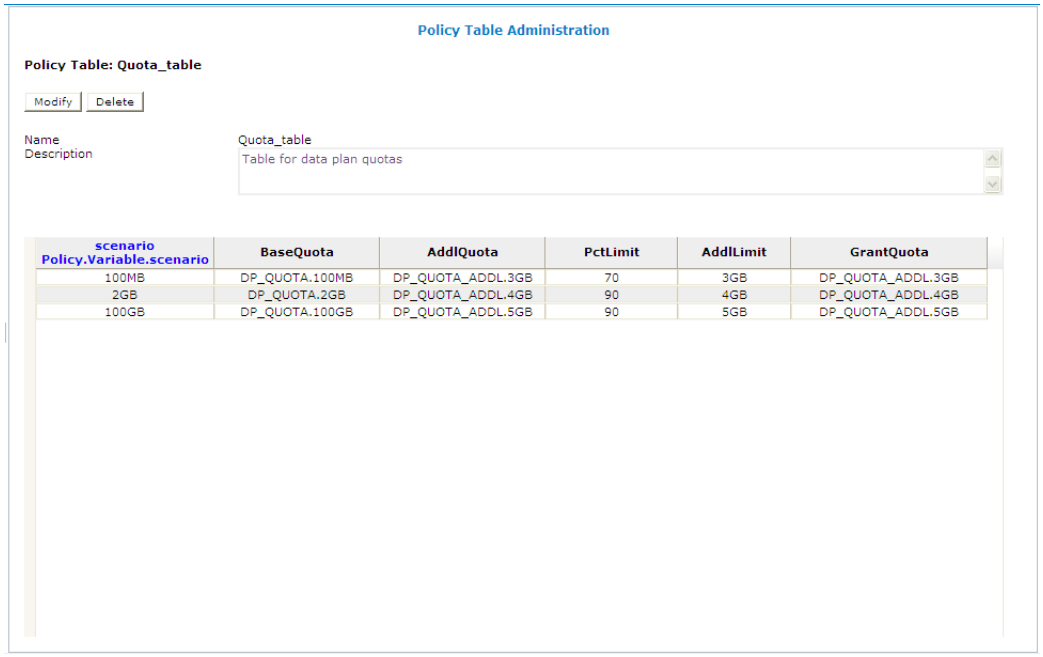
   Validation ensures that tables contain a key column, at least one row, and no empty cells. If the table is valid, a confirmation message displays. Click **OK** to close the window.

   If the table is invalid, a diagnostic message displays. Correct the table, and click **Validate** again.

   The table definition is validated.
8. Click **Save**.
   The policy table is validated, and if valid is displayed on the **Policy Table Administration** page.

You have created a policy table. You can now use the table in a policy.

Figure 10: Sample Policy Table shows the sample policy table discussed in *Policy Table Case Study*.



scenario Policy.Variable.scenario	BaseQuota	AddlQuota	PctLimit	AddlLimit	GrantQuota
100MB	DP_QUOTA.100MB	DP_QUOTA_ADDL.3GB	70	3GB	DP_QUOTA_ADDL.3GB
2GB	DP_QUOTA.2GB	DP_QUOTA_ADDL.4GB	90	4GB	DP_QUOTA_ADDL.4GB
100GB	DP_QUOTA.100GB	DP_QUOTA_ADDL.5GB	90	5GB	DP_QUOTA_ADDL.5GB

Figure 10: Sample Policy Table

Viewing Policy Tables

1. From the **Policy Management** section of the navigation pane, select **Policy Table Library**. A tree frame view displays **All Tables**.all existing policy tables. You will see all of the existing policy tables in the main frame when you click **ALL**.
2. Click the policy table name in the tree frame to view the details.

Associating Policy Tables with a Policy Rule

To associate a policy table with a new or existing policy rule, the policy table must already be defined. See *About Policy Tables* for more information on what a policy table is. See *Creating Policy Tables* for more information on how to define a policy table. See *Creating a Policy* for more information on creating and modifying a policy definition.

One or more policy tables can be associated with a new or existing policy rule from the **Table Associations** page of the Policy Wizard using this procedure:

1. Start the Policy Wizard.
2. On the **Table Associations** page, select the association type.
   - **use table** ***policy table*** **called** ***specified alias name***
   - **use table** ***policy table*** **called** ***specified alias name*** **returns** ***unique row***

The policy table option is added to the **Description** section of the page, where you select an existing policy table to use, and define an alias name for this policy table, if needed.

