CPS Mobile Configuration Guide, Release 22.2.0

First Published: 2022-08-25

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

Preface

About This Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document is a part of the Cisco Policy Suite documentation set.

For information about available documentation, see the *CPS Documentation Map* for this release at Cisco.com.

Note The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

Audience

This guide is best used by these readers:

- Network administrators

- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.

Conventions	Indication
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Note Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Important Notes

Important Any feature or GUI functionality that is not documented may not be supported in this release or may be customer specific, and must not be used without consulting your Cisco Account representative.

CHAPTER 1

Policy Builder Overview

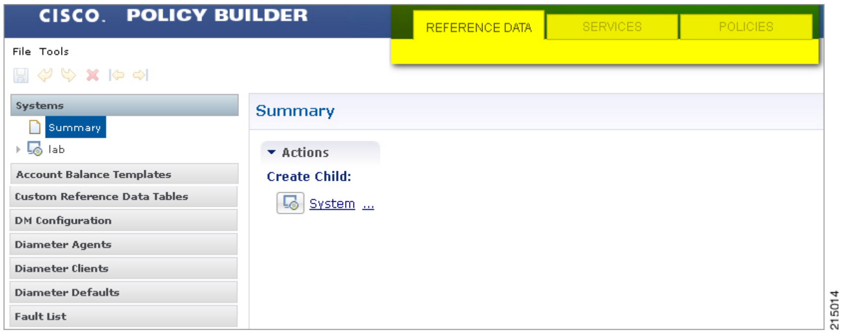
Overview

Cisco Policy Suite (CPS) provides a framework for building rules that can be used to enforce business logic against policy enforcement points such as network routers and packet data gateways. For example, a prepaid customer (one who pays as they go) might be denied service or prompted to top-up when their quota has expired, whereas a postpaid customer (one who has an ongoing billing relationship with the service provider) might only have their service downgraded or be automatically billed for additional data when their particular quota has expired.

CPS allows service providers to create policies that are customized to their particular business requirements through the use of the CPS Policy Builder, a web-based tool with a graphical user interface (GUI) that allows for rapid development of innovative new services.

The Policy Builder GUI supports both configuration of the overall CPS cluster of virtual machines (VMs) as well as the configuration of services and advanced policy rules. The following sections introduces the main aspects of the PB GUI as laid out in three tabs on the upper right of the interface: Reference Data, Services and Policies.

Figure 1: Cisco Policy Guilder GUI



Reference Data

The Reference Data tab of the PB GUI provides access for configuring various aspects of the system in order to make the system ready for operation. Reference Data are used to not only configure the system, but are also used to provide settings and parameters that are referenced by policy rules across various services; for example, Account Balances and Notifications are configured as Reference Data but are then referenced and reused by multiple services as needed. Details of the various Reference Data configuration options are described in more detail in other chapters of this guide.

The Reference Data tab contains static system, network, and template definition. It is not directly related to policy, services, or use cases, but does define the reference points for the following types of information:

- Systems, cluster, and instance data
- Jdbc query string definitions
- Balance and quota definitions
- Diameter agents, clients, and defaults information
- Query strings
- Custom reference data tables (custom look up tables such as apn names)
- Notification addresses and text templates
- Policy reporting criteria
- Subscriber data repositories
- Tariff switch times
- Fault list - For more information, refer to *CPS Operations Guide* for this release.

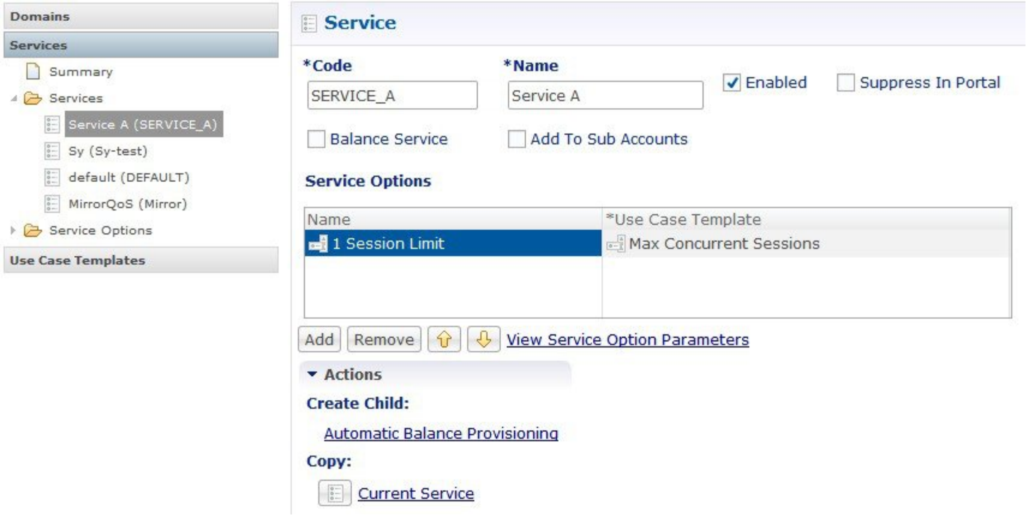
Services

The Services tab allows for creation of reusable policy rules that control how subscribers are granted network services, quota and notifications. Services are broken down into three core areas: Domains, Services and Use Case Templates. The following section provides an overview of the Services tab, however detailed instructions on how to build a service are covered in later chapters of this guide.

The creation of a new service begins with creating a Use Case Template (UCT) for the service. UCTs consist of Service Configurations specific to the service that will be created. For example, a Service Configuration might provide for the setup of a Gx Rule or Basic QoS. The UCT is also used to configure Use Case Initiators (UCI) which are instructions on when a specific Service Configuration should be in effect. An example of the UCI might be “only send this Gx Rule when the account balance is depleted”. Multiple UCIs can be configured for each Service Configuration allowing for complex logic as to when the configuration should or should not be in effect.

Once a UCT and associated UCIs are defined, it becomes the basis for Service Options, which are specific instances of the UCT that are populated with data specific to the service. Multiple Service Options can be created from a single UCT; for example, a UCT that provides for passing QoS parameters can be reused with different QoS values for different customers. Multiple Service Options can be layered to create the end Service.

Figure 2: Services tab



*Code: SERVICE_A

*Name: Service A

☑ Enabled ☐ Suppress In Portal

☐ Balance Service ☐ Add To Sub Accounts

Service Options

Name	*Use Case Template
1 Session Limit	Max Concurrent Sessions

The Domains panel within the Services tab handles the initial interaction of the client device with the policy engine, and covers tasks including client authentication, default provisioning of unknown clients and qualifying a client for particular system defaults and services.

For more information on the Services tab, refer to the Services, on page 229 chapter.

Policies

While the Services tab, through Use Case Templates and Service Options, makes it easy to create reusable and extensible services, the Policies tab allows direct access to the underlying policy engine. The Policies tab holds the CPS core system Blueprint, which is composed of various Extension Points that break the policy engine flow into sections that occur within the execution of the policy. For example, the point in the policy flow where a Gx connection is received, parsed, and processed before the point in the policy flow where the related subscriber data is evaluated.

Within the various Extension Points are Policies that define Conditions (events and data from the policy flow and external systems) that can then trigger Actions (manipulation of data and communication back to external systems).

Note that the configuration of services for most deployments will be handled through use of the Reference Data and Services tabs; advanced policies as defined on the Policies tab and discussed above are only required for complex deployments. It is recommended that only experienced users access the Policies tab as errors in custom policies can have negative impact on the operation of the system. Detailed discussion of custom policies is outside of the scope of this document.

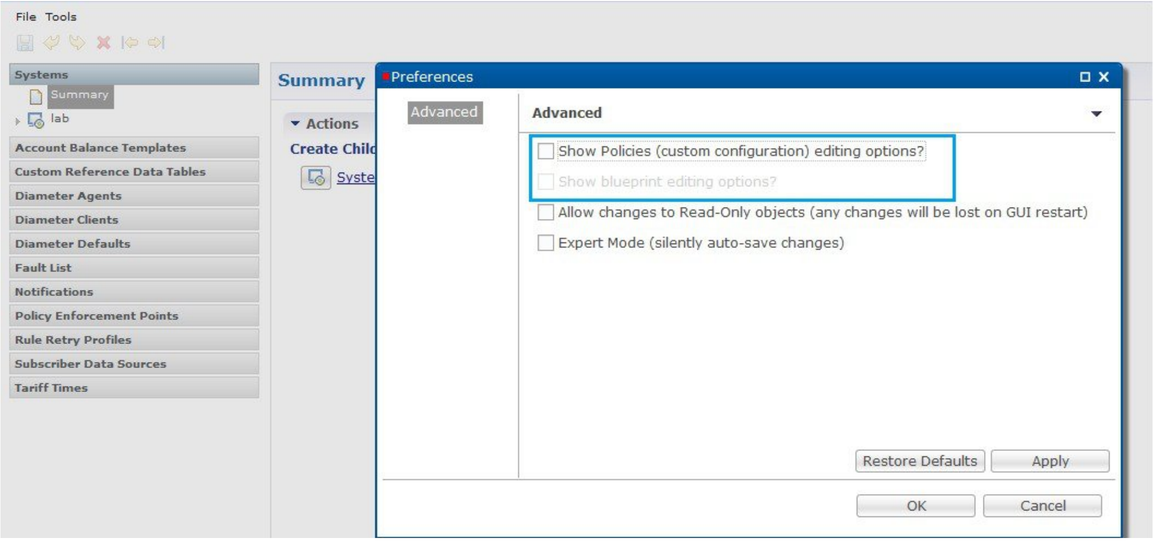
By default, the Policies and Blueprint tabs are disabled.

Important The Policy Builder offers the Blueprint section under **Policies** tab to enable Cisco recommended changes to the Policy Engine. Changes made without Cisco guidance are not supported and can result in poor performance, platform instability, or reduced capacity.

Enabling POLICIES tab

In Policy Builder, **Tools** > **Preferences** to open **Preferences** pop-up window.

Figure 3: Preferences - Policies



Advanced

☐ Show Policies (custom configuration) editing options?

☐ Show blueprint editing options?

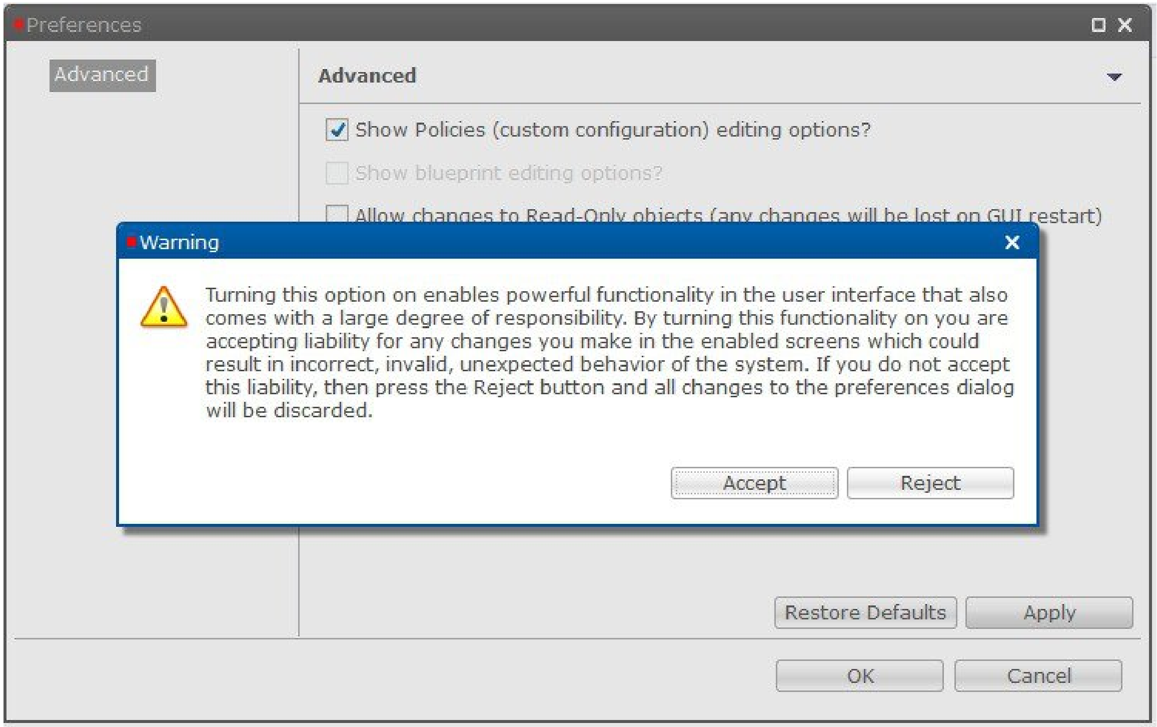
☐ Allow changes to Read-Only objects (any changes will be lost on GUI restart)

☐ Expert Mode (silently auto-save changes)

Select Show Policies (custom configuration) editing options? and click **Apply**.

Warning pop-up dialog box opens up.

Figure 4: Warning



Advanced

☑ Show Policies (custom configuration) editing options?

☐ Show blueprint editing options?

☐ Allow changes to Read-Only objects (any changes will be lost on GUI restart)

Turning this option on enables powerful functionality in the user interface that also comes with a large degree of responsibility. By turning this functionality on you are accepting liability for any changes you make in the enabled screens which could result in incorrect, invalid, unexpected behavior of the system. If you do not accept this liability, then press the Reject button and all changes to the preferences dialog will be discarded.

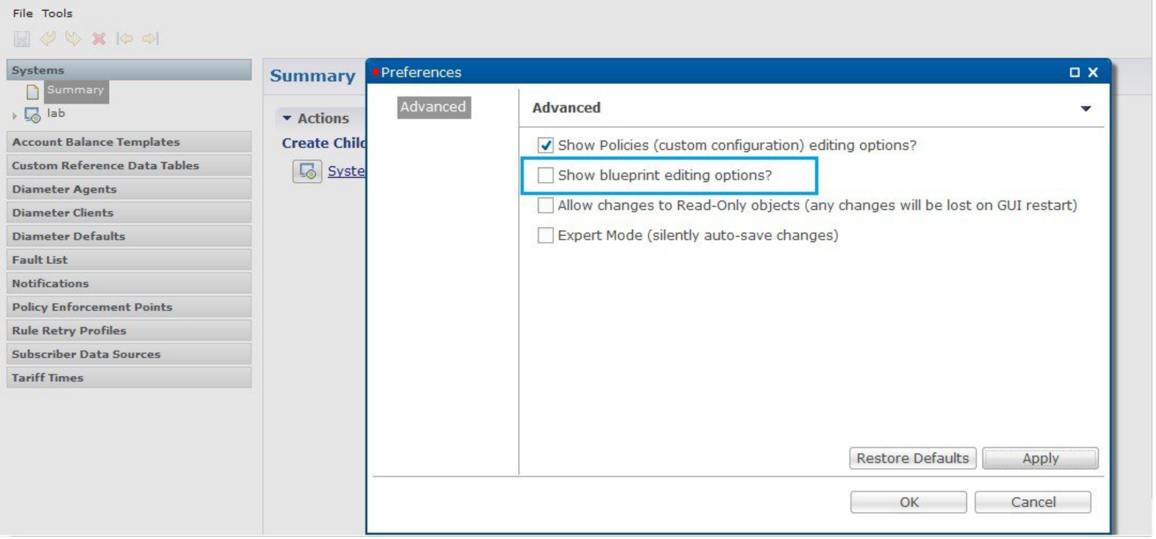
Click **Accept** so that **POLICIES** tab is visible in Policy Builder.

Enabling BLUEPRINTS tab

For **BLUEPRINTS** tab to be visible in Policy Builder, Show Policies (custom configuration) editing options? must be checked.

Select Show blueprint editing options? and click **Apply**.

Figure 5: Preferences - Blueprints 1



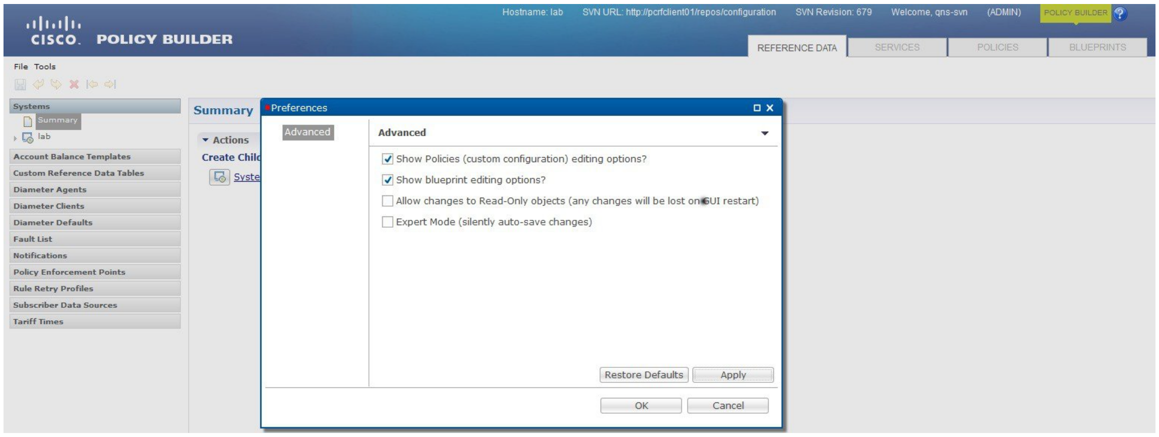
☑ Show Policies (custom configuration) editing options?

□ Show blueprint editing options?

□ Allow changes to Read-Only objects (any changes will be lost on GUI restart)

□ Expert Mode (silently auto-save changes)

Figure 6: Preferences - Blueprints 2



☑ Show Policies (custom configuration) editing options?

☑ Show blueprint editing options?

□ Allow changes to Read-Only objects (any changes will be lost on GUI restart)

□ Expert Mode (silently auto-save changes)

Warning pop-up dialog box opens up.

Click **Accept** so that **BLUEPRINTS** tab is visible in Policy Builder.

Note In case the **POLICIES** checkbox is unchecked while **BLUEPRINTS** checkbox is checked, the **BLUEPRINTS** checkbox is unchecked forcefully and the **BLUEPRINTS** tab is not visible.

Summary of Policy Tab Capabilities

- Conditional rules within specified Extension Points (Condition/Action)
- Trigger specific actions from an extensive catalog of Use Case Initiators
- Evaluate and manipulate session data as part of making policy decisions and returning services data to downstream systems

Advantages

- Allows for handling complex policy situations without writing custom code
- Support for custom or unusual business rules

Considerations

- Building custom policies requires a deep understanding of the call flow and underlying CPS platform
- Due to the flexibility of the Policy Builder, it is possible to create conflicting policies that can have a negative impact on system performance

Accessing the Policy Builder

The Policy Builder is the web-based client interface for the configuration of policies to the Cisco Policy Suite. Initial accounts are created during the software installation with the default CPS install username as **`qns-svn`** and password as **`cisco123`**.

URL to Access Policy Builder Interface:

- For HA: https://<*lbvip01*>:7443/pb

The Policy Builder provides a PAM based and SVN based authentication mechanism to support the authentication of Linux user credentials. The `disablePamAuthentication` flag is used to enable or disable user login and to perform PAM based authentication.

The following tables describes the user roles and credentials supported:

Table 1: User Roles and Authentication Mechanism

Linux access	SVN access	User Access to Policy Builder	User Roles	Authentication Mechanism
Read/Write	Not an SVN user	Yes	Read only	PAM (Linux Systems) (set disablePamAuthentication = false)
Read only	Not an SVN user	Yes	Read only	PAM (Linux Systems) (set disablePamAuthentication = false)
Read/Write	Read/Write	Yes	Admin	PAM (Linux Systems) (set disablePamAuthentication = false)

Linux access	SVN access	User Access to Policy Builder	User Roles	Authentication Mechanism
Read/Write	Read only	Yes	Read only	PAM (Linux Systems) (set disablePamAuthentication = false)
Read only	Read/Write	Yes	Admin	PAM (Linux Systems) (set disablePamAuthentication = false)
Read only	Read only	Yes	Read only	PAM (Linux Systems) (set disablePamAuthentication = false)
Not a Linux user	Read only	Yes	Read only	SVN (set disablePamAuthentication = true)
Not a Linux user	Read/Write	Yes	Admin	SVN (set disablePamAuthentication = true)
Not a Linux user	Not an SVN user	No	Invalid username or password error	PAM/SVN

CPS enables users to be aware of its current privileges while accessing Policy Builder as described below:

- If a user has read-write privilege then ADMIN is displayed adjacent to user name in the GUI.
- If a user has read-only privilege then READONLY is displayed adjacent to user name in the GUI.

The hostname is displayed in the login dialog box and system banner to differentiate between open windows while performing any operation of the CPS system. It indicates which system is being modified and prevents any errors or misconfigurations.

The hostname is displayed when the parameter `-Dhostname=lab` is configured in pb/qns.conf files. If it is not configured in the qns.conf file, it is displayed as a result of the command "hostname" on the server.

The hostname is displayed in the login panel only when the following argument is set to true:

```
-DshowSitenameLogin
```

Enable TACACS+ authentication for Policy Builder by enabling PAM authentication (set -DdisablePAMAuthentication to false) and enabling TACACS+ along with `tacacs_on_ui` flag set to true in `Configuration.csv` file.

Enabling Logout Option

To enable the logout option in Policy Builder, the following parameter must be configured in `/etc/broadhop/pb/pb.conf` file.

- –DlogoutLinkVisibility

To view the **Logout** link on Policy Builder banner, set the parameter to true value.

To support backward compatibility, `-DlogoutLinkVisibility` flag is not present in `pb.conf` by default. If flag is not present, then the value is considered as false.

When the parameter is configured or updated, `restartall.sh` is required.

Caution Executing `restartall.sh` will cause messages to be dropped.

Policy Builder Field Value Validation

The Policy Builder uses the eCore framework to configure UI fields and their data types. The Policy Builder validation is triggered when a field is updated. The validation depends on the data type and valid value that you have defined for the field.

When you start the Policy Builder, the last recorded valid value defined in the eCore is set as the default value. If the value is not set in the eCore, the valid value is taken based on the eCore data type. For numeric data types, the Policy Builder displays 0 as a default value. For string data types, the Policy Builder displays null (empty) as a default value.

The Policy Builder validates the value that is configured in the field.

When you enter a value in the field and the value passes validation, the newly entered value is recorded as the last valid value. If the validation fails, the last recorded valid value is reverted.

CHAPTER 2

Basic Systems Configuration

Overview

The Cisco Policy Suite provides the Policy Builder as an interface for policy management. Policies translate a Service Provider’s business rules into actionable, logical processing methods that the Cisco Policy Suite enforces on the network.

The Cisco Policy Suite ships with some standard base policies that serve as a starting point for customization to suit a Service Provider's specific business rules.

Policy Builder Repository Configuration

The Policy Builder uses a Subversion version control repository to store the configuration data created in the UI. The data entered in the UI is translated into XML (Eclipse Modeling Framework xmi files) when saved.

As work is done in the UI, changes are saved to a temporary directory on the pcrfclient01. (The directory is specified in the Repository configuration dialog.) Therefore, you can log out and back in and the latest changes will remain. However, if someone else makes a change and commits, then your local changes are lost.

There are two options for saving configuration changes:

- Publish to Runtime
- Save to Client Repository

When saving to the client repository, the configuration is pushed to Subversion, but it is saved in a client only repository and not copied over to the runtime environment repository. If you 'Publish to Runtime', the configuration is saved to the client repository and also copied to the runtime environment repository. The CPS servers check the runtime environment repository for changes and will update automatically when changes are committed.

Best Practices

Typically, publishing configuration changes to a lab environment to run tests is best. And then when satisfied with the test results, you can publish the new configuration to a production environment.

Revert

As Subversion is a source code tracking repository, each version of a configuration is numbered and stored in the Subversion repository history. Therefore, it is also possible to revert to any version of a configuration. The Policy Builder does not have a way to do this via the GUI, but using the Subversion command line tools, any version of the configuration can be made the current revision. For more information, refer to Subversion documentation for how to use the command line tools.

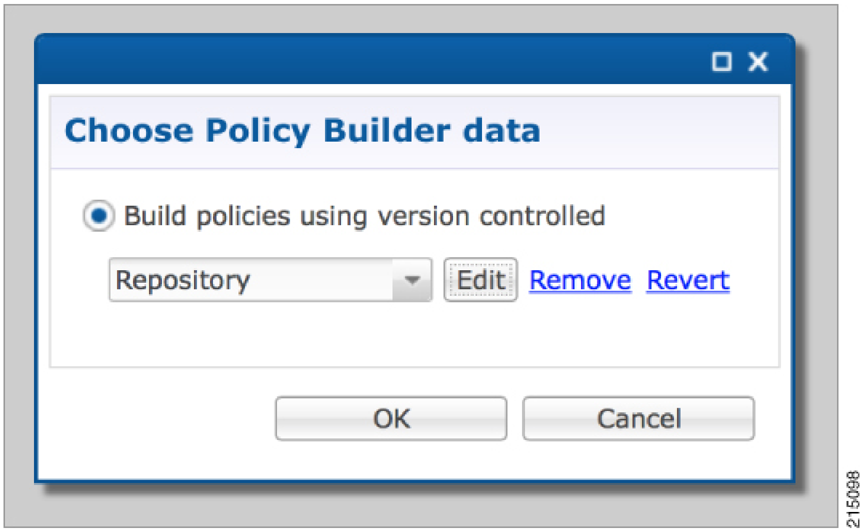
Default Repositories

The CPS deployment installs Subversion and creates a default client and runtime repository. The Subversion repositories are synced using Subversion's Master/Slave replication between the pcrfclient01 and pcrfclient02 nodes.

- Client - http://pcrfclient01/repos/configuration
- Runtime - http://pcrfclient01/repos/run

The Policy Builder start screen shows a dialog that lets you define repositories and choose a repository to check out for editing. A repository definition named “Repository” is installed by default and uses the default client repository (http://pcrfclient01/repos/configuration). The default PB user (qns-svn) with the default password is also setup.