3. In the **Description** section of the page, click **policy table** to select a policy table.
   The **Policy Table Data** window appears.
4. Select a table, and click **OK**.
5. Click **specified alias name** to associate a unique name with this table. An alias name is required
   The **Input a Value** window opens.
6. Enter an alias name following the format specified in the window, and click **OK**.

   The name describes the purpose of this table in this policy. You can then use the same policy table in multiple policies but define a different purpose each time with the alias name field.
7. If you selected the table association that specifies unique row option, click **unique row** and select an option.
   - **unique row** (default)— First matched row is selected.
   - **multiple rows**—All matches are selected.
8. Repeat these steps to associate another policy table with this policy rule, if needed.
9. If multiple policy tables are associated with this policy rule, use the ▲ (up) icon or ▼ (down) icon to move the table and change the order in which it is evaluated in the rule.
10. Click **Next** to continue to the **Conditions** page.

The selected policy tables are associated with this policy definition.

Associating a Parameter with a Policy Table Column

After you have defined a policy table and associated it with a policy rule, you can associate individual rule parameters with columns (fields) defined in the table.

1. In the condition or action, click on the parameter for which you want to use the policy table.
   A selection window opens.
2. Click **Use Policy Table**.
   A list of policy table fields (columns) opens.

   Tip: If no choices are available, no appropriate column is defined.
3. Select the policy table field (column) and click **OK** to use that field, or **Use Input Value** to enter an input value (not use the policy table) instead.
   The selection window closes.

When the rule is evaluated, the value of the parameter is replaced by the value in the policy table.

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. Select the policy table.

The **Policy Table Administration** page displays information about the policy table.

3. Click **Modify**.
   The table fields become editable. See *Creating Policy Tables* for information about the table fields.
4. Click **Validate**.
   The data modified is validated. If the table is valid, a confirmation message displays. Click **OK** to close the window. If invalid, a diagnostic message appears.
5. Click **Save**.

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 right of the policy table.
   - Open the policy and click **Delete**.

   A confirmation message displays.
3. Click **OK**.

The policy table is deleted.

Chapter 26

Managing Policy Checkpoints

Topics:

- *About Policy Checkpoints.....534*
- *Creating a Policy Checkpoint.....534*
- *Viewing and Comparing Policy Checkpoints...535*
- *Restoring a Policy Checkpoint.....535*
- *Restoring a Policy Checkpoint to MPE Devices.....536*
- *Deleting a Policy Checkpoint.....537*

This chapter describes the method of saving CMP objects and their configuration, as well as their association, to the CMP database at a specific point in time.

About Policy Checkpoints

A policy checkpoint is a method of saving the records in the CMP database at a specific point in time. The table below details which configurable objects are and are not saved as part of the checkpoint.

Records saved	Records not saved
• policies • policy groups • policy templates • policy tables • policy counter IDs • traffic profiles • traffic profile groups • MPE configuration templates • match lists • retry profiles • applications	• quota profiles • quota conventions • serving gateways/MCC-MNC mappings • charging servers • time periods • customer AVPs • services • rating groups • LI mediation functions

Note: The checkpoint function also saves associations between:

- Virtual MPE templates and real MPE templates
- MPE devices and virtual MPE templates
- Virtual MPE templates and other configuration objects

You can save up to ten checkpoints.

After a checkpoint is created, you can return to this set of records at any time by restoring the checkpoint.

Caution: When you restore a checkpoint, all existing data is permanently removed.

The checkpoint function is different from the import/export function in the following ways:

- Checkpoints are saved to the CMP database rather than to a file.
- A checkpoint saves all the records mentioned in the preceding table. The import/export feature allows you to select which records to import or export.
- A checkpoint can only be used on a specific CMP system and cannot be migrated to another CMP system.

Creating a Policy Checkpoint

To access this feature, specify a value greater than 0 for the **Allow policy backup and rollback** field on the **System Settings** page. To refresh the menu, log out and log back in. This field also controls the

maximum number of checkpoints that can be saved. For information on system settings, see the *CMP User's Guide*.