Figure 7: Choose Policy Builder Data



Choose Policy Builder data

● Build policies using version controlled

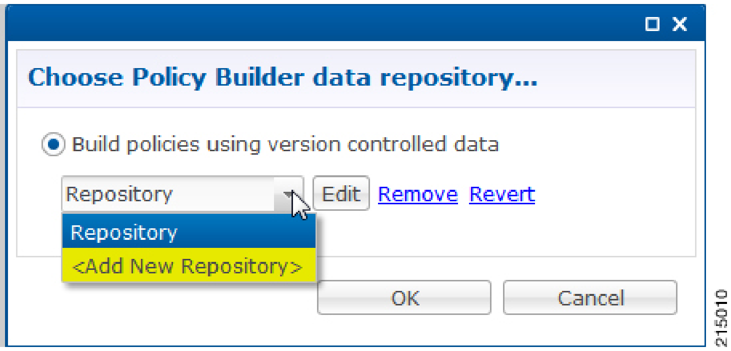
Repository

Adding a Client Repository Definition

Step 1 Start Cisco Policy Builder.

Step 2 In the **Choose Policy Builder data repository ...** dialog box, select **Add New Repository** from the drop-down list.

Figure 8: Adding a New Repository Definition

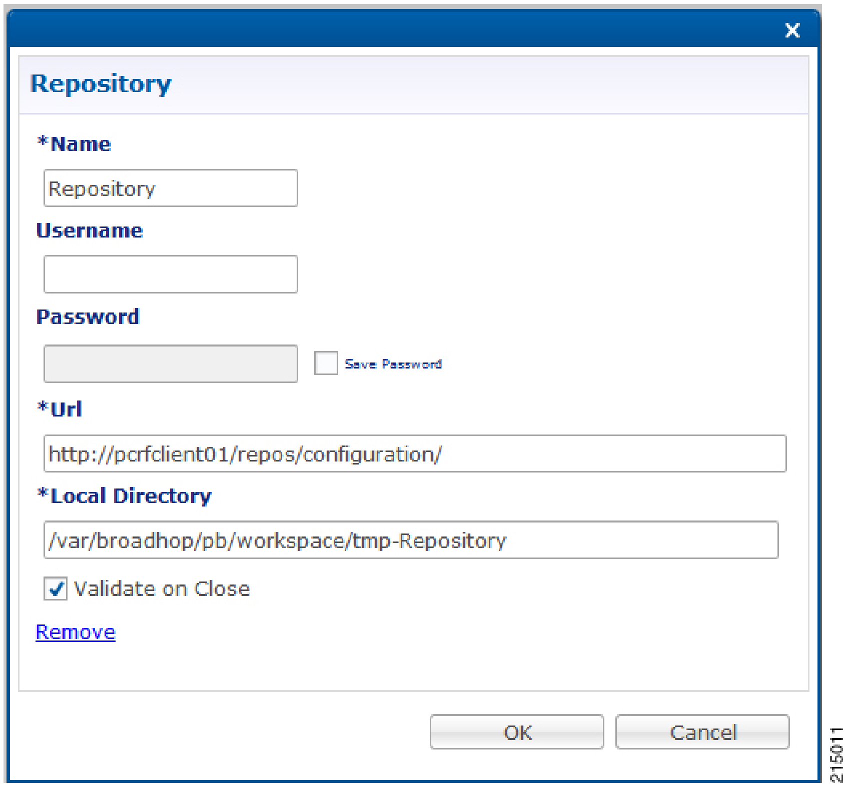


Choose Policy Builder data repository...

● Build policies using version controlled data

The **Repository** dialog box appears.

Figure 9: Repository Configuration Fields



Repository

*Name: Repository

Username:

Password:

□ Save Password

*Url: http://pcrfclient01/repos/configuration/

*Local Directory: /var/broadhop/pb/workspace/tmp-Repository

☑ Validate on Close

The following parameters can be configured under **Repository**:

Configure the parameters according to the network requirements.

Table 2: Repository Parameters

Parameter	Description
Name	This required field uniquely identifies your repository's site with a name. **Note** We recommend the following format for naming repositories: **`customername_project_date`**, where underscores are used to separate customer name, project and date. Date can be entered in the format: MMDDYYYY.
Username and Password	Enter a username that is configured to view Policy Builder data. The password can be saved for faster access, but it is less secure. A password, used with the Username, permits, or denies access to make changes to the repository.
Save Password	Select this check box to save the password on the local hard drive. This password is encrypted and saved as a cookie on the server.
Url	You can have several branches in the version control software to save different versions of configuration data. Create a branch in the version control software before assigning it in this screen. Enter the URL of the branch of the version control software server that is used to check-in this version of the data.
Local Directory	This value do not need to be changed. This is the location on the hard drive where the Policy Builder configuration objects are stored in version control. When you click either **Publish** or **Save to Repository**, the data is saved from this directory to the version control application specified in the **Url** text field. The field supports the following characrters: • Uppercase: A to Z • Lowercase: a to z • Digits: 1 to 9 • Non-alphanumeric: / **Note** The user needs to provide the specified characters above.
Validate on Close	Select this check box to see if the values for Username, Password, or the URL are legitimate and unique. If not, the screen displays an error message and provides a chance to correct the errors.
Remove	Removes the display of the repository in Cisco Policy Builder. **Note** The remove link here does not delete any data at that URL. The local directory is deleted.

Step 3 Click **OK** to save your work to the local directory.

Note When your change screens, Cisco Policy Builder automatically saves your work. Cisco recommends saving your work to the local directory by clicking on the diskette icon on the Policy Builder GUI or `CTRL-S` on the keyboard.

Step 4 If you are ready to commit these changes to the version control software, select **File** > **Save to Client Repository** on the Policy Builder home screen.

Editing a Client Repository Definition

Use this procedure to change any of the following details of client repository:

- Client repository name
- Username, password, and password save mechanism
- Client repository temporary save URL
- Client repository local directory save file path

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list in the **Choose Policy Builder data repository...** dialog box to select the desired repository.

Step 3 Click the **Edit** button.

Step 4 In the **Repository** dialog box, make the required changes.

Step 5 Click **OK** to save the changes to the repository definition.

Removing a Client Repository Definition

This procedure removes a repository from Cisco Policy Builder. This procedure does not delete the actual Subversion repository, just the definition for access in the Policy Builder.

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list in the **Choose Policy Builder data...** dialog box to select the desired repository.

Step 3 Click **Remove**. A confirmation dialog box appears.

Step 4 Click **OK** to delete the repository.

Saving Policy Builder Configuration Data to a Client Repository

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list on the **Choose Policy Builder data...** dialog box to select the desired repository.

Step 3 Click **OK** to open the Policy Builder GUI.

Step 4 Make the necessary modifications in the Policy Builder.

Step 5 To save the modifications done, select **File** > **Save to Client Repository**, or click the diskette icon on the Policy Builder GUI or use CTRL-S on the keyboard.

Step 6 Enter a commit message for the modifications done.

Step 7 Click **OK**. The modified configurations are saved to the client repository for later updating and publishing to the runtime environment.

Auto Save Policy Builder Configuration Changes

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

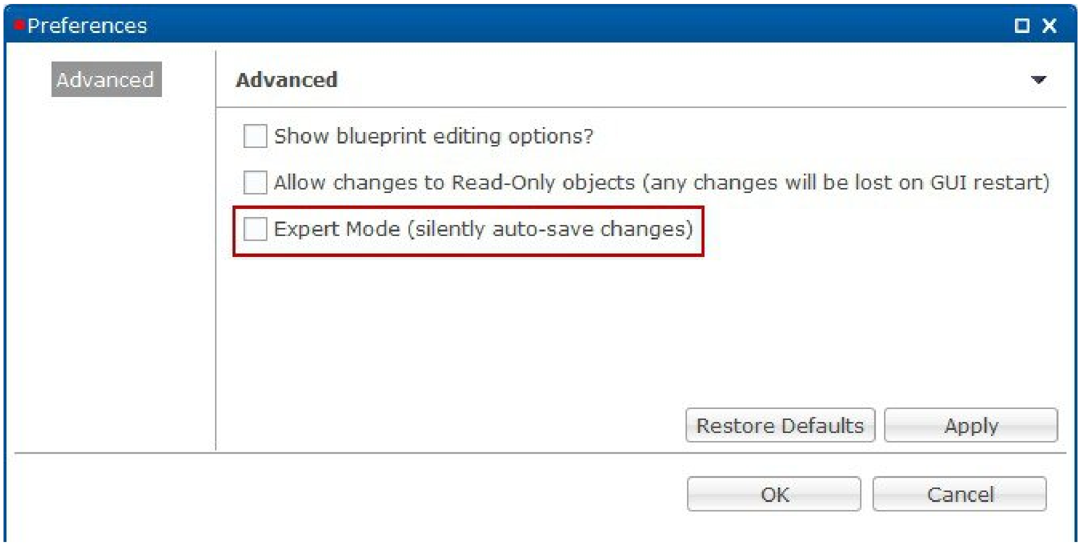
Step 2 Use the drop-down list on the **Choose Policy Builder data...** dialog box to select the desired repository.

Step 3 Click **OK** to open the Policy Builder GUI.

Step 4 Make changes to configuration data as necessary. For example, if you move from configuration to another configuration without saving the changes, a pop-up **Are you sure?** dialog box for saving the changes is displayed.

Step 5 Click **Yes** to save the changes. If you want to disable this notification, click **Tools** > **Preferences**. This opens **Preferences** window.

Figure 10: Preferences



Preferences

Advanced

Advanced

□ Show blueprint editing options?

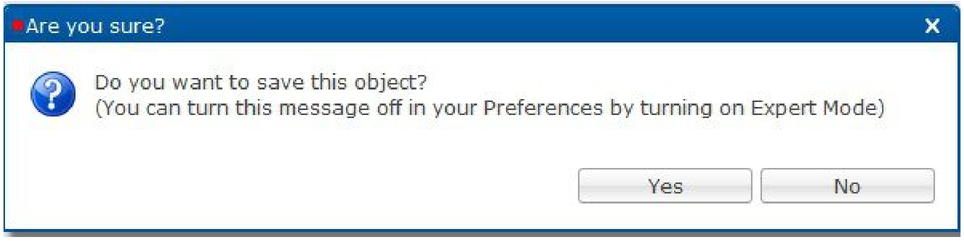
□ Allow changes to Read-Only objects (any changes will be lost on GUI restart)

□ Expert Mode (silently auto-save changes)

Step 6 Check **Expert Mode (silently auto-save changes)** flag to enable auto-save option.

Note By default, the flag is not checked. You have to check it in order to turn off the **Are you sure?** save prompt.

Figure 11: Are you sure?


Are you sure?

Do you want to save this object?
(You can turn this message off in your Preferences by turning on Expert Mode)

If the flag is not checked, the following options are displayed when updating/creating/copying an object:

- **Updating an Object**: While updating an object the PB asks **Do you want to save this object?** with option buttons as **OK** and **Cancel**. If you click **OK**, the data being worked on is saved and if you click **Cancel**, the data being worked on is not saved to the repository.
- **Creating an Object**: While creating an object the PB asks **Are you sure you want to create this object?** with option buttons as **OK** and **Cancel**. If you click **OK**, the new object is created with the default values and if you click **Cancel**, the object is not created.
- **Copying an Object**: While copying an object the PB asks **Are you sure you want to copy this object?** with option buttons as **OK** and **Cancel**. If you click **OK**, the object is copied and if you click **Cancel**, the object is not copied.
- This prompt is also displayed for **File** menu options when you use **Publish to Runtime Environment** or **Save to Client Repository...**.

Step 7 Once flag is checked, click **Apply** and **OK** to save the changes.

Publishing the Client Repository

To put changes into effect and have the Cisco Policy Builder server recognize the configuration changes made in your client session, use the Publish option and save the changes to the server repository.

Note To save the practice version, publish the client repository to the server. This is the version the server uses for production.

Do not publish to the Policy Builder unless you are completely satisfied with the configuration data in your client repository.

- Use the Policy Builder interface to either commit or set up a commit repository.
- Verify your work either by going to a web browser or by looking at the `config.properties` file.
- Unpublish with an SVN delete and restore.

When you are ready to put your Policy Builder changes into production, you need to publish them to Subversion. This preserves version history.

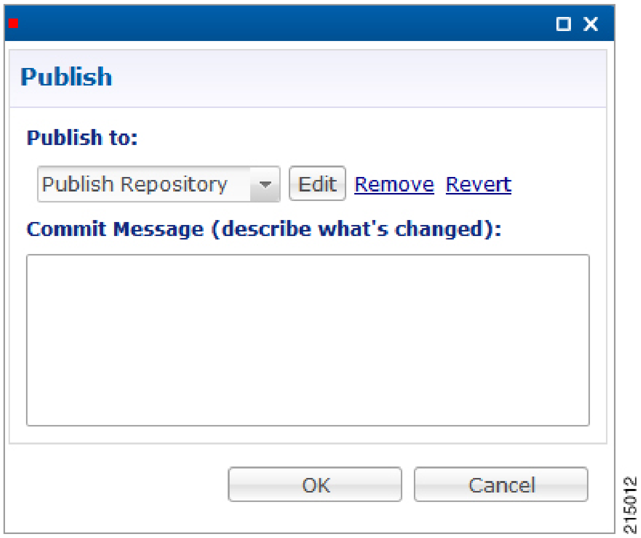
CPS supports to save the unpublished commit messages in a property file into the file system. This file is saved in the user directory under the selected repository location. For different users, Policy Builder will generate different property files.

Policy Builder saves the unpublished commit messages into the file system for the following cases:

- When loading **Publish** dialog box (**File** > **Publish to Runtime Environment…**) then saved commit message, if any, appears for that user in **Commit Message** pane.
- While publishing the policy configuration, if publish fails then the entered commit message is saved into the file system.
- While publishing the policy configuration, if publish succeeds then remove the message from file for the logged in user.
- If you click **Cancel** on **Publish** dialog box then the entered commit message is saved into the file system.
- If you click **Cross (x)** on **Publish** dialog box then the entered commit message is saved into the file system.
- When loading **Saving to Repository** dialog box (**File** > **Save to Client Repository…**) then saved commit message, if any, appears for that user in **Commit Message** pane.
- While saving to client repository, if operation fails then the entered commit message is saved into the file system.
- While saving to client repository, if operation succeeds then remove the message from file for the logged in user.
- If you click **Cancel** on **Saving to Repository** dialog box then the entered commit message is saved into the file system.
- If you click **Cross (x)** on **Saving to Repository** dialog box then the entered commit message is saved into the file system.

Step 1 To publish in Cisco Policy Builder, select **File** > **Publish to Runtime Environment**. The **Publish** dialog box appears.

Figure 12: Publishing to the Runtime Environment



Step 2 If you have already set up the repository to publish to, just enter a commit message.

Step 3 If you have not set up the repository, select **Add New Repository** from the **Publish to:** drop-down list and enter the required details for the new repository. For more information, refer to Adding a Client Repository Definition, on page 10.

Step 4 Verify the changes to Production repository:

- All changes are published to Subversion, so they are version-controlled and can be rolled back.
- To verify a publish as part of a troubleshooting process, take the URL seen in the previous screen and put it into a web browser (you may need to substitute the IP). The password is the same as in Cisco Policy Builder.
- If a traditional web browser cannot access the system, you can use a command line browser from the CPS VM's URL.

Error Notification during Publishing

During publishing, if there are any errors, the **Publish** dialog box will display the list of unresolved errors.

Note Policy Builder does not report errors for read-only objects.

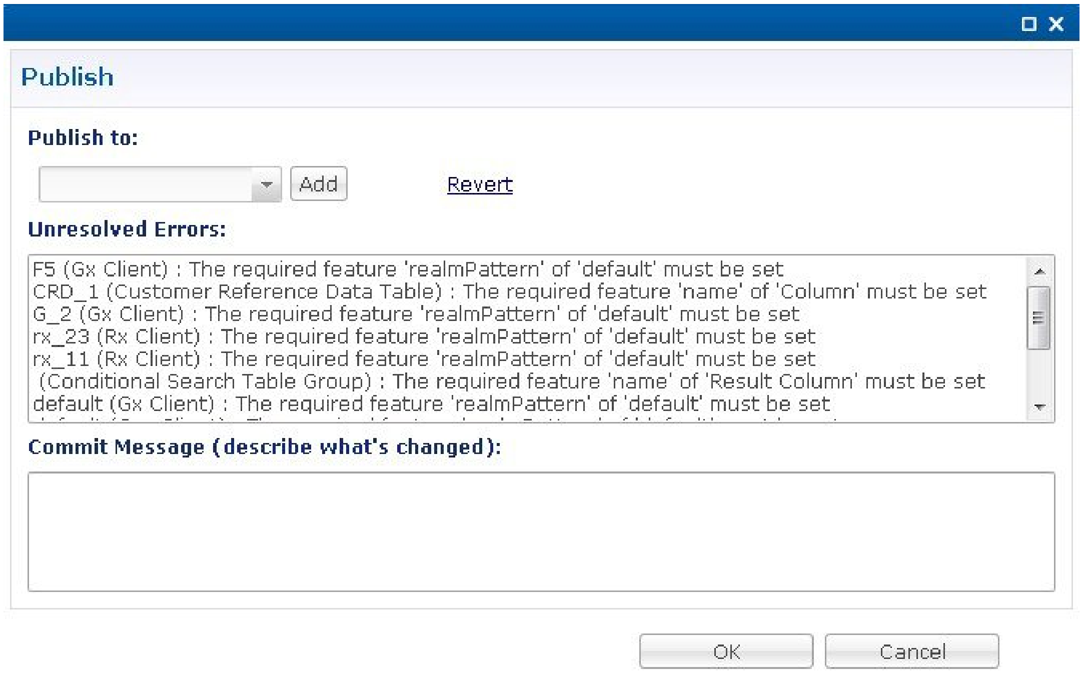
The errors are created in the session and are updated accordingly as the errors are resolved or are newly introduced with respect to their IDs.

The format of error string is as:

```
<Object_Name> <Feature_Name> :: <Error_String>
```

You can select and copy one or more of the errors in the list and paste them into another window (for example, in an email or in a file to mask the acceptable errors).

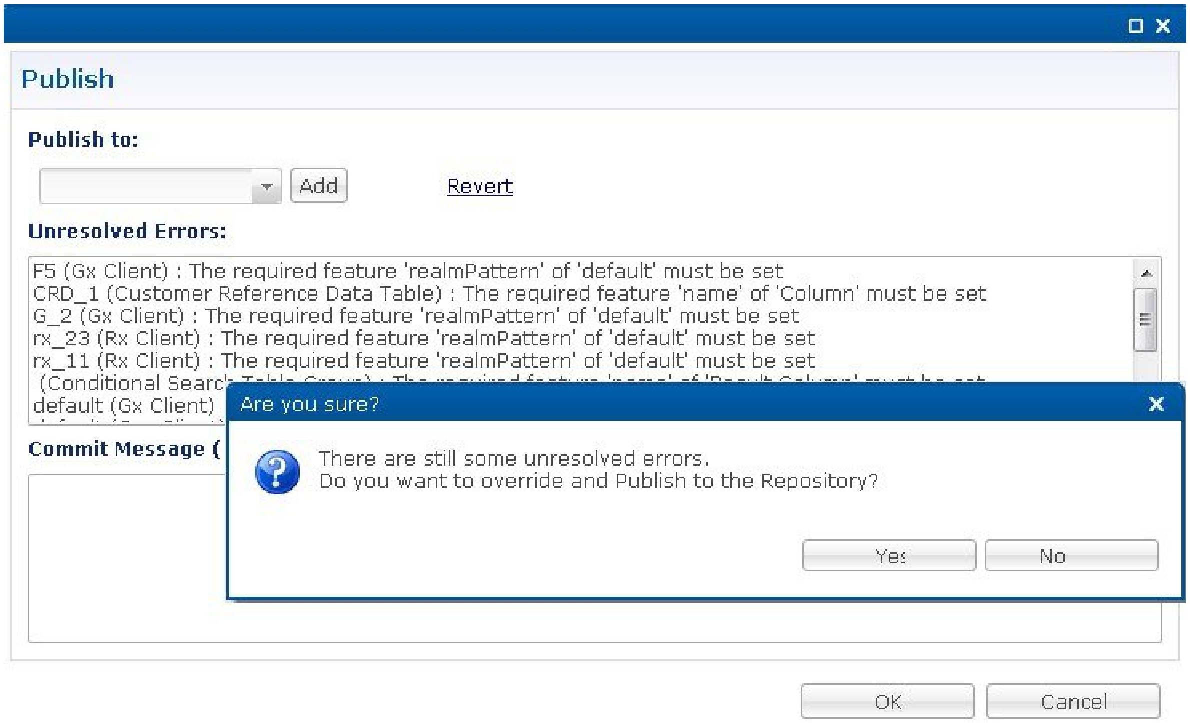
Figure 13: Publish - Unresolved Errors



F5 (Gx Client) : The required feature 'realmPattern' of 'default' must be set
CRD_1 (Customer Reference Data Table) : The required feature 'name' of 'Column' must be set
G_2 (Gx Client) : The required feature 'realmPattern' of 'default' must be set
rx_23 (Rx Client) : The required feature 'realmPattern' of 'default' must be set
rx_11 (Rx Client) : The required feature 'realmPattern' of 'default' must be set
(Conditional Search Table Group) : The required feature 'name' of 'Result Column' must be set
default (Gx Client) : The required feature 'realmPattern' of 'default' must be set

If you click **OK** with any unresolved errors in the list then you are prompted with a confirmation asking if the unresolved errors should be published to the repository.

Figure 14: Publishing with Errors - Override



F5 (Gx Client) : The required feature 'realmPattern' of 'default' must be set
CRD_1 (Customer Reference Data Table) : The required feature 'name' of 'Column' must be set
G_2 (Gx Client) : The required feature 'realmPattern' of 'default' must be set
rx_23 (Rx Client) : The required feature 'realmPattern' of 'default' must be set
rx_11 (Rx Client) : The required feature 'realmPattern' of 'default' must be set
(Conditional Searc
default (Gx Client)

There are still some unresolved errors.
Do you want to override and Publish to the Repository?

If you click **No**, then the publish does not happen.

If you click **Yes** then the commit message is amended to include a note that you have committed with **# errors**. For example, "`User forced the Publish with 3 unresolved errors: <user's commit message>`".

Masking Errors

You can mask the errors if needed where an error is reported by Policy Builder but can still be loaded by the Policy Server. This allows configuration of CPS so that the specified errors are not displayed and you do not ignore the list of unresolved errors and the real errors are not lost amongst a list of acceptable errors.

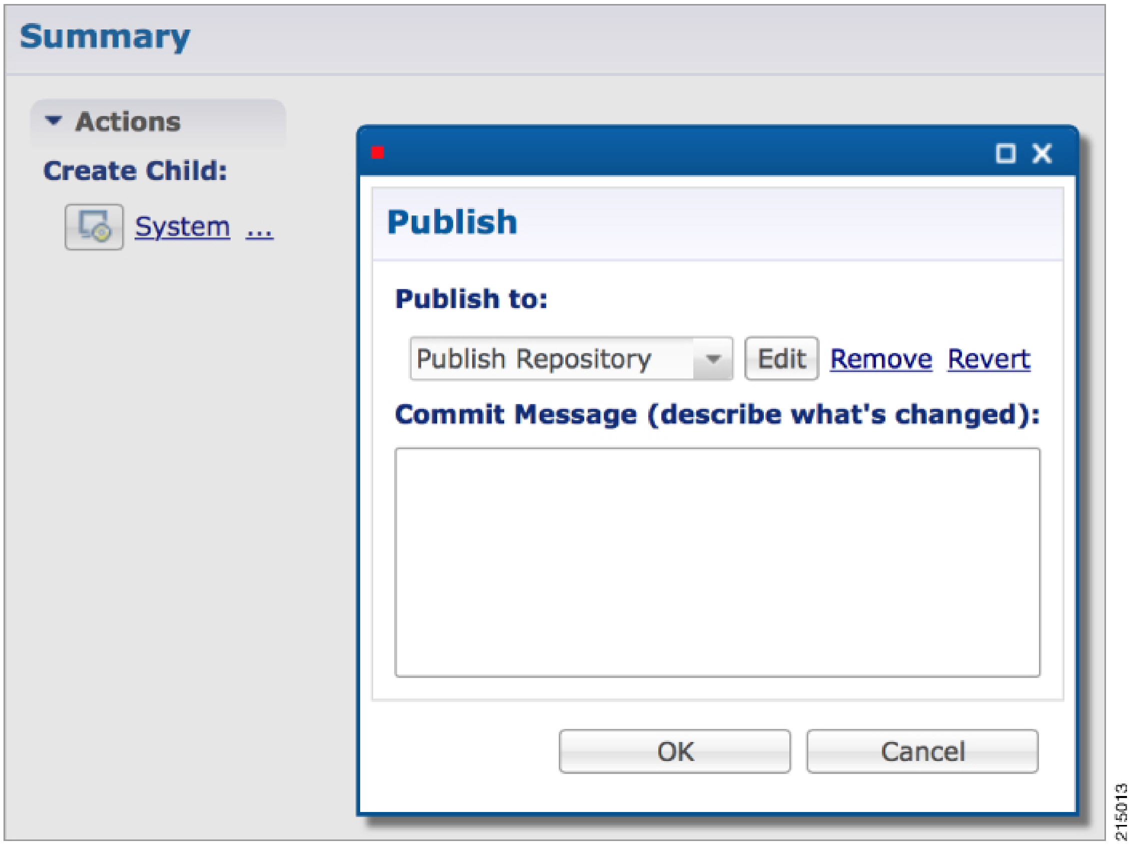
The file named `maskPublishErrors.txt` file is created in the folder `/etc/broadhop/pb` on Cluster Manager (CM). After creating the file, run `build_all.sh` from CM to rebuild CPS package and push the changes to each VM. The file is populated with the exact message displayed in the GUI. No wildcarding is allowed (so as to prevent accidentally filtering out important messages). The GUI does not display any messages that are in the `maskPublishErrors.txt` file. The GUI does not count any messages that are in the `maskPublishErrors.txt` file. If all of the errors in the list are masked because they are in the file then clicking **OK** in the **Publish** dialog will not cause the override dialog to be displayed.

Adding a Runtime Repository Definition

A repository definition named **Publish Repository** is installed by default and uses the default Runtime repository (http://pcrfclient01/repos/run). The default Policy Builder user (*qns-svn*) with the default password is also setup. The Runtime repository matches the value setup in the `/etc/broadhop/qns.conf` file.

The `qns.conf` file is read by all of the active Policy Server and Policy Director nodes and when the policy server process starts up, it checks out the configuration from the Runtime repository.

Figure 15: Runtime Repository Definition



Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list on the **Choose Policy Builder data repository...** dialog box to select the desired repository.

Step 3 After selecting the required repository, click **OK**.

Step 4 Make changes to Policy Configuration data as necessary.

Step 5 Select **File** > **Publish to Runtime Environment...**.

Step 6 Use the drop-down list to select **<Add New Repository>**.
The **Repository** dialog box appears.

Step 7 Enter the necessary values and click **OK** to save your work.

Step 8 Enter a commit message and click **OK** to publish to the new repository.

Editing a Runtime Repository Definition

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list on the **Choose Policy Builder data repository...** dialog box to select the desired repository.

Step 3 After selecting the required repository, click **OK**.

Step 4 Make changes to Policy Configuration data as necessary.

Step 5 Select **File** > **Publish to Runtime Environment...**.

Step 6 Use the drop-down list to select the desired repository.

Step 7 In the **Repository** dialog box, make your changes.

Step 8 Click **OK** to save the changes to the repository definition.

Step 9 Enter a commit message and click **OK** to publish to the new repository.

Removing a Runtime Repository Definition

This procedure removes a runtime repository definition from the Cisco Policy Builder. This procedure does not delete the actual Subversion repository, just the definition for access in the Policy Builder.

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list on the **Choose Policy Builder data repository...** dialog box to select the desired repository.

Step 3 After selecting the required repository, click **OK**.

Step 4 Make changes to Policy Configuration data as necessary.

Step 5 Select **File** > **Publish to Runtime Environment...**.

Step 6 Use the drop-down list to select the desired repository.

Step 7 Click **Remove**. A confirmation dialog appears.

Step 8 Click **OK** to delete the repository.

Step 9 Click **Cancel** to close the dialog box.

Saving Policy Builder Configuration Data to a Runtime Repository

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list in the **Choose Policy Builder data repository...** dialog box to select the desired repository.

Step 3 After selecting the required repository, click **OK**.

Step 4 Make changes to Policy Configuration data as necessary.

Step 5 Select **File** > **Publish to Runtime Environment...**.

Step 6 Use the drop-down list to select the desired repository.

Step 7 Enter a commit message.

Step 8 Click **OK**. The data will be saved to the client repository for later updating and publish to the runtime environment.

Switching to a Different Client Repository

You may have several variations of your client repository. One may reflect the configuration currently published to the server. Another might be developed for test purposes.

There are two ways to switch to a different repository:

- **File** > **Switch Repository...**
- **File** > **Exit/Logout**: You can select the required repository from **Choose Policy Builder data repository...** dialog box.

When you click **Ok** after repository selection, a validation prompt **Are you sure?** is displayed.

- Select **Discard** to discard the uncommitted changes.
- Select **Retain** to retain the uncommitted changes.

If the dialog box is dismissed without clicking escape or close, the uncommitted changes are retained.

Reverting Changes

There are two main SVN repositories (repos) in the system.

- Repository publish which contains ONLY the currently running set of policies.
- Runtime repository which contains a copy of the currently running set of policies along with copies of all previous sets.

To rollback Policy Builder changes, there are two methods:

- Rollback the configuration repository Policy Builder and then perform a publish as described in Unpublished Changes, on page 22.
- Rollback the runtime repository Policy Builder uses and the configuration repository Policy Builder uses.

  For more information, refer to Published Changes, on page 22.

Unpublished Changes

If you do not want to save the changes, click the **Revert** link on the Policy Builder start window. All changes that have not been committed to a repository will be removed.

Step 1 Open a browser and enter the URL of the Cisco Policy Builder.

Step 2 Use the drop-down list in the **Choose Policy Builder data repository...** dialog box to select the desired repository.

Step 3 Click the **Revert** link. A confirmation dialog appears.

The **Revert** link is only available if there are uncommitted local changes.

Step 4 Click **OK** to revert changes to the repository definition.

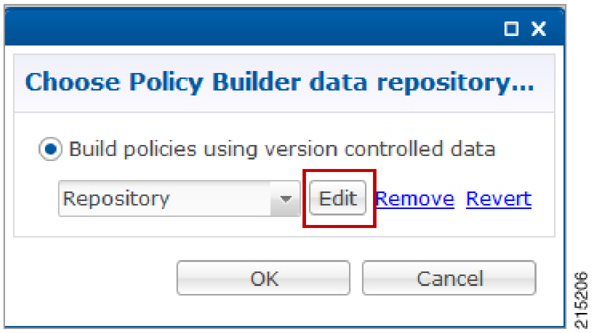
Published Changes

Step 1 Check the configuration repository name Policy Builder uses (config_repo). To check the name, use the following steps:

a) Open a browser and enter the URL of the Cisco Policy Builder.

b) In the **Choose Policy Builder data repository...** dialog box, click **Edit**.

Figure 16: Choose Policy Builder Data Repository



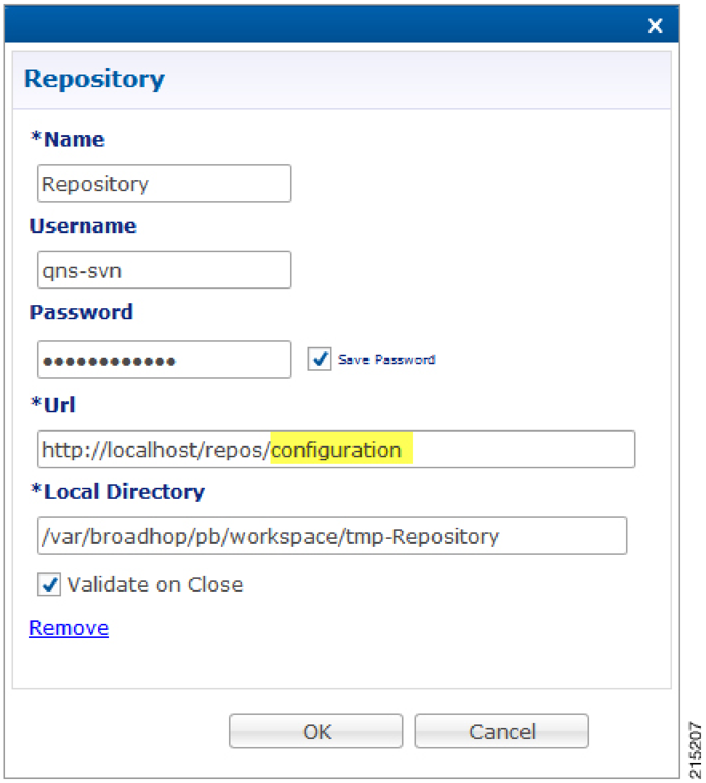
Choose Policy Builder data repository...

● Build policies using version controlled data

Repository

c) In the **Repository** dialog box, look at the contents of the **Url** field to see the repository name used by the Policy Builder. For example, it is **configuration**.

Figure 17: Repository



Repository

*Name

Repository

Username

qns-svn

Password

●●●●●●●●●●●● ☑ Save Password

*Url

http://localhost/repos/configuration

*Local Directory

/var/broadhop/pb/workspace/tmp-Repository

☑ Validate on Close

d) Record the Policy Builder repository name (config_repo). For example, it is **configuration**.

Step 2 To locate the ‘r’ number in the repository used by Policy Builder, execute the following command:

```
svn log http://pcrfclient01/repos/<config_repo> | more
```

The <*config_repo*> value comes from Step 1.d, on page 23.

The following is an example of the **svn log** command, where <*config_repo*> is **configuration** as shown in Step 1.d, on page 23.

```
svn log http://pcrfclient01/repos/configuration | more
------------------------------------------------------------------------
r367 | qns-svn | 2015-06-18 12:15:34 -0600 (Thu, 18 Jun 2015) | 1 line
second try
------------------------------------------------------------------------
r364 | qns-svn | 2015-06-17 15:46:19 -0600 (Wed, 17 Jun 2015) | 1 line
corrected java issue
------------------------------------------------------------------------
r361 | qns-svn | 2015-06-16 15:38:28 -0600 (Tue, 16 Jun 2015) | 1 line

Added new Policies
------------------------------------------------------------------------
r358 | qns-svn | 2015-06-16 15:06:57 -0600 (Tue, 16 Jun 2015) | 1 line
""
------------------------------------------------------------------------
r355 | qns-svn | 2015-06-16 14:58:41 -0600 (Tue, 16 Jun 2015) | 1 line
""
------------------------------------------------------------------------
r352 | qns-svn | 2015-06-16 14:52:29 -0600 (Tue, 16 Jun 2015) | 1 line
```

a) In the example above, the comment we are looking for is in **r361** which is the ‘r’ number we want to rollback to.

b) Record the **config_repo ‘r_number’**. In this example, it is **r361**.

Step 3 Execute the following command to delete the current version from the configuration repository Policy Builder uses:

```
svn delete http://pcrfclient01/repos/<config_repo> -m ‘deleting for rollback’
```

Use the <*config_repo*> value from Step 1.d, on page 23.

The following is an example of the `svn delete` command where <*config_repo*> is **configuration**.

```
svn delete http://pcrfclient01/repos/configuration -m ‘deleting for rollback’
```

Step 4 Execute the following command to restore the Policy Builder configuration repository to a previous version.

```
svn cp http://pcrfclient01/repos/<config_repo>@<r_number> http://pcrfclient01/repos/<config_repo> -m
‘rolling back to <r_number>’
```

The <*r_number*> value is from Step 2.a, on page 24 and the <*config_repo*> value is from Step 1.d, on page 23. The ‘-m’ option should be used to add a comment indicating what is being done.

The following is an example of the `svn copy` command with the <*r_number*> set to **361** and the <*config_repo*> set to configuration:

```
svn cp http://pcrfclient01/repos/configuration@361 http://pcrfclient01/repos/configuration -m ‘rolling
 back to 361’
```

Step 5 Execute the following command to verify if the rollback is successful:

```
svn log http://pcrfclient01/repos/<config_repo> | more
```

The <*config_repo*> value is from Step 1.d, on page 23.

The following is an example of the **svn copy** command:

```
svn log http://pcrfclient01/repos/configuration | more
-----------------------------------------------------------------------
r367 | qns-svn | 2015-06-18 12:15:34 -0600 (Thu, 18 Jun 2015) | 1 line
rolling back to 361
-----------------------------------------------------------------------
```

Note The output should have the ‘-m’ option's text entered in Step 4, on page 24 as the comment.

Step 6 Open Policy Builder and verify the polices to which you have rolled back. Normally the customer should be able to verify the policies in Policy Builder.

Step 7 Perform a publish in Policy Builder and make sure to add a comment indicating that the publish is being done to complete the rollback. For example, “publishing to complete rollback to <*r_number*>”.

System Configuration

The Systems node in the Reference Data tab represents the Cisco Policy Suite runtime environment as it exists in the network environment.

- System: There must always be at least one system defined in the Policy Builder. The system represents the customer deployment. In HA, the system represents a set of PCRF clusters that share the same session database. System is used to define any common things across the clusters, such as load balancing, and so on.
- Cluster: Each system contains one or more clusters - each of which represents a single High-Availability (HA) site environment. A cluster is used for define the configurations related to the blades. A cluster shares the same set of policy directors (that communicates as a group). A customer can take a fully installed PCRF and replicate it to a second cluster.

  Each cluster can contain node instances. A node instance corresponds to a physical node in a deployment cluster such as a session manager or Policy Director (load balancer). It is very rare that a deployed system needs to have node instances configured in the Policy Builder. Configurations flow downhill, meaning that if you define a Plugin Configuration for Unified API at the system level, each cluster and subsequently each instance gets that configuration by default.

  There are two types of clusters: HA and GR. This document discusses HA clusters. For information related to GR clusters, refer to *CPS Geographic Redundancy Guide* for this release.

Note In an HA environment you should not make any configuration in Cluster node.

Plug-in configuration done at cluster level overrides the same definition at system level. For example, if you configure Custom Reference Data at cluster level, it will override the Custom Reference Data configuration done at system level.

There is a default deployment configuration for mobile. **system-1** is the default system name and **cluster-1** is the default cluster name.

If a customer wants to change the system name, they need to change it in `qns.conf` (`/etc/broadhop/qns.conf`) file also to reflect it in Policy Builder:

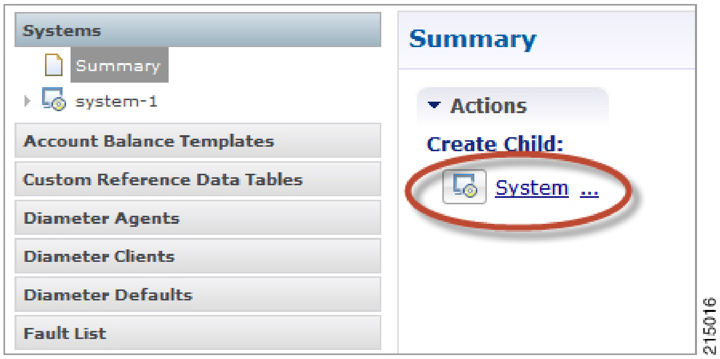
```
-Dcom.broadhop.run.systemId=<system name>
```

Adding a System

After installation, use this procedure to set up your Cisco Policy Builder by using an example populated with default data. You can change anything that does not apply to your deployment.

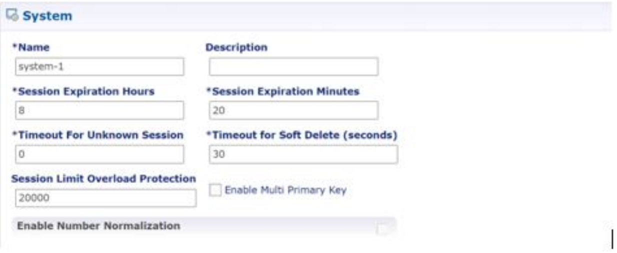
Step 1 Click the **Reference Data** tab, and then click the **Systems** node to display the **Systems** tree.

Figure 18: Systems Tree



Step 2 Click **System...** under **Create Child:** to open the **System** pane on the right side.

Figure 19: System Pane



System

*Name: system-1

Description:

*Session Expiration Hours: 8

*Session Expiration Minutes: 20

*Timeout For Unknown Session: 0

*Timeout for Soft Delete (seconds): 30

Session Limit Overload Protection: 20000

☐ Enable Multi Primary Key

Enable Number Normalization

Step 3 Fill in the **Name** field, and provide a description of this system. Enter the rest of the parameters based on your network requirements.

Table 3: System Parameters

Parameter	Description
Name	The name of the CPS system.
Description	Description of this entire system.
Session Expiration Hours	If no messages are received in x hours, the session will be removed. **Note** The maximum value allowed for this parameter is 590 hours. However, the combination of the number of hours specified for this parameter and the number of minutes specified for the **Session Expiration Minutes** parameter cannot exceed 35,400 minutes. Default value is 8.

Parameter	Description
Session Expiration Minutes	If no messages are received in x minutes, the session will be removed. **Note** The combined value of **Session Expiration Hours** multiplied by 60 plus **Session Expiration Minutes** should not exceed 35,400. Default value is 0.
Timeout for Unknown Session	Time in minutes that CPS keeps a session alive after the subscriber logs off. With this, other network entities involved in the session can let the session close gracefully. Default value is 0.
Timeout For Soft Delete	Determines the time in seconds during which a 'soft delete' session is maintained for a CPS session after session stop. Default value is 30.
Session Limit Overload Protection	This parameter is used to protect the session database from crashing. CPS does not allow session creation when a current system session count exceeds the **Session Limit Overload Protection** value. The default value is set to 0 which infinitely accepts the Diameter messages and CPS triggers alarms so that you change the value before session count goes beyond the database capacity. This value must be replaced by session capacity that is calculated for each deployment. Default value is 0. **Note** Session Limit Overload Protection value must be changed than using the default value (0). **Note** The recommended value for **Session Limit Overload Protection** has to be derived by Cisco Account representative for each deployment.
Enable Multi Primary Key	Select this check box to allow two primary keys to be utilized by maintaining a map of each separate primary key and storing the 'true' multi-primary key as a UUID related to the two maps. Changing this setting has a negative performance impact and should only be done at the request of the BU. Recommendation is to keep Enable Multi Primary Key unchecked. Default is unchecked.
Enable Number Normalization	Select this check box to enable number normalization under system configuration. The following fields are displayed under **Number Normalization List**: • Number Type - Type of IMSI/MSISDN. • Number Length - Length of the normalized IMSI/MSISDN. • Number Prefix - Prefix to be normalized from the number.
Cluster link	Click this link to create a cluster under this system.
Current System Link	Click this link to make a copy of this system, with its clusters and instances.

Step 4 If the created system needs to be used, then after publishing, the following property needs to be updated in the `qns.conf` configuration file:

```
-Dcom.broadhop.run.systemId=<system name>
```

where <*system name*> is the system name defined in the Step 3, on page 26.

Soft Delete Session

A soft delete session is an entry in the session database which maintains session data after session stop with an auto-generated unique primary key, but still maintains needed secondary keys. This allows messages which come after session stop to still be processed while also allowing a session with the same primary key to be immediately created. The CPS code determines when soft delete sessions are required and what secondary keys are needed.

Soft Delete Example (Mobile)

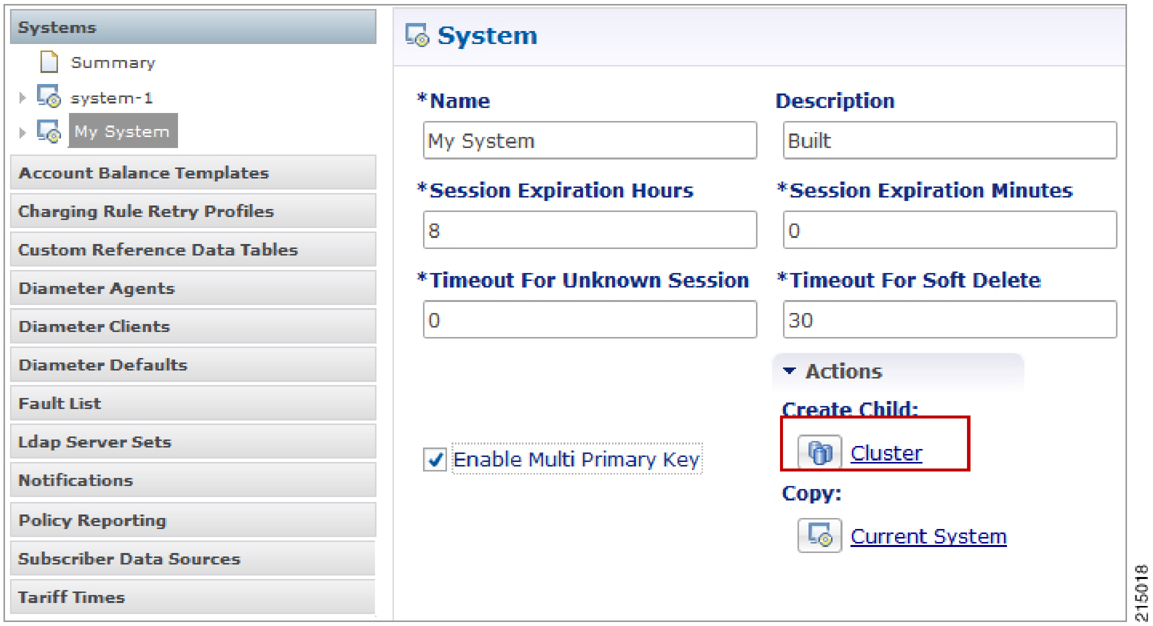
A Gx session with a Gy associated session exists. A Gx CCR-T is received that terminates the CPS session, resulting in a soft-delete session which contains Gy session information and associated Gy secondary keys. A Gy CCR-t is received and the soft-delete session is loaded and updated with the charging information through the end of the session. After the soft delete timeout, the soft delete session is removed.

Adding an HA Cluster

This section describes how to add an HA cluster. Asystem, a cluster, and an instance are set up at install time. If you have to change the cluster definition, or want to add more clusters, use these steps.

Step 1 In the **REFERENCE DATA** tab, under the **Systems** node, click your default system.

Figure 20: System Configuration



*Name: My System

Description: Built

*Session Expiration Hours: 8

*Session Expiration Minutes: 0

*Timeout For Unknown Session: 0

*Timeout For Soft Delete: 30

☑ Enable Multi Primary Key

Step 2 Under Actions, click the **Cluster** link to set up your cluster.

Since some data is relevant at the cluster level, you must always have at least one cluster (by default), even if it is a cluster of one instance.

Configure the following cluster parameters.

Table 4: Cluster Parameters

Parameter	Description
Name	The name of the cluster. This name must correspond to the value stated in the `com.broadhop.run.clusterId` parameter in `qns.conf` file on the Cisco Policy Server.
Description	A brief description of the cluster.
Db Write Concern	Controls the write behavior of the Session Manager, and specifies for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace, and Endpoint databases. Select one of the following options from the drop-down list: • OneInstanceSafe: The system waits for writing confirmation in primary member. • TwoInstanceSafe: The system waits for writing confirmation in the primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.

Parameter	Description
Failover Sla Ms	Specifies the time period, in milliseconds, to wait before starting failover database handling. Default value is 0 milliseconds.
Replication Wait Time	Specifies the time limit, in milliseconds, for the Db Write Concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern. This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. Default value is 100 milliseconds.
Trace Db Size Mb	Determines the size of the policy_trace database capped collection in megabytes. The capped collection never grows higher than the configured size. This parameter is applied to the Trace database. Default value is 512. For more information, see *Policy Tracing and Execution Analyzer* section in *CPS Operations Guide*.
SK Evaluation Time In Minutes	This parameter is used to avoid querying same secondary keys. Default vale is 60 minutes.

Parameter	Description
Max Timer T P S	Specifies the maximum number of internally generated transactions per second (TPS) the system produces. This parameter affects the RAR generated by CPS when they are triggered by an internal time event (change of time or quota refresh). For example, if the system needs to generate RAR messages to refresh quotas, the max TPS for the creation of the RAR messages is limited by this value. Default value is 2000. Internal timer TPS is calculated based upon the value specified for Max Timer TPS in Policy Builder, number of session shards, and number of Policy Server (QNS) VMs. Max Timer Expired TPS = (Max Timer TPS / Number of Session Shards) * (Lower of Number of Session Shards or Policy Server (QNS)) Here are examples that specify how the internal timer TPS is calculated: a. **When number of session shards are higher or same as number of QNS VMs:** If configured Max Timer TPS in Policy Builder is 2000, number of session shards are 88 and number of QNS are 50. In this case, max TPS per QNS VM is 2000/88 (no. of session shards) = 22 (value in floored). Actual maximum timer TPS is 22 * 50 (no. of QNS) = 1100. b. **When number of session shards are lower than QNS VMs:** If configured Max Timer TPS in Policy Builder is 2000, number of session shards are 12 and number of QNS are 20. In this case, max TPS per QNS VM is be 2000/12 (no. of session shards) = 166 (value is floored). Actual maximum timer TPS is 166 * 12 (no. of session shards) = 1992. **Note** In case there is CPS blade expansion, Max Timer T P S parameter must to be tuned to handle internal RAR TPS. For more information, contact your Cisco Account representative.

Parameter	Description
Re-evaluation diffusion buckets	Specifies the number of batches, or “buckets”, into which CPS divides the transactions to be processed when the rate limiting TPS function of CPS is triggered. The rate limiting feature is defined in the **Max Timer T P S** field above. When a TPS rate limit condition is encountered, CPS divides the total number of re-evaluation transactions to be processed by the number of buckets defined in this field. CPS processes the transactions in each bucket, one by one, while also adding a brief delay between the processing of each bucket. Refer to the **Re-evaluation diffusion interval** parameter below to configure this delay. This functionality prevents spikes in traffic when a large number of sessions qualify for re-evaluation at the exact same time. This functionality only diffuses the rate at which transactions are sent to the CPS policy engine. It does not wait for end-to-end processing to occur. To disable this functionality, set both **Re-evaluation diffusion buckets** and **Re-evaluation diffusion interval** parameters to 0 (zero). If the TPS rate limiting functionality has been disabled, this functionality is also disabled. Default value is 50 (buckets).
Re-evaluation diffusion interval (in milliseconds)	Specifies the delay, in milliseconds, before processing the next bucket. Enter the sum of all the delays between all the buckets. Assuming **Re-evaluation diffusion buckets** is configured as 50, and the **Re-evaluation diffusion interval** is configured as 20000 milliseconds, it introduces a delay of 408 milliseconds before proceeding with the next bucket of transactions. Delay between buckets = Diffusion Interval (ms) / (Diffusion Buckets - 1) Delay between buckets = 20000/49 Delay between buckets = 408 (ms) Default value is 20 milliseconds. With default configuration, there will be no diffusion. As 20/50 will be 0 (It ignores decimal).
Broadcast Msg Wait Timer Ms	Specifies the time period, in milliseconds, for the Policy Engine to wait between sending each Broadcast Policy Message. Default value is 50.
Max Sessions Per Shard	Specifies the maximum number of sessions that can be stored in each shard that has been created within a Session Database Replica Set. Value ‘0’ in this parameter means that monitoring is not implemented. **Note** It is recommended to add new shards and rebalance sessions during maintenance window. Default value is 0.

Parameter	Description
Lookaside Key Prefixes	To improve Gx/Rx lookup and caching performance, we can add the lookaside key prefixes. In order to identify the correct shard for subscriber lookup/query, the PCRF needs to know the secondary key (which is internally stored in secondary key cache) for mapping and the exact shard that will be queried for subscriber data. This helps prevent the system from scanning/querying all the available shards in the system to fetch the subscriber record. Reducing the data range for scanning/querying leads to enhanced system performance. The following keys should be added so that the secondary keys for session binding are stored in the secondary key cache. • diameter - This key should be added for local session affinity or when Sh interface is in use. • RxTGPPSessionKey - This key should be added only when Rx interface is used. • FramedIpKey - This key should be added if Gx Session lookup is based on IPADDRESS. • framedIpV6PrefixKey - This key should be added if Gx Session lookup is based on IPADDRESS. • USuMSubscriberIdKey – This key should be added only when SPR is used. • MSBMSubscriberIdKey – This key should be added only when balance is used. • RxClientSessionKey - This key should be added if PAS health check feature is enabled. • imsiApnKey - This key should be added if Gx Session lookup based on IMSI and APN is enabled or Load by IMSI and Load By Called Station ID is enabled. • msisdnApnKey - This key should be added if Gx Session lookup based on MSISDN and APN is enabled. • userIdentityKey - This key should be added when Sh related messages have 'msisdn' AVP or Sh profile has sipUri related information. CPS uses this key to find the session based on the message AVPs present in the request message. For example, when MSISDN is present in request message and sipUri information is present in profile. This would prevent the system from scanning/querying all the available shards in the system to fetch the subscriber record, which eventually leads to enhanced system performance. **Note** For GR setup, a Lookaside Key Prefix called **single** must be added under the Cluster session for each Cluster for faster session Lookups based on memcache when SingleSy feature is enabled.