Use this procedure to create a new checkpoint. A checkpoint saves policies, policy groups, policy templates, policy tables, traffic profiles, and traffic profile groups; other records 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:

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, you are prompted, `n checkpoints already exist, by creating this checkpoint the oldest one will be deleted. Continue?`. *n* indicates the maximum number of checkpoints).
3. Click **OK**.

The checkpoint is created.

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 database:

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.

Restoring a Policy Checkpoint

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.

Note: Charging servers, customer AVPs, services, LI mediation functions, rating groups, serving gateways/MCC-MNC mappings, and time periods are not saved in checkpoints, so be sure all related profile information exists in the CMP system before restoring. If related profile information is not available before you do a restore, the restore process will fail. Use the **More Info** link to view all required profile information for a checkpoint.

To restore to a checkpoint in the CMP database without autodeployment to the MPE devices:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**. The **Checkpoint/Restore** page opens.
2. Click **Restore**.
3. Select the checkpoint you are restoring.
4. Click **Restore**.
   You are prompted, `Caution: All current records are lost when a restoration is performed. It is recommended that you save a checkpoint before restoring a previous checkpoint. Are you sure that you want to restore to this Checkpoint?`
5. Click **OK**.
   A confirmation message displays. Click **OK**.
6. Click **Save**.

A checkpoint report appears, listing which policies and policy groups were restored and which were removed.

Restoring a Policy Checkpoint to MPE Devices

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: Charging servers, customer AVPs, services, LI mediation functions, rating groups, serving gateways/MCC-MNC mappings, and time periods are not saved in checkpoints, so be sure all related profile information exists in the CMP system before restoring. If related profile information is not available before you do a restore, the restore process will fail. Use the **More Info** link to view all required profile information for a checkpoint.

To restore to a checkpoint in the CMP database and autodeploy to all MPE devices in the system:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**. The **Checkpoint/Restore** page opens.
2. Click **Restore**.
3. Select the checkpoint you are restoring.
4. Click **Restore and Deploy**.
   You are prompted, `Caution: All current records are lost when a restoration is performed. It is recommended that you save a checkpoint before restoring a previous checkpoint. Are you sure that you want to restore to this Checkpoint and deploy it to MPEs?`
5. Click **OK**.
   A confirmation message displays.
6. Click **OK**.
7. Click **Save**.

A checkpoint report appears, listing which policies and policy groups were restored, which were removed, and to which MPE devices the deployment succeeded.

Deleting a Policy Checkpoint

To delete a saved checkpoint from the CMP system:

1. From the **Policy Management** section of the navigation pane, select **Policy Checkpoint/Restore**.
   The **Checkpoint/Restore** page opens.
2. Select the checkpoint you are deleting.
3. Click **Delete the selected checkpoint** to remove the checkpoint from the system.
   A confirmation message displays.
4. Click **OK**.
   The message `Checkpoint deleted successfully` appears in green on the page.

The selected checkpoint is deleted from the CMP database.

Glossary

A

AAA	Authentication, Authorization, and Accounting (Rx Diameter command)
ADC	Application Detection and Control Policy rules that enable detection and control of application traffic and associated enforcement action.
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 (for example, routing information) as well as authentication, authorization or accounting information.

B

B

BNG	Broadband Network Gateway is an example of a BNG device is a broadband remote access server (B-RAS).
bps	Bits Per Second
BSSID	Basic Service Set Identifier MAC address of the wireless access point.

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.
Circuit ID	Identifies the relay circuit from which a DHCP client-to-server packet was received.
CS	Circuit Switching

D

DEA	Diameter Edge Agent Device through which LTE roaming signaling traffic is funneled to protect network element addresses from being exposed to third parties.

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.
DOCSIS	Data Over Cable Service Interface Specification - An international telecommunications standard for adding high-speed data transfer to an existing cable TV system. Employed by many cable television operators to provide Internet access over their existing infrastructure.

E

EPS	Evolved Packet System EPS is the core or main component of an LTE (Long-Term Evolution) system.

F

FQDN	Fully Qualified Domain Name The complete domain name for a specific computer on the Internet (for example, www.oracle.com). A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GBR	Guaranteed Bit Rate A minimum bit rate requested by an application for uplink and downlink traffic.

G

GUI	Graphical User Interface The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.
Gx	The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.

H

HRPD	High Rate Packet Data

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

I

packet routing, fragmentation and re-assembly through the data link layer.