Parameter	Description
Disable Secondary Key Full Scan D B For Selected Keys	Specifies whether full scan for secondary key database lookups is enabled or disabled. By default, it is enabled. Disabling secondary key database lookups helps in reducing PCRF processing latencies. To disable full scan for specific keys: • Uncheck **Disable Secondary Key Full Scan DB For All Keys** • Add the list of key prefixes to be disabled for full scan
Disable Secondary Key Full Scan DB For All Keys	Enable or disable full scan for secondary key database lookups. By default, the secondary key database lookups is enabled (unchecked). Disabling secondary key database lookups helps in reducing PCRF processing latencies. If this is checked, when the memcache look up fails for a secondary key, the full database scan to find the session in database is not performed. **Note** When the secondary full scan database is disabled, number of 5065 errors thrown increases as memcache works on UDP and looking memcache alone can cause missed sessions count to increase.
Suppress Error Audit Traces To Trace DB	When enabled the application does not write error audit traces logs into `error_traces` collection. When disabled the application writes error audit traces logs into `error_traces` collection. Default value is enabled.
Session Tag Padding Configuration	To enable the Session Tag Padding Configuration, select (true) the checkbox. By default the checkbox is not selected (false). Makes sure that the MongoDB subscriber session size is consistent throughout the subscriber session life cycle. **Note** After performing a fresh installation or an upgrade, you must ensure the following conditions are met: • In multi-cluster setup, session tag padding feature related configuration should be same for all the PCRF clusters. • In multi-cluster setup, session tag padding feature related configuration should be same for all the UDC clusters. • Session tag padding feature configurations can be different for PCRF and UDC configuration.

Parameter	Description
Enable Session Query Without Padding	Enables the system to query for secondary key without padding. This parameter is required when there are old subscriber sessions (tag value without padding) and new subscriber sessions (with tag value with padding character) exists in the MongoDB. In case the system does not find the session using the key with padding data, system attempts to find the session using key without padding. This flag enables the system to trigger the query without padding. By default the checkbox is selected (true). **Note** For fresh installations, set **Enable Session Query Without Padding** to **false** and publish the Policy Builder. When upgrading the system, set the **Enable Session Query Without Padding** to **true** and publish the Policy Builder.
Initial Number Of Tags	Determines the total number of tags (including reserved tags) in the tag list of subscriber session header part to be created while creating subscriber session. This helps CPS system to have the constant size for subscriber session at runtime. To disable this configuration, set the value to 0. Reserved tags are not created when the value configured as 0. Default value is 10. **Note** If the number of secondary key/tags exceeds the predefined *Initial Number Of Tags*, system stores the additional tags. For example, if *Initial Number Of Tags* is configured as 10 and at runtime list of tags (from subscriber session document) need to store 12 tags, system stores 12 tags without rejecting any request.
Admin Database	• Primary Database IP Address: The IP address of the session manager database that holds session information for Cisco Policy Builder and Cisco Policy Server. • Secondary Database IP Address: The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pairs architecture. This field is present but deprecated to maintain downward compatibility. • Database Port: Port number of the database for session data. Default value is 27717. It is recommended to set port to 27721 or any other port different than 27717 so that the admin database is not in the same replica-set as sessions (it is tmpfs) and data can be lost.

Parameter	Description
Endpoint Database	This database refers to the endpoint collections under diameter and queuing DB. The endpoint database under diameter database has the information about the peers between CPS and other nodes. For example, GW. The endpoint database under queueing database has the information about the connectivity between Policy Director (LB) and Policy Server (QNS) VMs. • Primary Database IP Address: The IP address of the session manager database that holds session information for Cisco Policy Builder and Cisco Policy Server. • Secondary Database IP Address: The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pairs architecture. This field is present but deprecated to maintain downward compatibility. • Database Port: Port number of the database for Session data. Default value is 27717.
Trace Database	• Primary Database IP Address: The IP address of the session manager node that holds trace information, which allows for debugging of specific sessions and subscribers based on unique primary keys. • Secondary Database IP Address: The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pairs architecture. This field is present but deprecated to maintain downward compatibility. • Database Port: Port number of the database for Session data. Default value is 27717. For more information, see *Policy Tracing and Execution Analyzer* section in *CPS Operations Guide*.
Data Centre Parameter	Deprecated
Common Time Changes	Deprecated

Step 3 From the Systems tree, open up the cluster that you just added and check the plug-in configurations.

The configurations that you specify here are used only at the cluster level, and cascade down to the instance level if no configuration is set on the instance.

At this point, the plug-ins are available to the cluster but are not configured.

Click any one of them to open the detailed page in the right pane, and check and set your own configuration data. However, there is rarely a need to use the Threading Configuration or the Async Threading Configuration unless instructed to do so.

Step 4 If the configured cluster has to be used, after publishing, the following parameter must be updated in the `qns.conf` configuration file:

```
-Dcom.broadhop.run.clusterId=<cluster name>
```

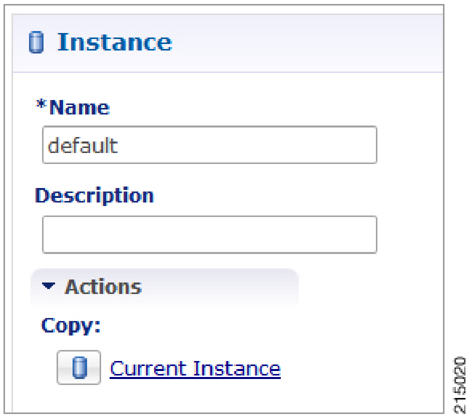
where, <*cluster name*> is the cluster name defined in Policy Builder.

Adding an Instance

Step 1 Begin with a Cluster at the **Systems** node in the **Reference Data** tab.

Step 2 Under **Create Child:**, click the **Instance** link to open the **Instance** pane.

Figure 21: Instance Configuration



Instance

*Name

default

Description

Step 3 Type the **Name** and **Description**.

Step 4 From the **Systems** tree, open up the instance node that you just added and check the plug-in configurations.

At this point, plug-ins are available but not configured at the instance level.

Click any one of the plug-ins to open the detailed page in the right pane and check and set your own configuration data.

Any of the configuration data you have here are used at the instance level, overriding any plug-ins set at the system level or the cluster level.

Adding a GR Cluster

At install time, a system, cluster, and instance are set up. If you need to change the cluster definition, or want to add others, use the information mentioned in Adding an HA Cluster and Endpoint Database Configuration.

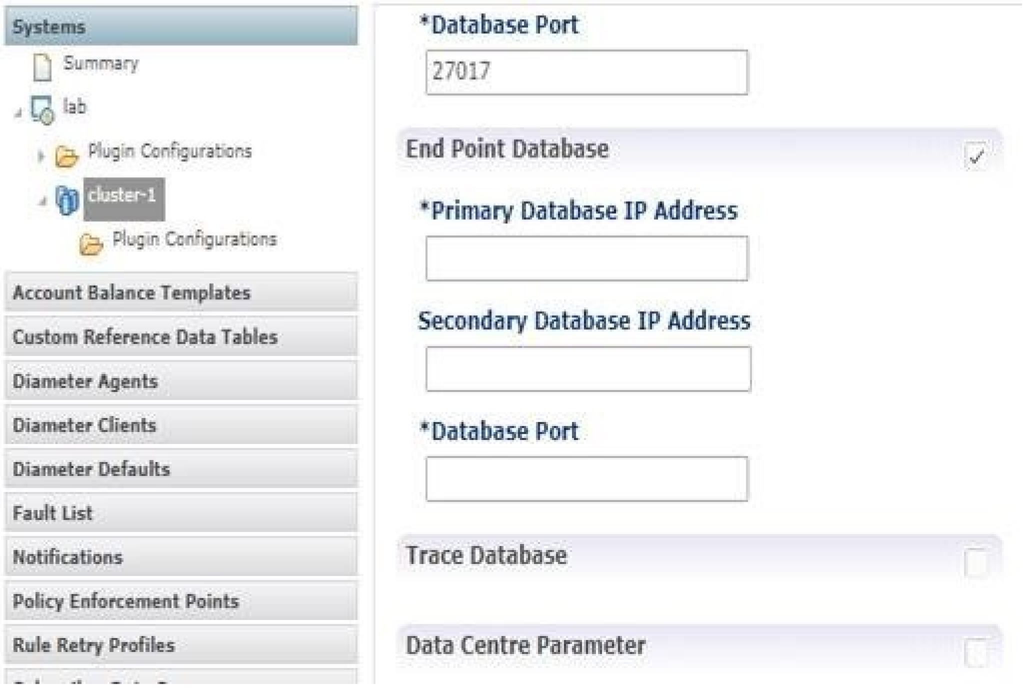
For configuration details, refer to Adding an HA Cluster, on page 28.

For Endpoint Database parameters, refer to Endpoint Database Configuration, on page 38.

Endpoint Database Configuration

For GR setup, Endpoint Database should be configured local to the site under Reporting/Balance Database.

Figure 22: Endpoint Database



*Database Port: 27017

End Point Database ☑

*Primary Database IP Address:

Secondary Database IP Address:

*Database Port:

Trace Database □

Data Centre Parameter □

CHAPTER 3

Plug-in Configuration

Overview

In CPS, reference data is considered information that is needed to operate the policy engine, but not used for evaluating policies. For example, in the **Reference Data** tab in Cisco Policy Builder, are the forms used to define systems, clusters, and instances, and to set times and dates used for tariff switching. The policy engine needs to refer to this data only to process policies correctly. However, the data does not define the policy itself.

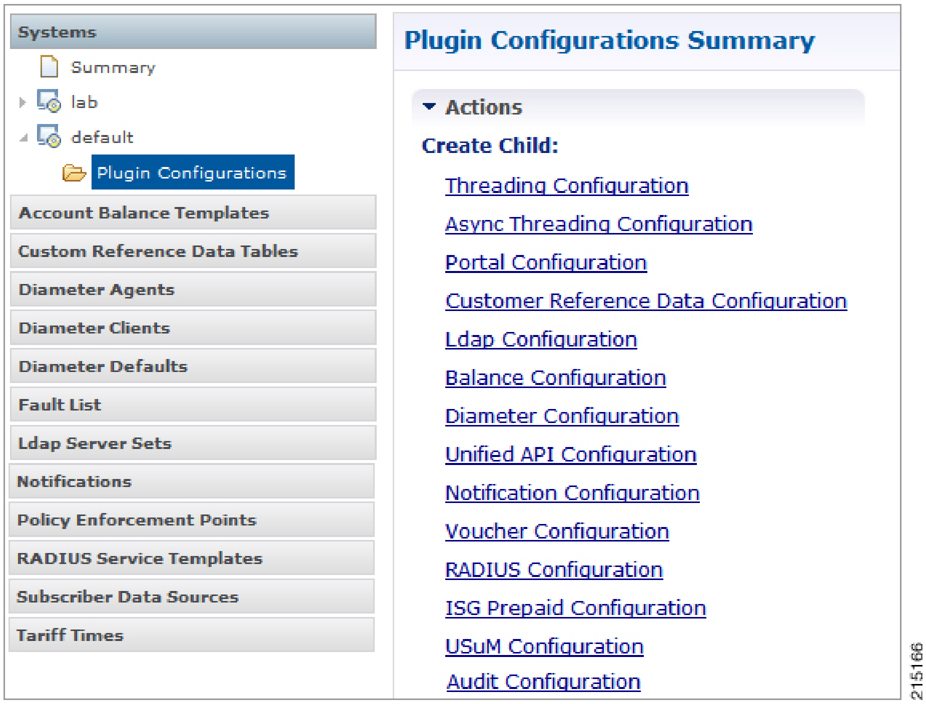
Cisco Policy Builder provides core plug-ins for customizing and optimizing your installation.

- Configurations set at the system level are system-wide except as noted in the bullet items below.
- Configurations set at the cluster level apply to that cluster and the instances in it. A value set here overrides the same value set at the system level.
- Configurations set at the instance level apply to the instance only and override the same value set at the cluster or system level.

Select the **Create Child** action in a **Plug-in Configuration** node in the **Systems** tree to define them. You can change any of the variables from the default, or choose not to use a plug-in, as necessary.

When you create a system from the example, the following configuration stubs appear at the cluster and instance level:

Figure 23: Create Child Action



Systems
- Summary
- lab
- default
  - Plugin Configurations

Account Balance Templates

Custom Reference Data Tables

Diameter Agents

Diameter Clients

Diameter Defaults

Fault List

Ldap Server Sets

Notifications

Policy Enforcement Points

RADIUS Service Templates

Subscriber Data Sources

Tariff Times

Plugin Configurations Summary

Actions

Create Child:

- Threading Configuration
- Async Threading Configuration
- Portal Configuration
- Customer Reference Data Configuration
- Ldap Configuration
- Balance Configuration
- Diameter Configuration
- Unified API Configuration
- Notification Configuration
- Voucher Configuration
- RADIUS Configuration
- ISG Prepaid Configuration
- USuM Configuration
- Audit Configuration

You are notified when a new policy is applied that overrides the existing configuration.

The notification is displayed as a warning icon above the configuration heading. When you hover over the warning icon, it displays the notification message as a tooltip. When there is an error and warning in the plugin configuration, then the error is overridden by a warning message.

A warning message is displayed under the following conditions:

- At the System level, if the selected plugin configuration is overridden by cluster or Instance plugin configuration.
- At the Cluster level, if the selected plugin configuration overrides the same plugin configuration at the system level or is overridden by the same plugin configuration at an Instance level.
- At the Instance level, if the selected plugin configuration overrides the same plugin configuration at system or cluster level.

Threading Configuration

A threading configuration utility is provided for advanced users.

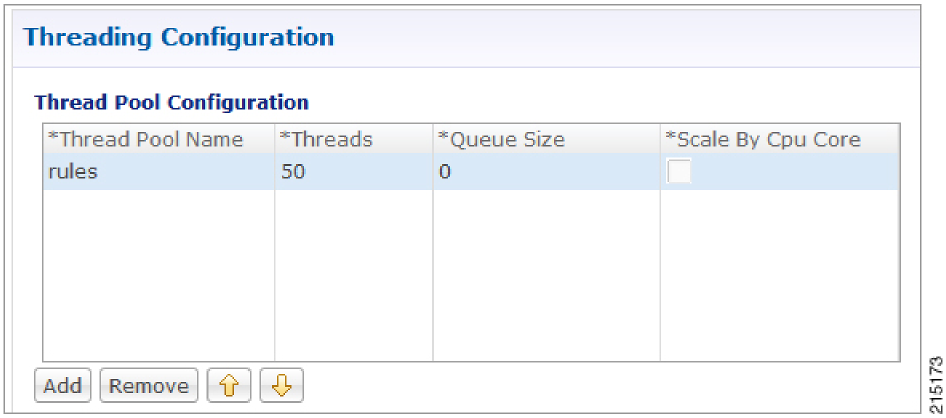
Click **Threading Configuration** in the right pane to add the threading configuration to the system. This is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware. For further information, contact your Cisco Account representative.

The Threading Plug-in is for Mobility. The only value to set is **rules**. It controls the total number of threads in the Policy Engine (QNS) that are executing at any given time. The default value is 50.

It is recommended not to configure the value below 50. It can be set higher to help increase performance in certain situations where the queue full issue or performance issue is being observed. The value also depends on call model, hardware type.

A configuration example is shown below:

Figure 24: Thread Pool Configuration



Threading Configuration

Thread Pool Configuration

*Thread Pool Name	*Threads	*Queue Size	*Scale By Cpu Core
rules	50	0	□

The following parameters can be configured under Threading Configuration:

Table 5: Threading Configuration Parameters

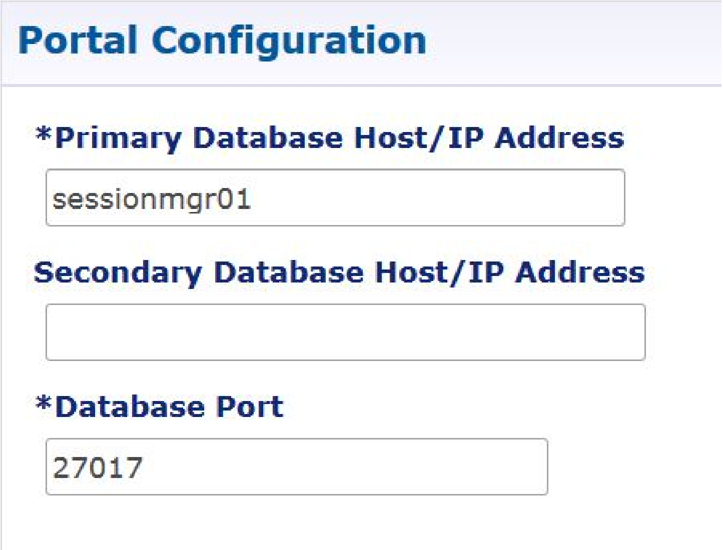
Parameter	Description
Thread Pool Name	Name of the Cisco thread pool i.e., rules.
Threads	Specify the threads to set in the thread pool. You can set rules thread ranging from 50 to 100 depending on the call flow (based on number of lookup operations). • rules = 50; Queue Size = 0; Scale By Cpu Core = unchecked • rules = 100; Queue Size = 0 (If TPS is > 2000 per Policy Server (QNS) depending on call model used; for example, if LDAP is enabled); Scale By Cpu core = unchecked The threads are driven based upon average response time of the message. The response time is call model dependent.

Parameter	Description
Queue Size	Specify the size of the queue before the threads are rejected. If value is greater than 50, performance may degrade because it holds the number of tasks in queue waiting for threads to be executed when TPS is high. If the value is lower than 50, the requests start dropping when all worker threads are busy in executing actions. The queue belongs to each Policy Server (QNS) process, and it holds incoming messages from Policy Directors (LB), but also internal events/messages (for example, an internal time change that triggers a policy evaluation). This is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware. Default value is 0. **Note** In most of the setups, keep the queue size value default.
Scale By Cpu Core	Select this check box to enable the processor cores to scale the maximum number of threads. By default, this check box is unchecked.

Portal Configuration

Click **Portal Configuration** from right pane to add the configuration in the system.

Figure 25: Portal Configuration



Portal Configuration

*Primary Database Host/IP Address: sessionmgr01

Secondary Database Host/IP Address:

*Database Port: 27017

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.

Parameter	Description
Secondary Database Host/IP Address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Database Port	This is required. This is the port the Balance database uses, that is, the port of sessionmgr.

Async Threading Configuration

Click **Async Threading Configuration** under **Systems** > ***Name of the system*** > **Plugin Configuration** in the right pane to add the configuration in the system.

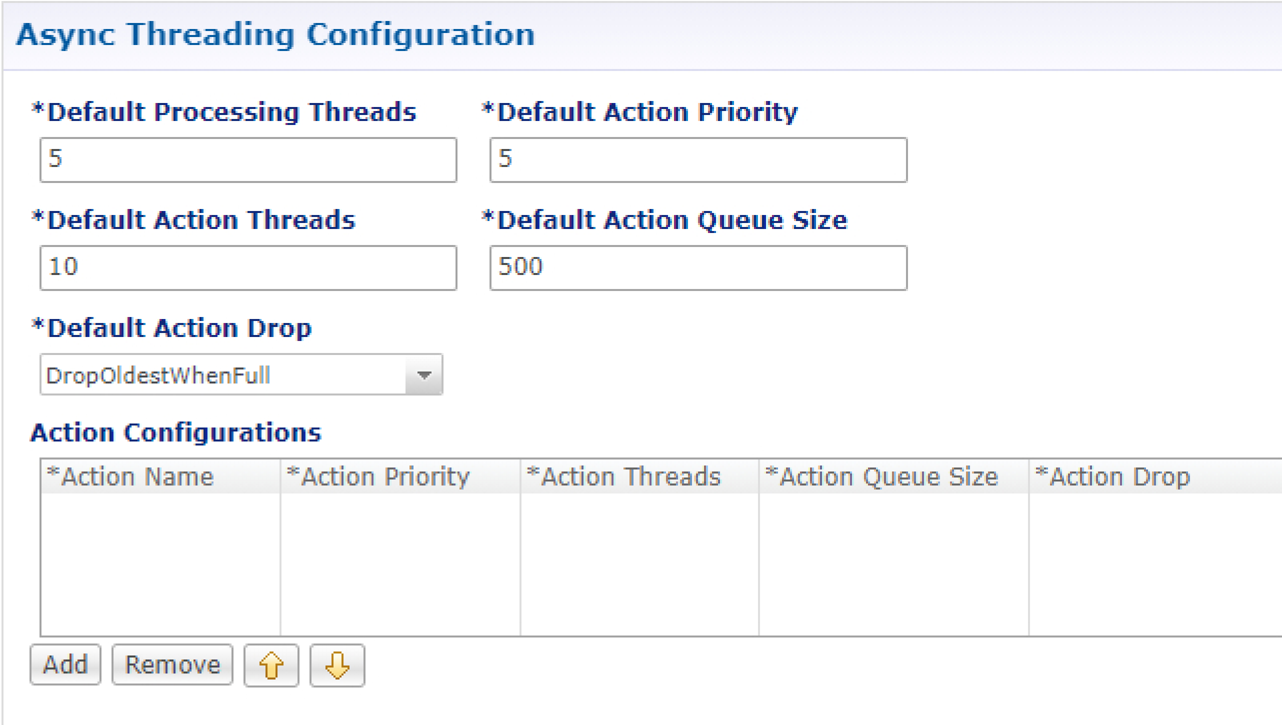
Use the default values for the Async Threading Plug-in. Similar to the Threading Plug-in, the Async configuration controls the number of asynchronous threads operating in the Policy Engine. The Policy Engine handles two basic types of messages - synchronous and asynchronous. Synchronous messages block and expect a response.

Asynchronous messages are sent into the Policy Engine but do not expect a response. Therefore, the Policy Engine can defer those to worker threads that operate along side the main Policy Engine threading execution without causing too much traffic for performance.

For example, when an NDM calls an aynsc action based on call flow and the same threads are used to perform async action across async submissions into engine from multiple NDM's.

Note Always select the link for Async Threading Configuration to configure your CPS system.

Figure 26: Async Threading Configuration



Async Threading Configuration

*Default Processing Threads: 5

*Default Action Priority: 5

*Default Action Threads: 10

*Default Action Queue Size: 500

*Default Action Drop: DropOldestWhenFull

Action Configurations

*Action Name	*Action Priority	*Action Threads	*Action Queue Size	*Action Drop

The following parameters can be configured under Async Threading Configuration.

Table 6: Async Threading Configuration Parameters

Parameter	Description
Default Processing Threads	Specifies the number of threads that are allocated to process actions based on priority. When you increase the value of this parameter, the number of asynchronous threads in the pool increases and more number of threads are able to execute asynchronous actions. Although the value depends on TPS, if increased too much, it degrades the performance. That is because these threads would occupy more resources to execute more actions simultaneously. By decreasing the value, the number of threads in pool decrease and there may be a delay in processing actions. Default value is 5.

Parameter	Description
Default Action Priority	Specifies the priority assigned to an action when it is not specified in the Action Configurations table. Default value is 5. If default action priority is set when there is no action specified in the action table, there is no impact. However, if action priority is specified in the action table and also in the default action priority, then the action with the higher priority takes precedence. **Example 1:** • Action Configuration table: 600 (task priority) • Default Action Priority: 700 In the preceding example, the default action takes priority over the action defined in the action configuration table. **Example 2:** • Action Configuration table: 600 (task priority) • Default Action Priority: 500 In the preceding example, the action defined in the action configuration table takes priority over the action defined in the default action priority.
Default Action Threads	Specifies the number of threads assigned to process the action when it is not specified in the Action Configurations table. These are action specific threads, therefore, based on the increased or decreased value, the number of threads are allocated to a specific action. It is recommended that the default action thread value be maintained. However, if there are actions that are executed more frequently, then enter a value in the action table that is higher than the one in the default action thread. Default value is 10.

Parameter	Description
Default Action Queue Size	Specifies the number of actions that can be queued up for an action when it is not specified in the Action Configurations table. Increasing this value increases the action-specific queue size. For example, if action specific threads are 10 and queue size is defined as 600, then CPS accepts 610 specific action threads. That is, 10 threads are executed while the balance 600 are in queue. **Note** It is recommended that the default action queue size should not be changed. If required, insert an action in the action table and increase the queue size of that action such that it takes precedence over the default action queue size. Decreasing this value decreases the action-specific queue size. For example, if action specific threads are 10 and queue size is defined as 400, then CPS at accept 410 specific action threads. That is, 10 threads are executed while the balance 400 are in queue. If total action specific requests are 500, the balance 90 are dropped. **Note** It is recommended that the default action queue size should not be changed. If a specific action is executed lesser number of times, insert an action in the action table and decrease the queue size of that action Default value is 500.
Default Action Drop	When **DropOldestWhenFull** action is selected, CPS drops the oldest queued action when a new action is added to the full queue. When **DropWhenFull** action is selected, CPS drops the new queued action when it is added to the already full queue. When **DoNotDrop** action is selected, none of the actions are dropped. This makes sure that all the actions are processed. Default value is **DropOldestWhenFull**.
Action Configurations Table	
Action Name	The name of the action. This must match the implementation class name. For example, com.broadhop.notifications.actions.ISendSMSNotificationRequest.
Action Priority	The priority of the action. Used by the default processing threads to determine which action to execute first. **Note** Based on the action, value should be defined. There is no default or recommended value.
Action Threads	Specifies the number of threads dedicated to processing this specific action. **Note** Based on the action, value should be defined. There is no default or recommended value.

Parameter	Description
Action Queue Size	Specifies the number of actions that can be queued up. **Note** Based on the action, value should be defined. There is no default or recommended value.
Action Drop	When **DropOldestWhenFull** action is selected, CPS drops the oldest queued action when a new action is added to the full queue. When **DropWhenFull** action is selected, CPS drops the new queued action when it is added to the already full queue. When **DoNotDrop** action is selected, none of the actions are dropped. This makes sure that all the actions are processed. Default value is **DropOldestWhenFull**.

Custom Reference Data Configuration

Configure your system, cluster, and instance for the first time to use Custom Reference Data Table plug-in. Then you can create as many tables as needed.

Important When you add new fields in CRD, manually update the new fields with appropriate values for all the existing entries in CRD. Otherwise DRA doesn't show any values for these new fields for existing entries and this can cause routing failures.

Click **Custom Reference Data Configuration** from right pane to add the configuration in the system.

- HA example:
    - Primary Database Host/IP Address: sessionmgr01
    - Secondary Database Host/IP Address: sessionmgr02
    - Database Port: 27717

The following parameters can be configured under Custom Reference Data Configuration.

Table 7: Custom Reference Data Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database. For example, sessionmgr01.
Secondary Database Host/IP Address	(Optional) This field is the IP address or a host name of a secondary, backup, or failover sessionmgr database. For example, sessionmgr02.

Parameter	Description
Database Port	Port number of the sessionmgr. **Note** Make sure that the value for this field is same as filled in for both the Primary Database Host/IP Address and Secondary Database Host/IP Address fields. Default value is 27717.
Db Read Preference	Describes how sessionmgr clients route read operations to members of a replica set. Select one of the following options from drop-down list: • Primary: All operations read from the current replica set primary member. • PrimaryPreferred: In most situations, operations read from the primary database host. However, if this host is unavailable, operations read from the secondary databse host. • Secondary: All operations read from the secondary members of the replica set. • SecondaryPreferred: In most situations, operations read from secondary members. However, if a secondary database host is unavailable, operations read from the primary database host. Default value is Primary. For more information, see http://docs.mongodb.org/manual/core/read-preference/.
Connection Per Host	Number of connections that are allowed for each database host. Default value is 100. Connection Per Host is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware.
Avp Persists	Use this table to configure certain AVPs that you want to store in the session database. AVPs that are not configured as part of this table, are not persisted. • Name: Enter the name for the AVP value. • Avp Name: The name of the CRD/policy derived AVP. To retrieve the stored AVPs from the session, use the Customer Reference Data Debug AVPs. This retriever is used to send the stored AVPs in any diameter message, and available in the **PolicyState/Session data to Custom AVP Mapping** under Custom AVP Profiles. **Restriction** When you configure the AVP Persists table in the Policy Builder, for each AVP, configure both the AVP name and name. If no values are added for these fields, then the particular AVP is not added to the Gx session. This scenario leads to unavailability of the specific AVP and hence, no custom AVP are sent.

For more information on Custom Reference Data API Usage, see the *CPS Operations Guide* for this release.

Balance Configuration

Click **Balance Configuration** in the right pane to add the configuration in the system.

The following parameters can be configured under Balance Configuration:

Table 8: Balance Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP Address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Database Port	This is required. This is the port the Balance database uses, that is, the port of sessionmgr.
Db Write Concern	Controls the write behavior of Session Manager and for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace and Endpoint databases. Select one of the following options from drop-down list: • OneInstanceSafe: This means the system waits for confirmation of writing in primary member. • TwoInstanceSafe: This means the system waits for confirmation in primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, see http://docs.mongodb.org/manual/core/read-preference/.
Failover Sla Ms	This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.

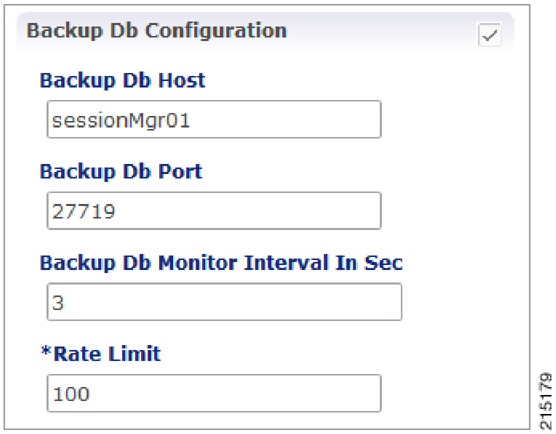
Parameter	Description
Max Replication Wait Time Ms	This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern. This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.
Default Minimum Dosage Time Based	This field is optional but recommended. This is the minimum amount of time that is granted for a reservation, assuming quota is not exhausted. If you want to manage subscriber balances on the basis of time used, check with the network device administrator and configure this value to be slightly larger than the minimum amount of time the network device such as an SCE or ISG accepts for a reservation. Minimum value is 2 seconds.
Default Minimum Dosage Volume Based	This field is optional but recommended. This is the minimum amount of volume that is granted for a reservation, assuming quota is not exhausted. If you try to make a reservation for 1 KB, and your minimum is 10 KB, the router rejects it because it is too small an amount to bother with.
Expired Reservations Purge Time (minutes)	The amount of time a record of expired reservations is retained and Cisco MsBM attempts to charge them. Expired reservations are charged only if sufficient quota is still available; that is, expired reservations do not retain the lock on quota that current reservations do. Default value is 0.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Recurring Refresh Max Delay (minutes)</td><td>
<p>The amount of time refreshing of recurring quotas are staggered across randomly, for sessions that are not actively using quota but are still established.</p>
<p>This parameter is used in cases where subscribers always have a session, but is not using their quota actively. This allows staggering of recurring refreshes where you have set all their subscribers to refresh at the same time, say midnight. It avoids spiking the CPU.</p>
<p>Default value is 0.</p>
<p>To calculate the Recurring Refresh Max Delay, use the following:</p>
<p>Recurring Refresh Max Delay = (Number of sessions / Max Timer TPS) * 2</p>
<p>For example:</p>
<p>If 30 million sessions are present on the system, and Max Timer TPS is configured to 2000, then</p>
<table>
<tr><td>Recurring Refresh Max Delay</td><td>= (30,000,000 / 2000) * 2</td></tr>
<tr><td></td><td>= 500 minutes ~ 8.33 hours</td></tr>
</table>
<p>In case you want to configure a lesser time for the Recurring Refresh Max Delay, then the Max Timer TPS needs to be increased accordingly.</p>
<p><b>Note</b> Cisco recommends using Re-evaluation diffusion buckets and Re-evaluation diffusion interval (in milliseconds) instead of Recurring Refresh Max Delay (minutes). For more information, see Adding an HA Cluster, on page 28.</p>
</td></tr>
<tr><td>Remote Database Lookup Filter Type</td><td>
<p>This drop-down list is used to do a lookup in remote databases bases on selected filter type. This is similar to Filter Type drop-down under API Router Configuration.</p>
<p>By default, NetworkId is selected.</p>
<p><b>Note</b> Filter type must be same in API Router Configuration and Balance Configuration in Policy Builder.</p>
</td></tr>
<tr><td>Reduce Dosage on Threshold</td><td>When checked, reservation dosages are reduced as a Cisco MsBM threshold is approached. This way, a dosage does not pass a threshold by a large amount before notification of the breach is sent out. When unchecked, normal dosage is granted. Recall that when enabled, messaging becomes much more chatty, but threshold breach accuracy is enhanced.</td></tr>
<tr><td>Submit Balance Events To Reporting</td><td>Submits balance transaction to the policy engine, and these can be reflected in reporting.</td></tr>
</table>

Parameter	Description
Enable Crd Balance Template Lookups	When checked, CPS is enabled to lookup CRD defined balance templates. If the CRD tables are not defined, this feature is disabled. **Note** Even if the CRD tables are not defined as required, and this feature is disabled, the **Dynamic Reference Data Key** field is still enabled but only for Policy Builder defined Account Balance Templates. For more information, see Table 101: Pull Value From....
Remote Database	
Name	String - Name of the remote database.
Key Prefix	Key prefix to be match for the remote database to be selected for lookup.
Connections Per Host	Number of connections that can be created per host. Default value is 5.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, see http://docs.mongodb.org/manual/core/read-preference/.
Primary Database Host/IP address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Port	Port number of the remote sessionmgr database. It must be the same for both the primary and secondary databases.
Backup Db Host On Local Site	String - The host name of backup database for remote balance for current site. Default value is sessionmgr01.
Backup Db Port on Local Site	The port number of backup database for remote balance for current site. Default value is 27719.

If you have a Geo-Redundancy setup, click **Backup Db Configuration**. It stores back up of entire balance records. If the primary balance database goes down, CPS will check the balance record on both secondary and backup databases, and take the latest version for processing.

Figure 27: Backup Db Configuration



Backup Db Configuration ☑

Backup Db Host: sessionMgr01

Backup Db Port: 27719

Backup Db Monitor Interval In Sec: 3

*Rate Limit: 100

The following parameters can be configured under **Backup Db Configuration**:

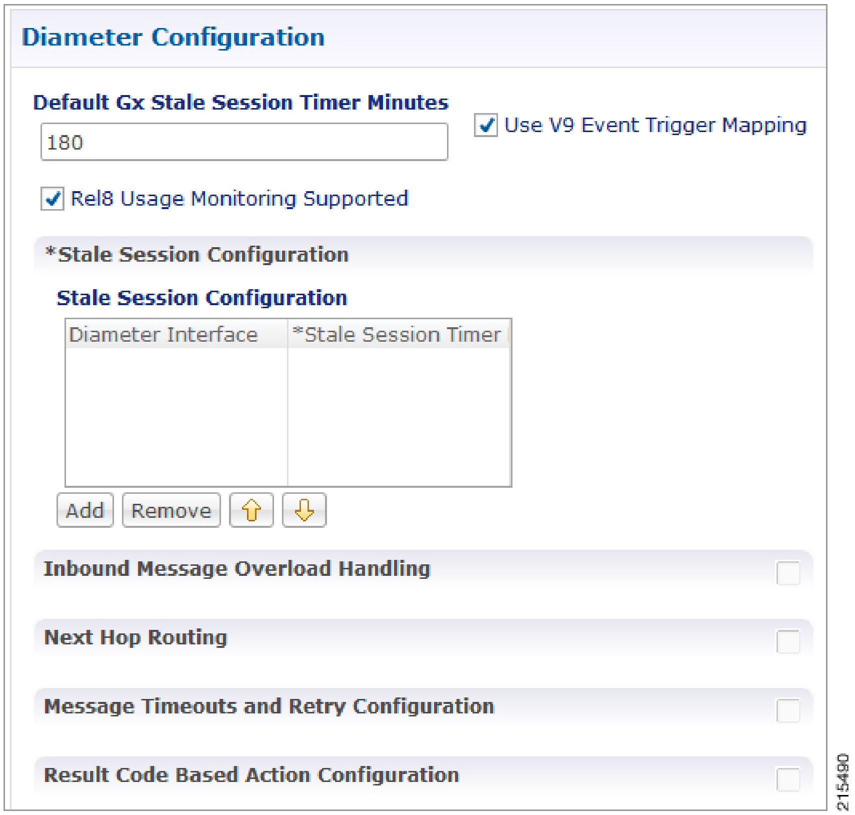
Table 9: Backup Db Configuration Parameters

Parameter	Description
Backup Db Host	Default value is sessionmgr01.
Backup Db Port	Default value is 27719.
Backup Db Monitor Interval In Sec	Used in thread which updates the primary balance DB (when primary balanceDB is available after fail over) with 'BackupBalance' db records. Default value is 3 seconds.
Rate Limit	Used to control the TPS (with how much TPS reconciliation should happen once primary balance db is up).

Diameter Configuration

Click **Diameter Configuration** in the right pane to add the configuration in the system.

Figure 28: Diameter Configuration



Diameter Configuration

Default Gx Stale Session Timer Minutes: 180

☑ Use V9 Event Trigger Mapping

☑ Rel8 Usage Monitoring Supported

*Stale Session Configuration

Stale Session Configuration

Diameter Interface	*Stale Session Timer

□ Inbound Message Overload Handling

□ Next Hop Routing

□ Message Timeouts and Retry Configuration

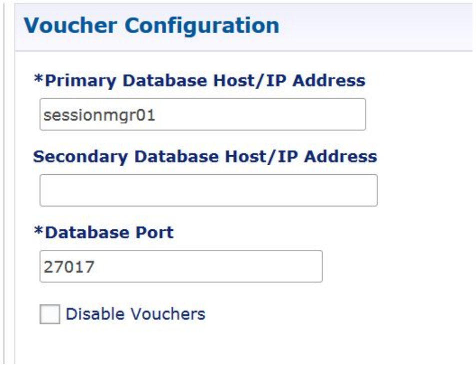
□ Result Code Based Action Configuration

For more information on the parameters under this plug-in, see Diameter Configuration, on page 75.

Voucher Configuration

Click **Voucher Configuration** in the right pane to add the configuration in the system.

Figure 29: Voucher Configuration



Voucher Configuration

*Primary Database Host/IP Address: sessionmgr01

Secondary Database Host/IP Address:

*Database Port: 27017

□ Disable Vouchers

The voucher plug-in uses the following defaults:

- HA example:

- Primary: sessionmgr01
- Secondary: sessionmgr02
- Port: 27718

The following parameters can be configured under Voucher Configuration:

Table 10: Voucher Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	The IP address or a host name of the Session Manager database that holds voucher information for Cisco Policy Builder and Cisco Policy Server.
Secondary Database Host/IP Address	The IP address or a host name of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary Database IP Address field.
Database Port	Port number of the sessionmgr. It must be the same for both the primary and secondary databases.
Disable Vouchers	Select the check box to disable voucher configuration.

Unified API Configuration

Click **Unified API Configuration** in right pane to add the configuration in the system.

The following parameters can be configured under Unified API Configuration:

Table 11: Unified API Configuration Parameters

Parameter	Description
Fields To Wrap With Cdata Tags	This is a CSV separated string. The Unified API can handle CDATA fields. Use the Plug-in configuration in Policy Builder to set CDATA fields for the main Unified API. The property `ua.cdata.fields` is used to set the fields that must be wrapped in CDATA tags for the client CommFactory to properly send and receive API requests. `-Dua.cdata.fields=networkId,password,data,oldNetworkId,oldPassword,newPassword` is the default.
Session Route Key	Session route key that vDRA uses to look up the peer group and route the Rx AAR message to the correct PCRF. When vDRA makes REST API requests to multiple PCRFs for session query using the Framed-IPv6-Prefix received in the Rx AAR message, one of the PCRF that has the corresponding Gx session sends this session route key in the response. vDRA then uses this key to look up the peer group and route the Rx AAR message to the correct PCRF.

Parameter	Description
Max API TPS Threshold	This value defines maximum API TPS supported per Policy Server (qns) process. Default value is 0. For API rate limiting at HAProxy, refer to Note [1].
HTTP Error Code on Threshold Reached	HTTP response code to send when API request is throttled (rate limiter acquire fails). Default value is 500 (Internal Server Error).
Submit Requests To Audit Log	Select the check box to log requests to API in audit log. Default value is True (checked).
Submit Read Requests To Audit Log	Select this check box to log read requests in audit log. Default value is False (unchecked).

[1] HAProxy has `maxconn <conns>` configuration which manages the total number of connections that haproxy, as a service, queues or processes at a single point of time.

Notification Configuration

Notification in Cisco Policy Builder relates to pushing messages from Cisco Policy Builder to subscribers. The messages are used to alert the subscriber of issues as well as opportunities on their network. Not only can you alert subscribers, but you can also send messages to any address, for example, system monitoring addresses.

Currently, Cisco Policy Builder offers following notification types for Mobile:

- Apple iOS devices/iPhone® push (iOS devices)
- Email (IMAP only)
- SMS notification (SMPP v 3.4)
- Realtime Notification

The following parameters can be configured under **Notification Configuration**. For more information about these parameters, see the Notification Services chapter.

Table 12: Notification Configuration Parameters

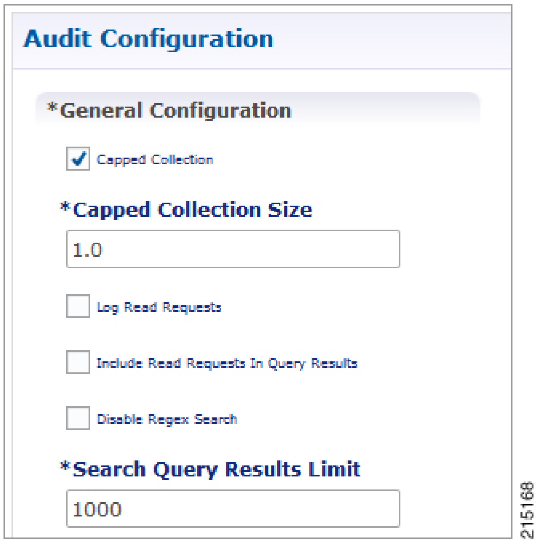
Parameter	Description
Apple Push Notification Configuration	Select this check box to configure the connection for a push to an Apple iOS device or iPhone.
Email Notification Configuration	Select this check box to configure the connection for an email notification.
SMS Notification Configuration	Select this check box to configure the connection for a SMS notification.

Parameter	Description
Realtime Notification Configuration	Select this check box to configure the connection for a realtime notification.

Audit Configuration

Click **Audit Configuration** in the right pane to add the configuration in the system.

Figure 30: Audit Configuration



Audit Configuration

*General Configuration

☑ Capped Collection

*Capped Collection Size

1.0

□ Log Read Requests

□ Include Read Requests In Query Results

□ Disable Regex Search

*Search Query Results Limit

1000

The following parameters can be configured in the **General Configuration** pane under Audit Configuration:

Table 13: Audit Configuration Parameters

Parameter	Description
Capped Collection check box	Select this check box to activate capped collection function.
Capped Collection Size	By default, the Audit History uses a 1 GB capped collection in MongoDB. The capped collection automatically removes documents when the size restriction threshold is hit. Configuration in Policy Builder is done in GB increments. It is possible to enter decimals, for example, 9.5 will set the capped collection to 9.5 GB.
Log Read Requests check box	Select this check box if you want read requests to be logged.
Include Read Requests In Query Results check box	Select this check box only if you want to include read requests to be displayed in query results.
Disable Regex Search check box	If you select this check box, the use of regular expressions for queries is turned off in the Policy Builder configuration.

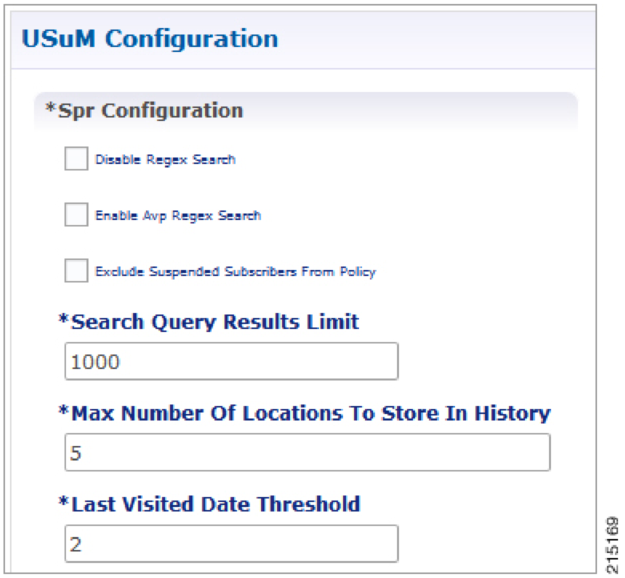
Parameter	Description
Search Query Results Limit	This parameter limits the search results.

For more information related to other parameters like Queue Submission Configuration, Database Configuration, Shard Configuration under Audit Configuration, refer to the *CPS Operations Guide* for this release.

USuM Configuration

Click **USuM Configuration** from right pane to add the configuration in the system.

Figure 31: USuM Configuration



USuM Configuration

*Spr Configuration

□ Disable Regex Search

□ Enable Avp Regex Search

□ Exclude Suspended Subscribers From Policy

*Search Query Results Limit: 1000

*Max Number Of Locations To Store In History: 5

*Last Visited Date Threshold: 2

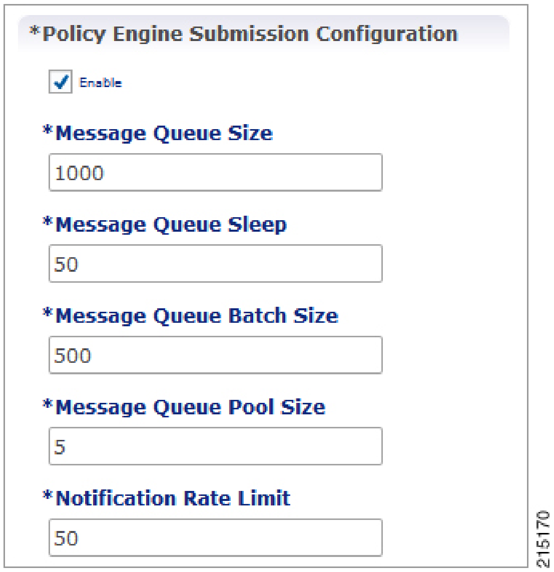
The following parameters can be configured in the **Spr Configuration** pane under USuM Configuration:

Table 14: USuM Configuration Parameters - 1

Parameter	Description
Spr Configuration	
Disable Regex Search	For SP Wi-Fi, you can use email ID which has realm, username, and so on, as key of SPR. So, part of the string needs to match for regex support. **Note** RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.
Enable Avp Regex Search	For regex search on values for AVP for SPR.
Exclude Suspended Subscribers From Policy	If the subscriber state is Suspended, SPR does not validate IMSI.

Parameter	Description
Search Query Results Limit	Used to limit search if you are not passing any IMSI/MSISDN (NetworkID) in control center to list subscriber. Default value is 1000.
Max Number Of Locations To Store In History	It is used to track subscriber last location to maintain history. Maximum "n" last locations are stored as location history.
Last Visited Date Threshold	This parameter is used to identify if the subscriber is visiting same location again (based on the location history). If the subscriber is vising the same location, then it will change the last visited date if current visited date is more than last visited date + "n" days defined here.

Figure 32: Policy Engine Submission Configuration



*Policy Engine Submission Configuration

☑ Enable

*Message Queue Size

1000

*Message Queue Sleep

50

*Message Queue Batch Size

500

*Message Queue Pool Size

5

*Notification Rate Limit

50

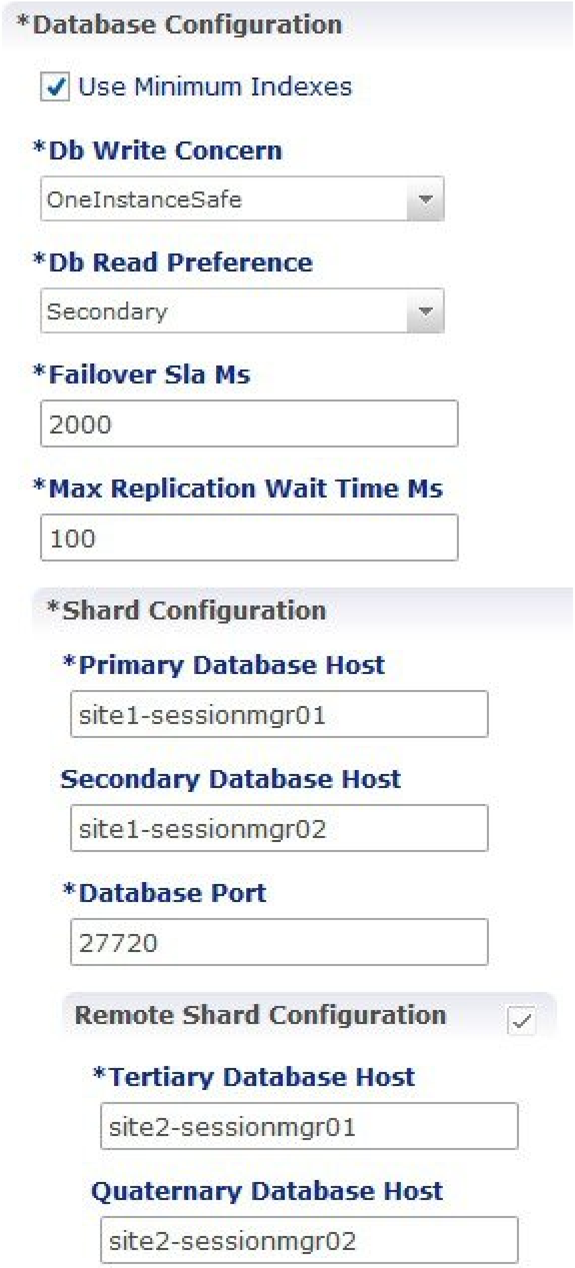
The following parameters can be configured in the **Policy Engine Submission Configuration** pane under USuM Configuration:

Table 15: USuM Configuration Parameters - 2

Parameter	Description
Enable check box	Keep it default.
Message Queue Size	Queue to hold data to generate internal SPR Refresh events for policy engine during Create, Update, Delete of subscriber.
Message Queue Sleep	Sleep before popping next batch for generating SPR Refresh events for policy engine for RAR processing.
Message Queue Batch Size	Batch size for fetching number of subscriberIds in one go for generating SPR Refresh events for policy engine for RAR processing.

Parameter	Description
Message Queue Pool Size	Message queue pool size to consume the data from queue and generate SPR Refresh events.
Notification Rate Limit	Rate limiting for generating SPR Refresh events. SPR Refresh events is used to generate RAR for active session where subscriber data has been change.

Figure 33: Database Configuration



*Database Configuration

☑ Use Minimum Indexes

*Db Write Concern: OneInstanceSafe

*Db Read Preference: Secondary

*Failover Sla Ms: 2000

*Max Replication Wait Time Ms: 100

*Shard Configuration

*Primary Database Host: site1-sessionmgr01

Secondary Database Host: site1-sessionmgr02

*Database Port: 27720

Remote Shard Configuration ☑

*Tertiary Database Host: site2-sessionmgr01

Quaternary Database Host: site2-sessionmgr02

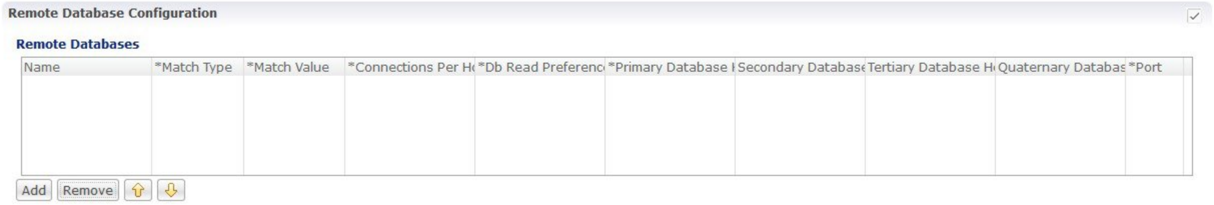
The following parameters can be configured in **Database Configuration** pane under USuM Configuration:

Table 16: USuM Configuration Parameters - 3

Parameter	Description
Database Configuration	
Use Minimum Indexes	It is used to decide what all indexes need to be created on SPR collection by default. You need all the indexes to be created (You can select this check box when number of subscribers are low, for example, less than 50K). Default value is unchecked.
Db Write Concern	Controls the write behavior of Session Manager and for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace and Endpoint databases. Select one of the following options from drop-down list: • OneInstanceSafe: This means the system waits for confirmation of writing in primary member. • TwoInstanceSafe: This means the system waits for confirmation in primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, refer to http://docs.mongodb.org/manual/core/read-preference/. **Important** For consistent profile updates across multiple sessions for same subscriber, Cisco recommends to set the **Db Read Preference** as *PrimaryPreferred*.
Failover Sla Ms	This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.