L

LTE

Long Term Evolution

The next-generation network beyond 3G. In addition to enabling fixed to mobile migrations of Internet applications such as Voice over IP (VoIP), video streaming, music downloading, mobile TV, and many others, LTE networks will also provide the capacity to support an explosion in demand for connectivity from a new generation of consumer devices tailored to those new mobile applications.

M

MAC

Media Access Control Address

The unique serial number burned into the Ethernet adapter that identifies that network card from all others.

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

M

mobile phone operator/carrier. See also MCC.

N

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.

O

Operator Name

Identifies the TWAN operator when the TWAN is not operated by a mobile operator usually encoded in the form of an Internet domain name.

P

pass

A quota profile that provides a one-time override of a subscriber's default plan.

PCC

Policy and Charging Control

Policy rules that define the conditions and actions used by a carrier network to control how subscribers and applications are treated and how network resources are allocated and used.

PCEF

Policy and charging enforcement function

A system responsible for enforcing policies on network subscriber authentication, authorization, accounting, and mobility. A PCEF

P

	device, such as a CMTS or GGSN, communicates with a PCRF device, such as a policy server.
PCRF	Policy and Charging Rules Function The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF. In the Policy Management system, PCRF is located in the MPE device. Software node designated in real-time to determine policy rules in a multimedia network.
plan	A quota profile that consists of a subscriber's basic, recurring service.
PLMN	Public Land Mobile Network A wireless communications network that uses land-based radio transmitters or base stations, intended for public use by terrestrial subscribers in vehicles or on foot. A PLMN is identified by its Mobile Country Code (MCC) and Mobile Network Code (MNC).
policy group	An ordered group of policies, organized for ease of administration or deployment.

P

PS	Packet Switching Priority Service

Q

QoS	Quality of Service Control mechanisms that guarantee a certain level of performance to a data flow.
quota	Specifies restrictions on the amount of data volume, active session time, or service-specific events that a subscriber can consume.
quota convention	Specifies the default values for rollovers and enables top-ups. A quota convention is associated with a plan.
quota profile	Defines how quotas are implemented and specifies the default values. Quota profiles consist of passes and plans.

R

RAA	Re-Authorization Answer (Gx or Rx Diameter command)
RADIUS	Remote Authentication Dial-In User Service A client/server protocol and associated software that enables remote access servers to communicate with a central server to authorize their access to the requested service. The MPE device functions with RADIUS servers to authenticate messages received from remote gateways. See also Diameter.

R

RAR	Re-Authorization Request (Gx or Rx Diameter command)
RAT	Radio Access Technology
Relay Identity	Identifies the TWAN relay identity type as either IPv4/IPv6 or FQDN.
rollover	A quota convention that allows a subscriber to carry forward unused units from one billing cycle to another.

S

S9	The S9 Diameter interface includes Rx, Gx, and Gxx messages, but when these messages are used between a visited PCRF and the home PCRF, the interfaces are collectively referred to as S9. Defined by 3GPP 29.215 as the interface between a visited PCRF and a home PCRF. There is no difference in processing of Rx over S9 versus. Rx not over S9. The S9 interface is binding capable for Gx and Gxx only. Rx over S9 is binding dependent.
server	In Policy Management, a computer running Policy Management software, or a computer providing data to a Policy Management system.
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.

S

SMS	Short Message Service A communication service component of the GSM mobile communication system that uses standard communications protocols to exchange short text messages between mobile phone devices. See also GSM.
	Shared Metric Service
SPC	Service Provisioning over COPS (Common Open Policy Service protocol)
SPR	Subscriber Profile Repository A logical entity that may be a standalone database or integrated into an existing subscriber database such as a Home Subscriber Server (HSS). It includes information such as entitlements, rate plans, and so on.The PCRF and SPR functionality is provided through an ecosystem of partnerships.
SSID	Service Set Identifier Used to uniquely identify a wireless LAN.

T

top-up	A quota convention that allows a subscriber to obtain additional units for an existing plan.
TWAN	Trusted Wireless Area Network

V

VoIP	Voice Over Internet Protocol

V

Voice communication based on the IP protocol competes with legacy voice networks, but also with Voice over Frame Relay and Voice and Telephony over ATM. Realtime response, which is characterized by minimizing frame loss and latency, is vital to voice 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.