Parameter	Description
Max Replication Wait Time Ms	This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern. This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.
Shard Configuration **Important** The host names must exactly be the same host name used when the corresponding replica-set is created in Mongo. Only the data holding members need to be configured (and not the arbiters).	
Primary Database Host	String - Primary Host Address.
Secondary Database Host	String - Secondary Host Address.
Database Port	Default value is 27720.
Remote Shard Configuration **Important** Remote shard configuration is used only for GR deployments. The host names must exactly be the same host name used when the corresponding replica-set is created in Mongo. Only the data holding members need to be configured (and not the arbiters).	
Tertiary Database Host	String - Tertiary Host Address.
Quaternary Database Host	String - Quaternary Host Address.

Figure 34: Remote Database Configuration



Remote Database Configuration

Remote Databases

Name	*Match Type	*Match Value	*Connections Per H	*Db Read Preferenc	*Primary Database I	Secondary Databas	Tertiary Database H	Quaternary Databas	*Port

Click **Add** to add a new row in the **Remote Database Configuration** pane. The following parameters can be configured in the **Remote Database Configuration** pane under **USuM Configuration**:

Note To enable CPS to route the Sh data based on Gx CCR-I origin-host pattern, you need to enable **Remote Database Configuration**. For more information, see External Profile Cache, on page 201.

Important Remote database configuration is used only for GR deployments. The host names must exactly be the same host name used when the corresponding replica-set is created in Mongo. Only the data holding members need to be configured (and not the arbiters).

Table 17: USuM Configuration Parameters - 4

Parameter	Description
Name	String - Name of the remote database.
Match Type	Select any one of the following values from the drop down: • StartsWith • Regex • EndsWith • Equals
Match Value	A string value which matches the MatchType specified. In case of Regex, you need to specify valid java regex pattern. This is used to lookup the remoteDB specified for a subscriber match for read/write operations on the SPR database.
Connections Per Host	This parameter is not used in USuM Configuration.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.
Primary Database Host	Host name of the remote sessionmgr database.
Secondary Database Host	(Optional) Host name of a secondary, backup, or failover sessionmgr database.
Tertiary Database Host	Host name of the tertiary database.
Quaternary Database Host	Host name of the quaternary database.
Port	Port number of the remote sessionmgr database. It must be the same for both the primary and secondary databases. Default value is 27720.

Scheduled Events

The Scheduled Events plug-in is configured in the Policy Builder to implement offline notifications and SPR cleanup. Offline notifications send an SMS notification to an off-line subscriber indicating that their quota is about to expire. SPR cleanup allows you to delete subscriber data that is no longer needed or valid. For example, a subscriber account no longer has any services assigned to it, and therefore should be deleted from the database.

Enable Scheduled Events

To enable the scheduled events framework, this feature has to be enabled in the feature set of Policy Server and Policy Builder. The following packages, when added to the respective servers, deploy the functionality of scheduledEvents during a session:

- In the Policy Builder – com.broadhop.client.feature.scheduledevents package is added.
- In the Policy Server – com.broadhop.scheduledevents.service.feature package is added.

To add **Scheduled Events Configuration**, perform the following steps:

Step 1 If this is HA environment, edit the corresponding features files in Cluster Manager VM:

In the `/var/qps/current_config/etc/broadhop/pb/features` file, add the following line:

```
com.broadhop.client.feature.scheduledevents
```

In the `/var/qps/current_config/etc/broadhop/pcrf/features` file, add the following line:

```
com.broadhop.scheduledevents.service.feature
```

Step 2 After modifying the feature files, execute the following commands:

```
/var/qps/install/current/scripts/build_all.sh
```

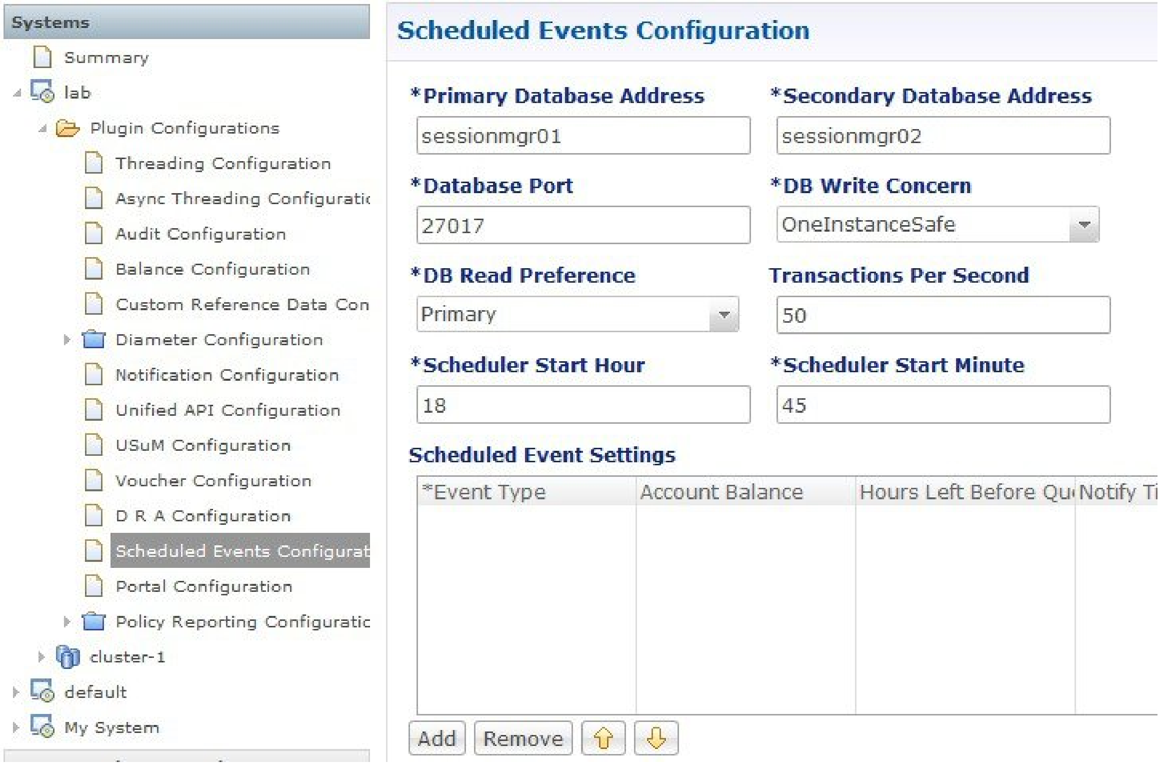
```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Scheduled Events Configuration

Step 1 Click **Scheduled Events Configuration** in the right pane.

Step 2 In the **Scheduled Event Configuration** pane and enter the values for the fields provided.

Figure 35: Scheduled Events Configuration



Scheduled Events Configuration

*Primary Database Address: sessionmgr01

*Secondary Database Address: sessionmgr02

*Database Port: 27017

*DB Write Concern: OneInstanceSafe

*DB Read Preference: Primary

Transactions Per Second: 50

*Scheduler Start Hour: 18

*Scheduler Start Minute: 45

Scheduled Event Settings

*Event Type	Account Balance	Hours Left Before Qu	Notify Ti

The following table describes the parameters that can be configured under **Scheduled Events Configuration**.

Table 18: Scheduled Events Configuration Parameters

Parameter	Description
Primary Database Address	The IP address of the sessionmgr database.
Secondary Database Address	The IP address of a secondary, backup, or failover sessionmgr database.
Database Port	The port used by the database; this is the sessionmgr port.
DB Write Concern	Controls the write behavior of Session Manager and for what errors exceptions are raised. Db Write Concern defined in Cluster page applies only to Admin, Trace and Endpoint databases. Select one of the following options from drop-down list: • OneInstanceSafe: This means the system waits for confirmation of writing in primary member. • TwoInstanceSafe: This means the system waits for confirmation in primary and one secondary member. Default value is OneInstanceSafe. For more information, see MongoDB documentation.

Parameter	Description
DB Read Preference	Describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: • Primary – Default mode. All operations read from the current replica set primary. • PrimaryPreferred – In most situations, operations read from the primary but if it is unavailable, operations read from secondary members. • Secondary – All operations read from the secondary members of the replica set. • SecondaryPreferred – In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary. For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.
Transactions Per Second	Controls the maximum number of internally generated transactions per second that the system will produce.
Scheduled Start Hour	The hour at which the event is triggered. The value specified should be in the range of 0 to 23 (24-hour format).
Scheduled Start Minute	The minute at which the event is triggered. The value specified should be in the range 0 to 59.
Event Type	The type of event that will be triggered. You can select either of the following: **QuotaExpiration** – The scheduled event will be triggered when the system detects that a subscriber's quota is going to expire within the number of hours specified in the **Hours Left Before Quota Exhausts** parameter. **SubscriberInactivity** – The scheduled event will be triggered when the system detects that a subscriber is inactive. If you select this event type, the **Hours Left Before Quota Exhausts** and **Notify Time in Hours** parameters are ignored.
Account Balance	Processes only those subscribers whose account balance is specified in the configuration. Other subscribers are ignored. The **Account Balance** and **Service** parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.

Parameter	Description
Hours Left Before Quota Exhausts	Used only with the QuotaExpiration event type. This parameter specifies the number of hours before the subscriber's quota expires. The system checks this field in the scheduled events loop and looks for quotas that are about to expire within the number of hours specified. If the number of hours before expiration is less than the value in this column, then subscribers with that quota will be added to the eventsCollection in the ScheduleEvents mongo database. For example, if this value is 8, when the scheduled events task runs, any subscribes who have the service specified and whose quota will expire in less than 8 hours will be added to the eventsCollection. Once in eventsCollection, new actions are taken for that subscriber depending on scheduled event configuration.
Notify Time in Hours	Used only with the QuotaExpiration event type. This parameter specifies the number of hours before a notification is sent to the subscriber. This parameter is used in conjunction with the **Hours Left Before Quota Exhausts** parameter. When this number is reached, CPS submits a QuotaExpiredEvent to the policy engine with the subscriber's balance information. When this occurs, the state of the entry in the eventsCollection changes to "notified." For example, if **Hours Left Before Quota Exhausts** = 8 and **Notify Time in Hours** = 4, an entry is created with the subscriber's balance information in the eventCollections 8 hours prior to quota expiration, and a QuotaExpiration event is submitted to the policy engine 4 hours before expiration. You can set up polices to send out notifications when this event occurs; for example, you might set up scheduled events to send out notifications 8 hours, 6 hours, 4, hours, and 2 hours before a subscriber's quota expires, reminding the subscriber to "top up."
Service	Processes only those subscribers who have the configured service associated. Other subscribers are ignored. The **Account Balance** and **Service** parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.
Max Number of Days	Used only with the SubscriberInactivity event type. This parameter specifies the duration in days to retain the subscriber in the inactive state. If the status of a subscriber remains inactive for longer than the configured maximum number of days, the subscriber is automatically deleted from the database.

Parameter	Description
Command	A string value that is used to provide additional information about the event that is being submitted. This string can be used in the polices that look for events submitted to the policy engine. For example, when used with a QuotaExpiration event type, the command could be set to "8 hours" or "6 hours," or to any other string. A policy can use this string in its condition parameters to send one notification as opposed to another, or to take one action as opposed to another.

LDAP/Ud Configuration

CPS has capability to access subscriber profile data either from internal or external database. LDAP/Ud feature fetches subscriber profile data from the external database.

In this section, LDAP plug-in configuration is used an example.

LDAP plugin queries the LDAP server to fetch attributes depending on the configuration. This feature has capability to refresh the profile and fetch the latest updated attribute from the LDAP server. CPS connects to multiple LDAP severs and queries them depending on the LDAP server priority.

Note Refer to *CPS Installation Guide for VMware* to configure this plugin.

Click **LDAP Configuration** from the right pane to add the configuration in the system.

Click **Ldap Server Configuration**.

Figure 36: LDAP Configuration

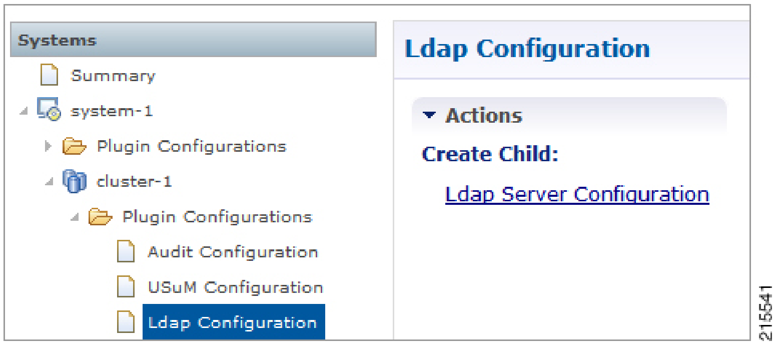
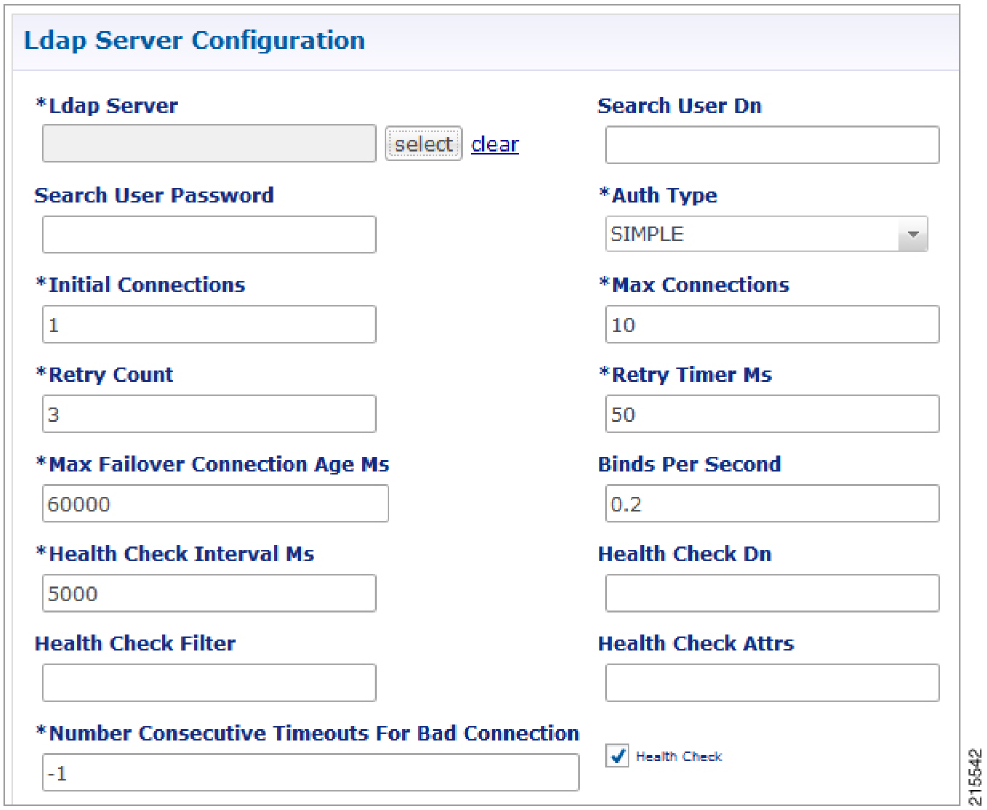


Figure 37: LDAP Server Configuration



Ldap Server Configuration

*Ldap Server:

Search User Dn:

Search User Password:

*Auth Type: SIMPLE

*Initial Connections: 1

*Max Connections: 10

*Retry Count: 3

*Retry Timer Ms: 50

*Max Failover Connection Age Ms: 60000

Binds Per Second: 0.2

*Health Check Interval Ms: 5000

Health Check Dn:

Health Check Filter:

Health Check Attrs:

*Number Consecutive Timeouts For Bad Connection: -1

☑ Health Check

The following parameters can be configured under **LDAP Server Configuration**:

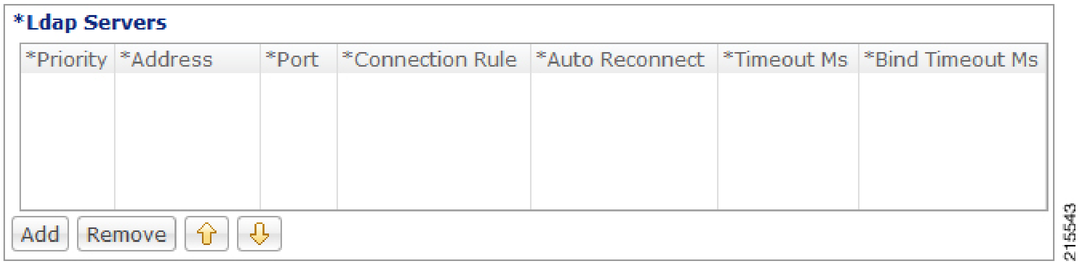
Table 19: LDAP Server Configuration Parameters – 1

Parameter	**Description**
Ldap Server	Assign this to the LDAP Server Set.
Search User Dn	The user DN for connecting to the LDAP server; for example, `cn=managerou=accountso=profile`.
Search User Password	The password for connecting to the LDAP server. **Note** The same password must apply to all servers defined in this configuration.
Auth Type	The LDAP authorization type required by the LDAP server. Default: SIMPLE
Initial Connections	Set the initial connections to “50.” This represents the number of connections from a Policy Director (load balancer) to the LDAP server(s).
Retry Count	The total number of tries the system executes for a given LDAP query. For example, a value of 2 indicates one try and then one more attempt when the query times out.

Parameter	Description
Retry Time Ms	The time period when the policy engine retries to a second Policy Director (load balancer) to send the request. **Note** Setting this value too low results in a large number of additional requests. This value should be set to a value close to the SLA provided by the LDAP server in servicing requests.
Max Failover Connection Age Ms	The time in milliseconds a secondary connection is used before checking to determine if the original primary server is available. This is the time to fall back from a failover connection. CPS returns the connection to the LDAP connection pool and gets another connection. Default: 60000 milliseconds (1 minute)
Binds Per Second	The maximum rate at which to connect to the LDAP server. Setting this to a high value may result in extra load on the peer LDAP server.
Health Check Interval Ms	The time in milliseconds to generate a health check message; for example, 5000 milliseconds (5 seconds).
Health Check Dn	The health check DN that is sent on the health check LDAP query.
Health Check Filter	The filter that is sent on the health check LDAP query.
Health Check Attrs	A comma-delimited list of attributes to retrieve in the LDAP health check query.
Health Check	Select this check box to enable the health check.
Number Consecutive Timeouts For Bad Connection	The number of timeouts that trigger a bad connection and force a reconnection. A value of -1 disables this function, preventing CPS from marking any connection bad. Default: -1

Add entries to the LDAP Servers to represent the primary and secondary connections from the CPS system to the LDAP servers.

Figure 38: LDAP Servers



*Ldap Servers

*Priority	*Address	*Port	*Connection Rule	*Auto Reconnect	*Timeout Ms	*Bind Timeout Ms

You can configure the following parameters under **LDAP Servers**:

Table 20: LDAP Server Configuration Parameters – 2

Parameter	Description
Priority	The priority of the server when sending requests. Higher number is equal to higher priority.
Address	The IP address of the server to send requests.
Port	The port address of the LDAP Server.
Connection Rule	This setting is not currently used.
Auto Reconnect	This setting is not currently used.
Timeout Ms	The SLA for queries for the LDAP server. Cisco recommends a value of 5000 milliseconds.
Bind Timeout Ms	The SLA for binds to the LDAP server.

Subscriber Lookup Server Configuration

Note Refer to the section *Subscriber Lookup Feature Installation* in *CPS Installation Guide for VMware* to configure this plugin.

You can configure CPS to act as an LDAP server to support LDAP search queries that use framedIp/msisdn/imsi/framedIpv6Prefix key to get subscriber details.

In case multiple sessions are found for matching the same LDAP query, CPS responds with details of all the sessions to LDAP client.

The search query can come to any clusters in the deployment. For configuring cluster peer, refer to Cluster Peer Configuration, on page 72. The cluster that receives the request forwards the request to all other clusters based on Cluster Peer Configuration.

In Policy Builder, click **Subscriber Lookup Server Configuration** from the right pane to add the configuration in the system.

The following parameters can be configured under **Subscriber Lookup Server Configuration**:

Table 21: Subscriber Lookup Server Configuration Parameters

Parameter	Description
Bind DN/Bind DN (Admin) Password	Used to authenticate the LDAP search request before getting processed. Default: admin/password
Ldap Server Port	Used to configure the port where you want to start the LDAP server. Default: 1399

Parameter	Description
Request Timeout (ms.)	Used to configure the time LDAP server waits to get response. Default: 5 millisec
Health check Filter Name	Used to add the attribute name to identify a health-check request.
Health check Filter Value	Used to add the filter value to identify a health-check request.
Session update Time in ms.	If checked, returns the session update time in milliseconds in the query response. If unchecked, session update time is returned in seconds. Default: unchecked
Input Mapping	Used to map Filter Id received from LDAP client to one of the internal CPS lookup keys. Is Unique Key: Indicates the key is unique for the sessions and only one session would exist for the key. If selected for non unique key, only single active session is returned for the query. Default: unchecked
Output Mapping	Used to define the response attributes for the client. Response attribute name can be mapped to internal CPS session attributes for added flexibility.
Ldap Clients	Used to configure CPS to support multiple client authentication parameters.
Health Check Attributes	Used to define the response attributes and values to be returned to LDAP client for Health-check requests.

Cluster Peer Configuration

Configuration in qns.conf

Note "-" is not allowed in the cluster name (both local and peer).

- Local cluster must be specified with `local.cluster.peer` parameter in `/etc/broadhop/qns.conf` file. This parameter is used to find out the local cluster name and is used to create local cluster queue.

  Example: `-Dlocal.cluster.peer=Cluster1`

- All cluster peers must be specified with `broadcast.cluster.peers` parameter in `/etc/broadhop/qns.conf` file. This parameter is used to find out all other clusters and to create redisQ between local cluster and other clusters. Each cluster name must be separated with semicolon. Add all the clusters including local cluster name.

  Example: `-Dbroadcast.cluster.peers=Cluster1;Cluster2;Cluster3`

Configuration for RedisQ Servers

- Redis server peers must be configured in /etc/broadhop/broadcast-cluster.conf file:

  This file has information about the redisQ servers. You need to provide Policy Directory (lb) VIP address if this is a HA setup. Each cluster specified in broadcast.cluster.peers must have one entry in this file to represent redis server related to that cluster.

  Syntax: <*ClusterName*>-clusterBroadcastQ.redis.qserver=<*lbvipIPadress*>

  where, <*lbvipIPadress*> is the IP address of Policy Director (LB) VIP.

  ClusterName is the local cluster peer (configured for local.cluster.peer parameter in qns.conf file) of every cluster.

  Example:

  ```
  [root@lb02 broadhop]# cat /etc/broadhop/broadcast-cluster.conf
  Cluster1-clusterBroadcastQ.redis.qserver=IPaddress1
  Cluster2-clusterBroadcastQ.redis.qserver=IPaddress2
  Cluster3-clusterBroadcastQ.redis.qserver=IPaddress3
  ```

Note

- During replica-set failover, some of the LDAP search requests coming from LDAP clients to a CPS site fail to respond back with session details. This is because CPS reads the session details from the nearest secondary replica-set member, and with two replica-set members present on a site when the Primary member goes down the only remaining secondary member transitions to Primary state. During this transition, there is no Secondary member available in the nearest location (or local site) and therefore Mongo is not able to read the session information. As a result, the CPS application responds back to the LDAP request without any session information. However, since the failover transition period is less than 30 seconds, so a retry from the LDAP client after this period results in an LDAP response with session information.
- If local session affinity is enabled in CPS, then during migration of sessions to replica-set of a remote CPS site, some of the LDAP search requests coming from LDAP clients to the local CPS site fail to respond back with session details. This is because CPS reads the session details from the nearest secondary replica-set member, and with migration in progress the nearest secondary members of the remote site replica-set present on the local CPS site is not in sync with the corresponding Primary member present on the remote site. This can happen due to latency between the two CPS sites. As a result, the CPS application responds back to the LDAP request without any session information. However, depending upon the delay in sync between the two site replica-set members, a retry of the LDAP client request results in an LDAP response with session information.

CHAPTER 4

Diameter Configuration

Diameter Configuration

The Diameter Configuration section allows for the configuration of the diameter plug-in. We recommend configuring the diameter plug-in at system level.

At System Level

In order to define a Diameter Configuration at system level, you need to perform the following steps:

1. Login into Policy Builder.
2. Select **Reference Data** tab.
3. From the left pane, select **Systems**.
4. Select and expand your *system name*.
5. Select **Plugin Configurations**.
6. Select **Diameter Configuration**.

At Cluster Level

In order to define a Diameter Configuration at cluster level you need to perform the following steps:

1. Log in into Policy Builder.
2. Select **Reference Data** tab.
3. From the left pane, select **Systems**.
4. Select and expand your *system name*.
5. Select and expand your *cluster name*. If no cluster has been created, create one by selecting the **Cluster** action.
6. Select **Plugin Configurations**.
7. Select **Diameter Configuration**.

The following parameters can be configured under Diameter Configuration.

Table 22: Diameter Configuration Parameters

Parameter	Description
Default Gx Stale Session Timer Minutes	This timer is armed every time a message is received or sent for any given Gx session. When the timer expires (or more precisely within the next minute after the timer expires) a Gx RAR having the Re-Auth-Request-Type AVP set to AUTHORIZE_ONLY (0) message is triggered for that Gx session. If a Gx RAA is received having Result-Code AVP value set to DIAMETER_UNKNOWN_SESSION_ID (5002) or DIAMETER_UNABLE_TO_COMPLY (5012) the Gx session is deemed as stale and removed from the PCRF internal database. On any activity over Gx interface (RAR/CCR) the timer is reset. Default value is 180 minutes. **Note** • This timer unit is minute. • Stale Gx session removal triggers the PCRF session termination procedure for any other diameter sessions that were bound to the Gx session.
Use V9 Event Trigger Mapping	This option allows for a different set of list of valid values and their interpretation to be used for the Event-Trigger enumerated AVP in order to accommodate the change that occurred in the Gx specification between 3GPP TS 29.212 v9.5 (and prior) and 3GPP TS 29.212 v9.7 (and following including v10 v11 and v12). Default value is checked. List of valid values is provided in Table 23: Use V9 Event Trigger Mapping Valid Values, on page 77. **Note** • The Event-Trigger AVP list of valid values and their interpretation defined in 3GPP TS 29.212 v9.6 is not supported. • Use V9 Event Trigger Mapping checked uses 3GPP TS 29.212 v9.5 as a reference while 3GPP TS 29.212 v110.10 is used as a reference when not checked.
Rel8 Usage Monitoring Supported	This option allows for the Gx usage monitoring feature to be supported even when the PCEF advertises support for Rel8 feature under Supported-Features AVP in Gx CCR-i. Default value is checked.
Rel15 Ext Bw Nr Supported	When checked, it enables the support for 3GPP Rel-15 Extended BW-NR feature. PCRF sends response to AF/PCEF with Rel-15 Extended BW-NR feature bit set when the feature is enabled and AF/PCEF has also set the bit in the request message. PCRF sends extended QoS AVPs only if the configuration is enabled. When unchecked, it disabled the support for 3GPP Rel-15 Extended BW-NR feature. Default value is unchecked (disabled).

Parameter	Description
Stale Session Configuration	When a new row is added in "Stale Session Configuration" table the default value for the GX_TGPP SD_V11 and SY_V11 Stale session timer is 180 minutes. **Note** The maximum value allowed for the **Stale Session Timer** parameter is 35000 minutes. If GX_TGPP Stale Session Timer value is not configured in this table, then the value is selected from the retained/old variable "Default Gx Stale Session Timer Minutes". If there are multiple values configured against any interface then the lowest among all would be considered as the stale session timer.
DRMP Prioritization	When enabled allows you to configure different message processing priorities based on the DRMP value received in the incoming request. • Default Inbound Priority - The default inbound priority value. • Inbound DRMP Prioritization • DRMP - DRMP AVP value in the incoming request. • Priority - Priority value assigned to the incoming message. Based on this value the message processing is prioritized. Higher Priority messages are be processed first compared to lower priority messages.

Note If Gx stale session timer is set for both "Default Gx Stale Session timer Minutes" and "Stale Session Configuration" then the value configured Under "Stale Session Configuration" would take the precedence.

Table 23: Use V9 Event Trigger Mapping Valid Values

Interpretation - Use V9 Event Trigger Mapping is checked	Value	Interpretation - Use V9 Event Trigger Mapping is not checked
SGSN_CHANGE	0	SGSN_CHANGE
QOS_CHANGE	1	QOS_CHANGE
RAT_CHANGE	2	RAT_CHANGE
TFT_CHANGE	3	TFT_CHANGE
PLMN_CHANGE	4	PLMN_CHANGE
LOSS_OF_BEARER	5	LOSS_OF_BEARER
RECOVERY_OF_BEARER	6	RECOVERY_OF_BEARER
IP_CAN_CHANGE	7	IP_CAN_CHANGE

Interpretation - Use V9 Event Trigger Mapping is checked	Value	Interpretation - Use V9 Event Trigger Mapping is not checked
QOS_CHANGE_EXCEEDING _AUTHORIZATION	11	QOS_CHANGE_EXCEEDING _AUTHORIZATION
RAI_CHANGE	12	RAI_CHANGE
USER_LOCATION_CHANGE	13	USER_LOCATION_CHANGE
NO_EVENT_TRIGGERS	14	NO_EVENT_TRIGGERS
OUT_OF_CREDIT	15	OUT_OF_CREDIT
REALLOCATION_OF_CREDIT	16	REALLOCATION_OF_CREDIT
REVALIDATION_TIMEOUT	17	REVALIDATION_TIMEOUT
UE_IP_ADDRESS_ALLOCATE	18	UE_IP_ADDRESS_ALLOCATE
UE_IP_ADDRESS_RELEASE	19	UE_IP_ADDRESS_RELEASE
DEFAULT_EPS_BEARER _QOS_CHANGE	20	DEFAULT_EPS_BEARER _QOS_CHANGE
AN_GW_CHANGE	21	AN_GW_CHANGE
SUCCESSFUL_RESOURCE _ALLOCATION	22	SUCCESSFUL_RESOURCE _ALLOCATION
RESOURCE_MODIFICATION _REQUEST	23	RESOURCE_MODIFICATION _REQUEST
PGW_TRACE_CONTROL	24	PGW_TRACE_CONTROL
UE_TIME_ZONE_CHANGE	25	UE_TIME_ZONE_CHANGE
USAGE_REPORT	26	TAI_CHANGE
TAI_CHANGE	27	ECGI_CHANGE
ECGI_CHANGE	28	CHARGING_CORRELATION _EXCHANGE
CHARGING_CORRELATION _EXCHANGE	29	APN_AMBR_MODIFICATION _FAILURE
USER_CSG_INFORMATION _CHANGE	30	USER_CSG_INFORMATION _CHANGE

Interpretation - Use V9 Event Trigger Mapping is checked	Value	Interpretation - Use V9 Event Trigger Mapping is not checked
DEFAULT_EPS_BEARER _QOS_MODIFICATION_FAILURE	31	NA
NA	33	USAGE_REPORT
	34	DEFAULT_EPS_BEARER _QOS_MODIFICATION_FAILURE
	35	USER_CSG_HYBRID _SUBSCRIBED_INFORMATION _CHANGE
	36	USER_CSG_HYBRID _UNSUBSCRIBED _INFORMATION_CHANGE
	37	ROUTING_RULE_CHANGE
	39	APPLICATION_START
	40	APPLICATION_STOP
	42	CS_TO_PS_HANDOVER
	43	UE_LOCAL_IP_ ADDRESS_CHANGE
	44	HENB_LOCAL_IP_ ADDRESS_CHANGE
	45	ACCESS_NETWORK_ INFO_REPORT

Inbound Message Overload Handling

This feature provides a mechanism for the OAM (PCRF) protection when the configured value of handling incoming messages exceeds. It provides a way to prioritize the incoming messages and selectively process them.

The following parameters can be configured under Inbound Message Overload Handling window:

Table 24: Inbound Message Overload Handling Parameters

Parameter	Description
Default Priority	Default priority to be assigned to an incoming message if no specific priority is defined in the Message Handling Rules table. Default value is 0.
Message Sla Ms	Service Level Agreement (SLA) in milliseconds, defines the number of milliseconds that are associated with an incoming event or message within which Policy Director (load balancer) has to submit it to Policy Server (QNS) for processing. In case the configured duration times out, the Default Discard Behavior is applied. Maximum time (in millisec) that a message has in an inbound message handling queue waiting for a worker thread. Configuring this value avoids processing a message to time out by a remote peer. An SLA time that is too large can result in wasted processing on messages already timed out on a remote peer (i.e. PGW) and creation of stale sessions. An SLA time that is too small can result in dropping the messages that could have been successfully processed. Default value is 1500 ms. **Note** The value must be less than timeout configured at Gateway. If you have not selected **Inbound Message Overload Handling** check box under Diameter Configuration, you can define `inboundMessageSlaMs` and `inboundMessageQueueSize` in `/etc/broadhop/qns.conf` file. If `inboundMessageSlaMs` is not defined in `qns.conf` file, then default value of 9000 is used. Example: `-DinboundMessageSlaMs=2000` After modifying the configuration on Cluster Manager execute `reinit.sh` or `copytoall.sh` scripts for applying the changes on all VMs as described in the *CPS Installation Guide for VMware* for this release. If you select **Inbound Message Overload Handling** check box under Diameter Configuration, then the value you configured in Policy Builder is used. The "Message Sla Ms" time out configuration value should be less than the timeout value in PGW or PCSF.

Parameter	Description
Inbound Message Queue Size	Number of messages waiting to be processed before the inbound overload feature is activated. Default value is 1000. If **Inbound Message Overload Handling** check box is not selected under Diameter Configuration, define `inboundMessageSlaMs` and `inboundMessageQueueSize` in `/etc/broadhop/qns.conf` file. If `inboundMessageQueueSize` is not defined in `qns.conf` file, then default value of 1000 is used. Example: `-DinboundMessageQueueSize=5000` After modifying the configuration on Cluster Manager execute `reinit.sh` or `copytoall.sh` scripts for applying the changes on all VMs as described in the *CPS Installation Guide for VMware* for this release. If InboundMessage Overload Handling check box is selected under Diameter Configuration, then the value you configured in Policy Builder is used. **Note** It is recommended not to increase this queue size beyond the default value. This queue size is applicable per Policy Server (qns) node. Configure the message queue size to allow buffering for a burst of messages that can be processed before SLA expiry. A queue size that is too large consumes memory resources. A queue size that is too small drops messages. Configure this parameter help to prevent unnecessary consumption of memory resources for messages that cannot be processed in time.
Default Instance Rate Limit	Use this parameter to trigger the overload protection handling. If this is configured to value *x* TPS, then whenever *x* exceeds CPS applies message handling rules to additional requests. 0 (default) TPS indicates no limit. **Note** It is recommended to use the default value to avoid limit on the performance of Policy Server (QNS). Default value is 0.

Parameter	Description
Gx Emergency Message Priority	Default priority assigned to messages related to an emergency session. This parameter categorizes Gx messages as emergency priority based on APN. Emergency priority messages are queued ahead of non-emergency service messages for quick servicing and prevent them from being dropped using overload controls. If the queue is full, the lowest-priority message is dropped. **Recommended Value:** Regex match of SOS APNs for emergency priority classification. Set emergency priority to highest for priority handling in Policy Server (QNS) Inbound Message Queue. Default value is 1.
Default Discard Behavior	Default behavior to be applied to an incoming message if no specific priority is defined in the Message Handling Rules table. • MESSAGE_DROP: Discards the request. • DIAMETER_TOO_BUSY: Sends a response message having Result-Code AVP value set to DIAMETER_TOO_BUSY (3004) Default value is MESSAGE_DROP.
Apply Discard Behavior For Emergency Messages	Indicates if Emergency Messages can be discarded under overload conditions. Default value is not checked.
Rx Message Prioritization	Defines Rx eMPS message handling priority under overload condition based on Rx AAR MPS-Identifier and Reservation-Priority AVPs. When Rx Message Prioritization is enabled and if MPS-Identifier and Reservation-Priority AVPs are available in Rx_AAR, then the messages are not dropped even in overload condition. Depending on the message **Priority** defined in table, the message can be moved to the front in the inbound queue. This feature indicates that, the Rx_AAR is prioritized based on MPS-Identifier and Reservation-Priority AVPs configured only. If the inbound message doesn't have these parameters included, the message is not prioritized. Prioritization of messages is only applicable to incoming request messages. For more information on parameters, see Table 25: Rx Message Prioritization Parameters, on page 83.
Message Handling Rules	Defines specific inbound message overload handling rules based on different criteria. For more information, see Table 26: Message Handling Rules Parameters, on page 84.

Note If you do not select Inbound Message Overload Handling check box in Diameter Configuration, you can define inboundMessageSlaMs and inboundMessageQueueSize in `/etc/broadhop/qns.conf` file. For more information, see Table 24: Inbound Message Overload Handling Parameters, on page 80.

Table 25: Rx Message Prioritization Parameters

Parameter	Description
MPS Identifier	MPS-Identifier indicates that an AF session relates to an MPS session. It contains the national variant for MPS service name. MPS-Identifier value = <NS (National Security) Specific To Deployment>
Reservation Priority	The AF specifies the Reservation-Priority AVP at request level in the AA-Request in order to assign a priority to the AF session as well as specify the Reservation-Priority AVP at the media-component-description AVP level to assign a priority to the IP flow. The Reservation-Priority AVP available at the request level only is used under Rx Message Prioritization table. Range: Any number Example: 10
Priority	A user defined priority based on MPS-Identifier and Reservation-Priority combination. Make sure that the Message priority defined in Rx Message Prioritization table and should be unique per row. Higher Priority messages are processed first compared to lower priority messages. Range: Any number (User priority) Example: 10

Note Rx Message Prioritization table does not supports multiple values in a single column. Rx Message Prioritization table must be configured with unique combination for each row.

Table 26: Message Handling Rules Parameters

Parameter Type	Attribute	Description
INPUT	Diameter Client	(Optional) This field is used to configure different priorities for different clients based on realms. For more information, see Diameter Clients, on page 119.
	Protocol	Specific application id value to be used for scoring. This value is used to match Auth-Application-Id AVP value. For more information, see Table 27: Protocols, on page 85.
	Command Code	Specific command code value to be used for scoring. This value is used to match the Command-Code field. These command codes map to different types of Diameter messages (CCR = 272 RAR = 258 etc). Default value is 0.
	Request Type	Specific request type value to be used for scoring. This value should match the value of the CC-Request-Type AVP for Gx CCR messages. • 0: Request Type not used for scoring • 1: INITIAL_REQUEST (1) • 2: UPDATE_REQUEST (2) • 3: TERMINATION_REQUEST (3) Default value is 0. Request type should match the value of the Rx-Request-Type AVP for Rx AAR messages. • 0 INITIAL_REQUEST (0) • 1 UPDATE_REQUEST (1) Request type should match the value of SL-Request-Type AVP for Sy SLR messages. The possible values are: • INITIAL_REQUEST (0) • INTERMEDIATE_REQUEST (1) It has to be configured to zero if the incoming message does not have a request type AVP. For example, Rx STR does not have a request type AVP or Rx-Request-Type AVP is unavailable in Rx AAR as it is not a mandatory AVP per 3GPP TS 29.214.

Parameter Type	Attribute	Description
OUTPUT	Priority	Priority value assigned to the message. Higher numerical value has the higher priority. Default value is 0. For example, 10, 20, 100, 200, 300, 500 and so on.
	Per Instance Tps	Transactions per second limit per process. This value is the TPS that these messages are limited to. Note that this is per CPS process so if there are 20 Policy Server VM's with 1 Policy Server java process the total TPS is this number x 20. The actual system's transaction per second limit can be calculated using the following formula: Per Instance Tps x Number of instances per VM x Number of VMs. Default value is 0. For example, 1000, 2000, 5000 and so on.
	Discard Behavior	Behavior to be applied to an incoming message. • MESSAGE_DROP: Discards the request. • DIAMETER_TOO_BUSY: Sends a response message having Result-Code AVP value configured to DIAMETER_TOO_BUSY (3004). Default value is MESSAGE_DROP.

Note A Diameter message even if prioritized under an overload condition could be dropped by CPS if one of the following conditions are met:

- Per Instance TPS configured limit exceeds except for Gx Emergency/Rx eMPS/DRMP calls.
- Inbound Message Queue size exceeds for a message.
- Inbound Message Sla Ms exceeds for a message.

Table 27: Protocols

Attribute	Description
GY_V8	Standard Gy application as per 3GPP TS 32.299
GX_SCE	Custom Gx implementation
RF_V10	Not supported

Attribute	Description
RF_VERIZON	Not supported
RX_TGPP	Standard Rx application as per 3GPP TS 29.214
SH_TGPP	Standard Sh application as per 3GPP TS 29.329
SY_V11	Standard Sy application as per 3GPP TS 29.219
SD_V11	Standard Sd application as per 3GPP TS 29.212
GX_TGPP (default)	Standard Gx application as per 3GPP TS 29.212
GXX_TGPP	Not supported
RX_CLIENT	Local MINE adapter
GY_V8_PROXY	Gy proxy implementation as per RFC 3588
GX_TGPP_PROXY	Gx proxy implementation as per RFC 3588
SY_TGPP_PROXY	Sy proxy implementation as per RFC 3588
SY_OCS	Sy Proxy from OAM (PCRF) end
GY_RECHARGE_WALLET	Support Gy client functionality with external OCS (ECUR model only)
SY_PRIME	Custom Sy implementation as per RFC 3588
RX_TGPP_PROXY	Rx proxy implementation as per RFC 3588
SY_OCS_SERVER	OCS Sy server endpoint conforming to 3GPP TS 29.219

Note When a Diameter Stack with a diameter realm is imported with unassigned protocol, the default value of GX_TGPP is used.

Stale Session Message Handling Configuration

This feature enables CPS application to act according to the configuration when request processing crosses the given SLA time period for the incoming request. When the feature is enabled the request or responses which are crossing the configured SLA are dropped.

By default, stale session message handling is disabled. To enable this configuration, you need to configure the Stale Session Message Handling configuration in Policy Builder and publish the changes.

Note The configuration changes are reflected at the run time and no process restart is required.

The following table describes the parameters under **Stale Session Message Handling Configuration**.

Table 28: Stale Session Message Handling Configuration Parameters

Parameter	Description
End to End Sla Ms	Maximum time in milliseconds the CPS system must take for request processing. The request processing time for this value must be LB > QNS > DB > QNS > LB round trip. Default: 2000 ms
Include Request LB queue time in QNS SLA	When checked, LB - QNS request queue time is considered in QNS SLA when enabled. Default value is disabled.

Note

- The End To End SLA value must always be greater than the existing QNS-SLA configured in the `qns.conf` file.
- All the Policy Director (LB) and Policy Server (QNS) VMs need to be in time sync to ensure that the functionality of this feature works as expected.

Next Hop Routing

This feature provides support for inter-working with a DRA that is not configured in topology hiding mode. This is required because while the DRA advertises its own origin host and realm values when the diameter connection is established all the diameter application messages feature the actual host's origin host and realm (i.e. PCEF TDF AF). PCRF needs a way to figure out which particular DRA connection should use in order to deliver a message to the desired host.

While selecting the peer that is used to deliver the request (with or without using the Next Hop Routes table) load balancing across the peers having the same rating is done. Load balancing starts from the peers having highest rating and covers all the peers in a round robin manner. If none is UP load balancing is tried with the peers having the second highest rating and again covers all the peers in a round robin manner and so on.

Note Next Hop Routes table is used only for PCRF initiated requests. The response messages for any incoming request is always delivered on the same connection where the request was received or not delivered at all. This is in order to avoid asymmetric routes.

The DRA should explicitly advertise support for a Diameter application other than Relay. The Relay application having Application Identifier 0xffffffff is not supported.

The following parameters can be configured under Next Hop Routing table:

Table 29: Next Hop Routing Parameters

Parameter	Description
Next Hop Realm	DRA realm name as received in Origin-Realm AVP in CER or CEA message. **Note** All the next hop realms (Next Hop Realm) should match the Origin-Realm AVP value in the incoming CER/CEA message.
Next Hop Hosts	DRA hosts name list as received in Origin-Host AVP in CER or CEA message. **Note** All the next hop host names (Next Hop Hosts) should match the Origin-Host AVP value value in the incoming CER/CEA message.
Application Id	Diameter application id advertised as being supported by the DRA. It contains information that identifies the particular service that the service session belongs to.
Destination Realms Pattern	Actual destination realm name pattern as received in Origin-Realm AVP in AAR message. The pattern needs to follow the standard Java regular expression syntax described here.
Destination Host Pattern	Actual destination host name pattern as received in Origin-Host AVP in AAR message. The pattern needs to follow standard Java pattern conventions. The pattern needs to follow the standard Java regular expression syntax described here.

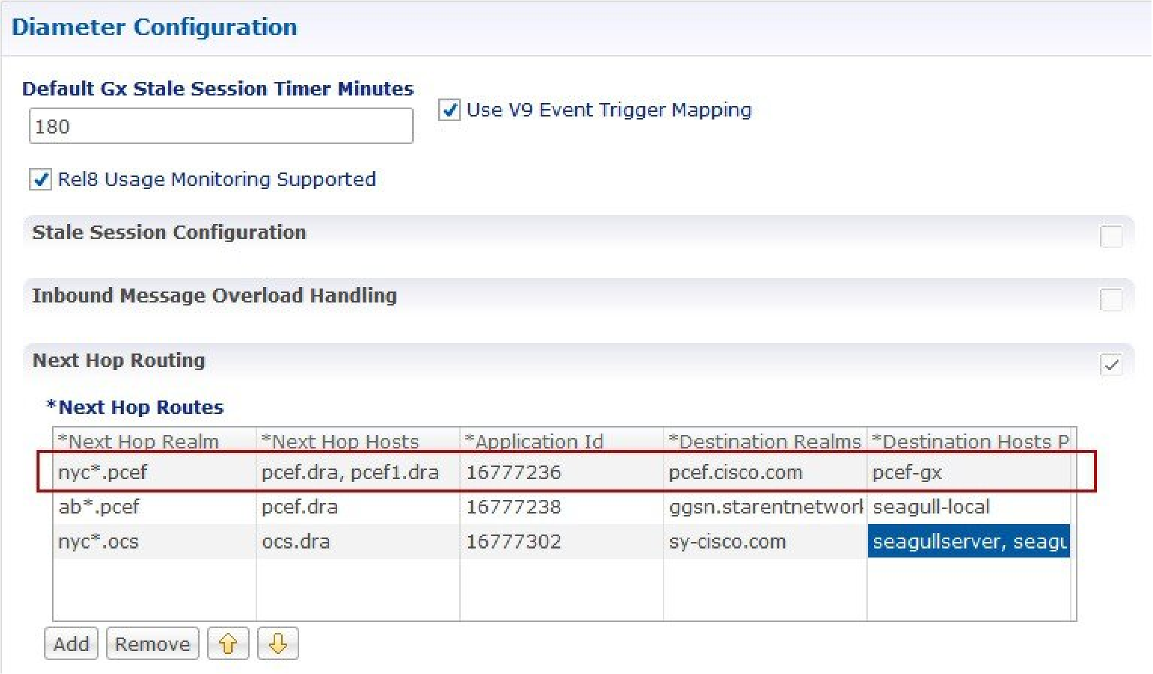
While populating the Next Hop Routes table, we recommend that you create only one entry for each Next Hop Realm value - Application Id value pair while all the DRA host names are provided as a list under Next Hop Hosts field. This is not a requirement though.

Note The order in which the DRA hosts are provisioned in the Next Hop Hosts field for any given next hop route is not relevant. The DRA host having the highest rating (priority) value is used. In case multiple hosts have the same rating one is randomly selected. Refer to Diameter Stack Configuration, on page 107 for more details about host rating. Outbound realm rating of next hop is not considered except for SY_PRIME.

CPS supports grouping of realms and application identifiers using wildcarding and assigns it to a group of next hop peers. CPS routes outgoing messages by selecting the peer with highest priority.

An example configuration for Grouping and Wildcarding in the Next Hop Routing table is shown below:

Figure 39: Grouping and Wildcarding in the Next Hop Routing Table



Diameter Configuration

Default Gx Stale Session Timer Minutes

180

☑ Use V9 Event Trigger Mapping

☑ Rel8 Usage Monitoring Supported

Stale Session Configuration □

Inbound Message Overload Handling □

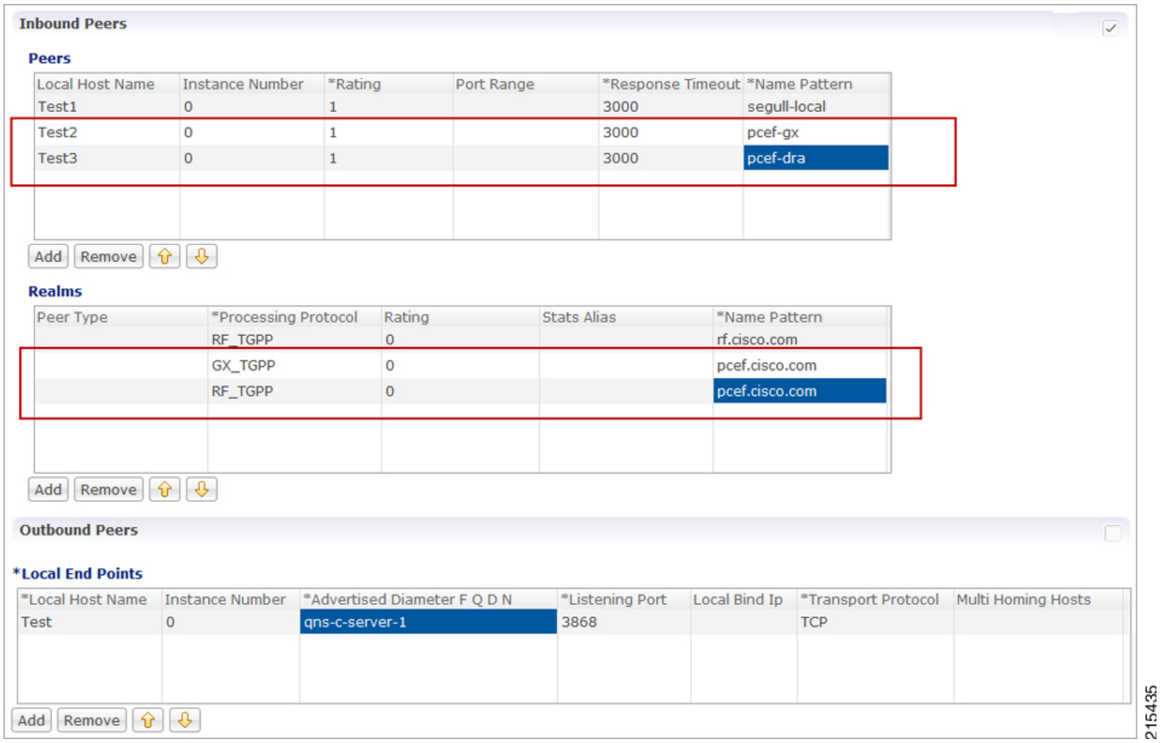
Next Hop Routing ☑

*Next Hop Routes

*Next Hop Realm	*Next Hop Hosts	*Application Id	*Destination Realms	*Destination Hosts P
nyc*.pcef	pcef.dra, pcef1.dra	16777236	pcef.cisco.com	pcef-gx
ab*.pcef	pcef.dra	16777238	ggsn.starentnetworl	seagull-local
nyc*.ocs	ocs.dra	16777302	sy-cisco.com	seagullserver, seagu

Destination Realm and Destination Hosts are used to map with the Peer configuration as defined in the Diameter Stack. The figure given below shows the mapping of the message containing the Realm from a peer to a protocol or interface. For more information on peer configuration refer to Diameter Stack Configuration, on page 107.

Figure 40: Rating



Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
Test1	0	1		3000	segull-local
Test2	0	1		3000	pcef-gx
Test3	0	1		3000	pcef-dra

Realms

Peer Type	*Processing Protocol	Rating	Stats Alias	*Name Pattern
	RF_TGPP	0		rf.cisco.com
	GX_TGPP	0		pcef.cisco.com
	RF_TGPP	0		pcef.cisco.com

Outbound Peers

***Local End Points**

*Local Host Name	Instance Number	*Advertised Diameter F Q D N	*Listening Port	Local Bind Ip	*Transport Protocol	Multi Homing Hosts
Test	0	qns-c-server-1	3868		TCP	

Message Timeout and Retry Configuration

Message Timeout and Retry Configuration table can be configured under Diameter Configuration plug-in in Policy Builder.

This table allows for the configuration of different message timeout value and retry behavior using the combination of Application Id, Command Code and (experimental) result code parameters.

Note Sh Interface (Auth-Application-Id 16777217) message retry information can be configured using:

- Message Timeout and Retry Configuration table
- Setting Up Additional Profile Data

Only one of the two retry configuration options should be used for Sh Interface.

The following parameters can be configured in the Message Timeouts and Retry Configuration table.

Table 30: Message Timeout and Retry Configuration Parameters

Parameter	Description
Application Id	The Diameter Application ID (Auth-Application-Id) on the message which is to be retired. Default: 0
Command Code	The Diameter command code of the message which is to be retried. Default: 0
Result Code	This is the result code received in the diameter response for which the user wants to retry. The values configured should be a valid diameter result code value or an experimental result code value. For example, 3002 (DIAMETER_UNABLE_TO_DELIVER) received in RAA**.** Permanent failure result codes 5*xxx* and successful result codes 2*xxx* should not be configured (where, *x* denotes a valid number). However, if configured, CPS retries for it. **Note** For retry on timeout, the result code should be configured as 7000. Default: 0
Is Experimental	If this check-box is selected, it means that the value configured in the Result Code column is an Experimental-Result-Code value. This is necessary because there are few values which are the same for both experimental-result-code and result-code. Default: Not selected
Action	The action for the CPS platform to take after the Diameter Response is received. The options are Retry or None. • Retry - CPS retries the request message identified by the value in the command code column depending on the retry count configured in Retry Count column. • None - No retry. Default: None
Action Timer (Ms)	The amount of time in milliseconds for CPS to wait before doing a retry. It is the wait time between retries. CPS doesn't retry immediately and drops all the stress on the system[2]. Default: 0
Retry Count	The number of times to retry when the action is “Retry”. **Note** This retry count does not include the initial attempt made by CPS. Default: 1

Parameter	Description
Retry on Alternate Node	Configures CPS to retry on any alternate peer configured in Policy Builder. Default: Not selected
Backoff Algorithm	The back-off algorithm used while determining the actual delay between retry attempts. Currently, only one option (CONSTANT_INTERVAL) is supported. • LINEAR_INTERVAL: Causes the configured retry interval to increase linearity with each attempt using the formula retry interval = Action Timer (Ms) x current retry attempt number. For example, Action=Retry, Action Timer (Ms)=200, Retry Count=3, Backoff Algorithmm=LINEAR_INTERVAL will trigger the first retry after 200 x 1 = 200 ms, the second retry after 200x2 = 400 ms, the third retry after 200x3 = 600ms • CONSTANT_INTERVAL: Causes the configured retry interval to be used (without any change) for delay for all retry attempts (other options like exponential back-off where retry interval increases exponentially are currently not supported/implemented). Default: CONSTANT_INTERVAL

[2] If the timeout and retry count is not configured then the default values (`diameter.default.timeout.ms` and `diameter.default.retry.count`) defined in `/etc/broadhop/qns.conf` are used.

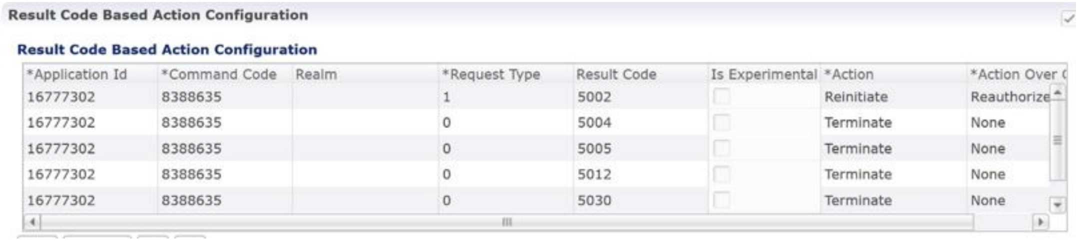
The `diameter.default.timeout.ms` and `diameter.default.retry.count` parameters configured in `qns.conf` file are taken into consideration only in case of timeout (result code = 7000) and do not impact the behavior in any other case (result code other than 7000).

If no values are defined in the `qns.conf` file, then the default values of `diameter.default.timeout.ms=3000` and `diameter.default.retry.count=1` are used. If Result Code = 7000 is defined in the Message and Retry Configuration table in Policy Builder, then this configuration takes precedence over `qns.conf` file parameters.

Result Code Based Action Configuration

CPS can be configured to take specific action over Gx and Sy based on response received on Sy/Sd interfaces. CPS can be configured to continue (default) terminate or re-initiate the session.

Figure 41: Result Code Based Action



Result Code Based Action Configuration

Result Code Based Action Configuration

*Application Id	*Command Code	Realm	*Request Type	Result Code	Is Experimental	*Action	*Action Over
16777302	8388635		1	5002	□	Reinitiate	Reauthorize
16777302	8388635		0	5004	□	Terminate	None
16777302	8388635		0	5005	□	Terminate	None
16777302	8388635		0	5012	□	Terminate	None
16777302	8388635		0	5030	□	Terminate	None

The following parameters can be configured in the Result Code Based Action Configuration table.

Table 31: Result Code Based Action Configuration

Parameter	Description
Application Id	The diameter interface in numeric format (Auth-Application-Id) on which the message is received. For example Sy (16777302) and Sd (16777303). Currently only Sd and Sy interfaces are supported. Default: 0
Command Code	The diameter message type. For example SLR (8388635) in case of Sy and RAR (258) in case of Sd. Default: 0
Realm	New key added as Sy client realm. If the realm value is not specified, then the realm key is not be considered (CPS only performs action on key `applicationid:commadcode:realm:requestType:resultcode`).
Request Type	The request type of the message for Sy interface. For example INITIAL_REQUEST (0) INTERMEDIATE_REQUEST (1). For Sd Request Type is not valid. Default: 0
Result Code	The result-code received in the response for which the action over Gx and/or Sy/Sd is to be taken. Default: 0
Is Experimental	If this check-box is selected, it means that the value configured in the Result Code column is an Experimental-Result-Code value. This is necessary because there are few values which are the same for both experimental-result-code and result-code. Default: Not selected
Action	The action to be taken over the Sy/Sd interface when the response is received. Possible actions are Continue/Terminate/Reinitiate. • Continue (default) In case of Continue CPS just continues with the session and does not clear the session from the DB. • Terminate (for Sd) In case of Terminate CPS removes the session from database after triggering a Session Removal RAR over Sd interface. Terminate (for Sy) In case of Terminate CPS removes the session from database after triggering a Session Removal STR over Sy interface. • Reinitiate (for Sd) In case of Reinitiate CPS first triggers a Session Removal RAR over Sd interface. Once we receive Sd RAR response (any result-code) CPS removes the old session and triggers creation of a new session by sending out a TSR towards TDF. Reinitiate (for Sy) In case of Reinitiate CPS first triggers a Session Removal STR over Sy interface. Once we receive Sy STR response (any result-code) CPS removes the old session and triggers creation of a new session by sending out SLR towards OCS.

Parameter	Description
Action Over Gx	The action to be taken over the Gx interface when the response is received. Possible actions are None/Terminate/Reauthorize. Currently Action over Gx is not supported for Sd RAR. • None (default): No action would be taken on Gx interface. • Terminate: In case of Terminate CPS would terminate the Gx session by sending a RAR with Session Release Cause. Also CPS would be sending STR which would then clear the corresponding Sy device session. If the action over Gx is TERMINATE the action over Sy does not matter as the Sy session would be terminated. • Reauthorize: In case of Reauthorize CPS would mark the Sy session as waiting for action over Gx and would mark corresponding Gx session as needing action over Gx as Re-Auth. The Gx Network Device Manager would then perform the ReAuthorization by sending RAR over Gx interface. On receiving RAA the action over Sy interface would then be performed. If the Gx session is stale and we receive DIAMTER_UNKNOWN_SESSION_ID the Sy session would then be automatically terminated irrespective of the action configured on Sy interface. **Note** The actions TERMINATE and REAUTHORIZE over Gx does not work with SLA-Initial if the SLR is sent synchronously. In case the SLR is triggered synchronously and the action over Gx is configured as TERMINATE/REAUTH the CPS would log an error message and would continue the session. The synchronous/asynchronous sending of SLR can be configured in the SpendingLimitReport service configuration.

Message Buffering Configuration

When Gx features for OneGxRulePerFlow is enabled then the gateway triggers simultaneous Gx-CCR-Us for APPLICATION-START within a short time span. This causes a burst of CCR-U message on CPS. Because of the burst, CPS fails to process all the CCR-U message due to "cache out of date" errors and sends DIAMETER_UNABLE_TO_DELIVER errors to gateway. So in order to support the processing of all the CCR-U messages, Message Buffering Configuration can be used.

Message Buffering Configuration can be configured under **Diameter Configuration** plug-in in Policy Builder.

The following parameters can be configured under **Message Buffering Configuration**:

Table 32: Message Buffering Configuration Parameters

Parameter	Description
Buffer Timeout In Milliseconds	The time in milliseconds to hold the diameter messages in the buffer after the buffering has been triggered for a particular session ID. Default value is 15 ms.

Parameter	Description
Max Buffered Messages Per session	Maximum number of messages that are held in the message buffer for a particular session ID. Default value is 64.
Disable Early Processing	Disable the early processing of buffered message before the configured buffer-timeout (15 ms). If the message buffering has started then CPS triggers an early timeout (after 5 ms) and check the buffer status. If the buffer has single message or contains messages without any holes (in correct sequence) then it sends the first message to Policy Server (qns) node for processing. Default value is unchecked.
Allow Gaps In Buffer	Do not drop the messages from the message buffer when a hole/gap is detected while processing the buffered messages (i.e. after ordering the buffered message it detects that certain messages are missing). Default value is unchecked.
Message Buffering Table	This table is used to specify the criteria for buffering the messages. CPS buffers only those messages that have a matching entry in this table. For more information on parameters, refer to Table 33: Message Buffering Table Parameters, on page 95.

Table 33: Message Buffering Table Parameters

Parameter	Description
Application Id	Application ID of the interface whose message are to be buffered. For example, 16777238 for Gx messages.
Command Code	Command code of the diameter message for the above application ID. For example, 272 for CCR messages.
Origin Realm Pattern	Origin-realm from the diameter request message to check for message buffering. It supports pattern matching as per the JAVA regular expression. This is an optional field and if not configured then CPS applies the configuration to any realm for the matching application ID and Command Code.
Origin Host Pattern	Origin-host from the diameter request message to check for message buffering. This is an optional field and if not configured then CPS applies the configuration to any host for the matching application ID and Command Code. **Note** In case of multiple entries for same application ID and command code combination, CPS matches the origin-realm and origin-host from the message with the realm and host patterns defined in the table and use the row that matches first.

Parameter	Description
Buffer Start Avp Code	Diameter AVP code for the AVP that would trigger the start for buffering the messages. For example, 1006 is the diameter AVP code for Event-Trigger AVP. **Note** Allowed parameters are of string type so that child AVP path can also be used. For example, To give **Charging-Rule-Report** > **Rule-Failure-Code**, you have to mention '1018.1031' (where, 1018 is an AVP Code for 'Charging-Rule-Report' and 1031 is an AVP Code for 'Rule-Failure-Code'). All rows having same 'Application Id' and 'Command Code' should have same Order AVP Code and Order AVP Type. CPS goes through all the rows one by one and verifies whether configured AVP exist in the incoming message and buffers the message accordingly.
Buffer Start Avp Type	A drop-down list to select the data-type of the AVP to trigger buffering of message. This is required for correctly extracting the AVP value.
Buffer Start Avp Value	The possible values for the diameter AVP for starting the buffering of message. List supported to configure multiple values.
Order Avp Code	The diameter AVP code for the AVP whose value can be used for sequencing/ordering the buffered message while sending them to Policy Server (qns) node for processing.
Order Avp Type	A drop-down list to select the type of the Order AVP for extracting its value. CPS currently supports only numeric values for ordering the buffered messages.

Memory Impact

- The memory usage of diameter endpoint process (qns process on lb) may be increased when it starts buffering messages for multiple sessions.

Configuration and Restrictions

- Buffered messages are lost if the diameter-endpoint (qns process) on LB node goes down.
- All the CCR-U messages in the burst are processed sequentially, that is, only after a CCA-U is sent out for a CCR-U message then the next CCR-U message is taken up for processing.
- CPS initiated messages (for example, Gx RAR) are not considered for buffering and are sent out as they are triggered. Also, if terminate message (for example, Gx CCR-T) is received in between a message burst then CPS drops all further messages from the buffer after processing the terminate message.
- As the buffered messages are processed sequentially the response time (towards PCEF) increases. For example, for a burst of 64 simultaneous CCR-U messages, CCA-U for the last message (that is, CCR-U message with highest sequence number) is after a duration of 64*20+15 ms (approx. 1300 ms).

- The response time (towards PCEF) for normal messages (not received in a burst but matches the message buffering criteria) has an impact of at least 5 ms (the early processing time). For example, if CCR-U processing takes 20 ms then for a single user plane CCR-U message, the minimum response time is 25 ms.
- If CPS receives negative response from Policy Server (qns) node while processing a buffered message then CPS stops processing the message buffer for that session and drops all further buffered messages.
- While processing a buffered message if Policy Director (lb) node does not get a response from Policy Server (qns) node within the configured time (SLA) then it drops all the remaining messages from the message buffer of that session. The SLA time is calculated from the time the message was sent from Policy Director (lb) to Policy Server (qns) node and the time that the message spends while waiting for processing in the message buffer.
- CPS checks only for 3GPP vendor ID while matching the diameter AVP code defined for Buffer start AVP and Order AVP. If vendor ID is not available in the received AVP then it is assumed to be of default 3GPP vendor ID.
- While processing the buffered messages, if another burst of CCR-U messages is received then CPS appends those messages to the existing buffer. In doing so if the buffer size reaches the Max Buffered Messages per session then CPS drops those messages.
- CPS maintains the order only for buffered messages. Order is not checked for messages across multiple message bursts for same session.

PolicyDRA Health Check

PolicyDRA Health Check is used to initiate a dummy AAR message that results in querying the binding database allowing the PCRF to take corrective action based on the response.

PolicyDRA Health Check is configured under **Diameter Configuration** plug-in in Policy Builder. Select **PolicyDRA Health Check** and **Binding Db** configuration to enable the feature.

The following parameters can be configured under **PolicyDRA Health Check**:

Table 34: PolicyDRA Health Check Configuration Parameters

Parameter	Description
Binding Db	When selected, it enables the feature. When unselected, the feature is disabled. • Health Check Time Interval: Time interval in seconds when periodic AAR is sent. **Note** The Health Check Time Interval and Revalidation Time under **RevalidationTime** service configuration should not be configured with the same value. For more information on Revalidation Time, refer to *RevalidationTime* in *Service Configuration Objects* chapter. • Session Release T P S: Per Policy Server (QNS) Gx RAR (with session release cause) TPS when binding database is down. Default value is 0.
Alarm Config	When selected, it enables the generation of alarms or traps. When unselected, the alarms are not generated. • Primary Ip Address: Primary database IP address where the alarm information is stored. Whenever PolicyDRA binding database down is detected i.e., when AAA comes with error result code, CPS generates a trap/notification/alarm. The generation time of this alarm is stored in the database configured. After the Alarm Clearance Interval, the trap/notification/alarm is cleared by CPS. In between this duration, CPS does not generate trap/notification/alarm on detection of binding database failure. Only one trap/notification/alarm is generated by CPS. • Secondary Ip Address: Secondary database IP address where the alarm information is stored. • Port: Port number of the database. Default value is 0. • Alarm Clearance Interval: Timer interval in seconds after which the alarm is cleared. • Policy Dra Resultcode: AAA result-codes for which alarms are generated. • Severity: Severity of the alarm. Default value is Critical.
Enable Proxy	When checked, it makes sure P-Bit is set and Destination-Host AVP is not set for the outgoing AAR messages for PAS Health check. Default value is unchecked.

Note To improve the performance when PolicyDRA Health Check is enabled, you must configure ‘RxClientSessionKey’ key as the Lookaside Key Prefix so that memcache is used and full database scan is avoided. This is highly recommended for higher capacity systems.

Diameter Messages Action on Threshold in LB

When **Diameter Messages Action on Threshold in LB** check box is enabled and **Diameter Message Count Threshold for PD** is configured with value greater than 0, the Policy Director processes keep track of messages being handled at process level and when number of messages being tracked crosses the configured **Diameter Message Count Threshold for PD**, the messages are dropped or responded with DiameterBusy.

Diameter Messages Action on Threshold in LB configuration is optional. When this configuration is not used, all the messages are sent from LB (Policy Director) to Policy Engines.

- The following parameters can be configured under **Diameter Messages Action on Threshold**:

Table 35: Diameter Messages Action on Threshold

Parameter	Description
Diameter Interface	Diameter Interface in Diameter message selected from drop-down list.
Command Code	Command code in Diameter message. When Command Code is set to 0, it applies to all Command Codes of the Application ID configured in the row.
Request Type	CCR Request type. Default value is 0. When Request Type is set to 0, it applies all the CCR Request types, namely Initial(1), Update(2) and Terminate(3). For non-CCR messages default 0 is must be set.
Action	What action to take when the Diameter message is received at LB (Policy Director) when outstanding Diameter messages have reached the **Message Count Threshold.** Possible Values: MESSAGE_DROP and DIAMETER_TOO_BUSY Default value is MESSAGE_DROP.

- **Diameter Message Count Threshold for PD**: This value defines the maximum number of a Diameter Inbound/Outbound messages per PD (Policy Director) process from the table **Diameter Messages Action on Threshold in LB**. Default value is 0.
- **Max TPS per PD**: Defines maximum TPS supported per PD process. Default value is 0.
- **Default Discard Behavior**: Describes the action to be taken when a Diameter request message is received in LB and rate limiter acquire fails. Possible values include **MESSAGE_DROP** and **DIAMETER_TOO_BUSY**. Default value is **MESSAGE_DROP**.

Note

If **DIAMETER_TOO_BUSY** is selected from the drop-down list, at very high TPS, it can lead to higher CPU consumption on Policy Director (LB) VM. This can lead to performance degradation. Cisco recommends using **MESSAGE_DROP**.

Session Id Handling Configuration

Session Id Handling Configuration provides an option to parse part of the Diameter session ID attributes and store them in session AVP.

The following table describes parameters that can be configured under **Session Id Handling Configuration**.

Table 36: Session Id Handling Configuration

Parameter	Description
Diameter Interface	Diameter Interface DM for which the Session ID handling is required.
Input Regex	Provide an inverse regex to derive the new AVP. **Example:** Consider the Session ID is pcef01.dstest01.2b4.gx;375030;1285311481;BB2001@MCC2001. To get the Gw_Version BB2001@MCC2001, write an inverse regex ".*;.*;.*;" which returns BB2001@MCC2001 as value.
Output Policy AVP Name	Policy derived AVP name to be stored.
Save to Session	Save the policy derived AVP to session.
Origin Realm	Origin-realm from the diameter request message to parse the session ID.
Origin Host	Origin-host from the diameter request message to parse the session ID.

Gx Offline Stale Session Cleanup

Important

This feature is only enabled for deployments with arbitervip running on pcrfclient VMs.

Stale session builds up due to network issues, timeout at PAS and so on. As a result CPS starts rejecting new sessions due to capacity or session license limit. The offline Stale Session cleanup helps to remove the stale sessions having duplicate IMSI and AON combination.

Execute the following command in the pcrfclient where the application is running to stop the application:

```
monit stop stale-session-cleaner-helper
```

Execute the following command in the pcrfclient where the application is not running to restart the application:

```
monit restart stale-session-cleaner-helper
```

The following table lists parameters in the `/etc/broadhop/stale-session-cleaner/stale-session-cleaner.conf file`:

Table 37: Gx Offline Stale Session Cleanup Configuration Parameters

Parameter	Description
-Dadmin.primary.host	VM name which hosts the primary member of the PCRF Admin replica-set. Any sessionmgr VM names. Default value is localhost. Example: sessionmgr01
-Dadmin.secondary.host	VM name that hosts a secondary member of the PCRF Admin replica-set. If the primary Admin member fails, the Stale Session Cleaner tries to connect to this secondary member. Any sessionmgr VM names. Default value is localhost. Example: sessionmgr02
-Dadmin.port	Port of the PCRF Admin replica-set. Possible values can be Integers. Default value is 27017. Example: 27721
-Dmemcache.host	The Host on which memcache is running on. Strings in the following format: `<host>:<port>` Default value is localhost.
-Dmemcache.port	The Port number of memcache. Possible values are Integers. Default value is 11211.
-Dtps.per.shards	Maximum number of executions per second per shard. Possible values are Integers. Default value is 200.
-Dmongo.query.batch.size	Number of records in the results for each query to the Session replica-set. Possible values are Integers. Default value is 1000.

Parameter	Description
-Dfactor.count.audit.log	If the number of deleted sessions reaches a multiple of this parameter's value, it performs audit log. For example, if the parameter value is 100, then the deleted count is printed in the logs on 100 deletions, 200 deletions, 300 deletions, and so on. Possible values are Integers. Default value is 10000.
-Dsession.count.threshold	Specify the minimum count of session at which the utility triggers stale session cleanup. Possible values are Integers. Default value is 15000000.
-Dsession.threshold.timer	The frequency in minutes where utility monitors session threshold breach to start deletion of stale session. Possible values are Integers. Default value is 5.
-Dsession.cache.update.timer	The frequency in minutes where utility updates the latest session ID in the local cache. This parameter should be in the multiple of "session.threshold.timer." Possible values are Integers. Default value is 30.
-Dnumber.of.shards	Total number of shards for the Session replica-sets. Possible values are Integers. Default value is 80.
-Dlogback.configurationFile	The path to the log configuration file. Any directory path with a logback file for the application. Default value is /etc/broadhop/logback-stale-session-cleaner.xml.

Cleaning Stale Session

Important This feature is only enabled for deployments with arbitervip running on pcrfclient VMs.

The services for the application are running on pcrfclient from first deployment, but the application does not start unless the arbitervip is present on the pcrfclient VM. The default value for admin database is 127.0.0.1. Application only starts to delete stale sessions when admin database is correctly configured.

Stale session build up due to network issues when CPS is processing bulk traffic. Stale sessions are observed when there is an increase in incoming request and timeouts are observed. Session replica-sets are piled-up with the sessions and once the session capacity limit is breached, CPS start rejecting new session requests.

The existence of stale sessions in session replica sets results in storage of duplicate sessions, i.e. multiple sessions from a subscriber UE to the same APN. This feature is to identify the duplicate sessions (match with same IMSI + APN) in regular intervals and keep the latest session and remove the older duplicate sessions to make sure that there is no additional overhead in call processing.

Note Enabling/disabling this feature does not have any impact on existing stale session functionality.

This utility cleans the stale sessions without sending RARs to the gateway. This utility does not deletes corresponding records from SK database.

The following table lists parameters in the `/etc/broadhop/stale-session-cleaner/stale-session-cleaner.conf` file:

Table 38: Stale Session Cleanup Configuration Parameters

Parameter	Description
-Dadmin.primary.host	VM name which hosts the primary member of the PCRF admin replica-set. Any sessionmgr VM names. Default value is localhost. Example: `-Dadmin.primary.host=sessionmgr01` Possible Values: Primary Admin database name
-Dadmin.secondary.host	VM name that hosts a secondary member of the PCRF admin replica-set. If connecting to primary admin member fails, the Stale Session Cleaner tries to connect to this secondary member. Any sessionmgr VM names. Default value is localhost. Example: `-Dadmin.secondary.host=sessionmgr02` Possible Values: Secondary Admin database name
-Dadmin.port	Port of the PCRF admin replica-set. Default value is 27017. Example: `-Dadmin.port=27721` Possible Values: Integers (port number)

Parameter	Description
-Dmemcache.host	The hostnames on which memcache is running on. Comma separated memcached server hostnames. Utility distributes memcached keys among the specified servers based on consistent hashing. **Note** If any of the specified instances is down, then utility cannot save memcache keys related to those instances and sale sessions corresponding to those keys are not cleaned. Default value is pcrclient01,pcrfclient02. Example: `-Dmemcache.host=pcrclient01,pcrfclient02` Possible Values: Strings in the following format: `<hostName1>,<hostName2>`
-Dmemcache.port	The port number of memcache. Default value is 11211. Example: `-Dmemcache.port=11211` Possible Values: Integers
-Dtps.per.shards	The number of parallel tasks for scanning and cleaning the sessions. **Note** If the session creation TPS per shard (can be determined by max possible Gx CCR-I TPS / no. of shards) is higher than value configured, then utility does not process the older sessions. Default value is 200. Example: `-Dtps.per.shards=200` Possible Values: Integers
-Dmongo.query.batch.size	The number of records to return in each batch of the response from the MongoDB instance. Default value is 1000. Example: `-Dmongo.query.batch.size=1000` Possible Values: Integers

Parameter	Description
-Dfactor.count.audit.log	It prints the logs if the number of deleted sessions reaches a multiple of this parameter’s value. For example, if the parameter value is 100, then the deleted count is printed in the logs on 100 deletions, 200 deletions, 300 deletions, and so on. Default value is 10000. Example: `-Dfactor.count.audit.log=10000` Possible Values: Integers
-Dsession.count.threshold	Session clean up is kicked in after total active session count is greater than `session.count.threshold` value. Default value is 15000000. Example: `-Dsession.count.threshold=15000000` Possible Values: Value must always be greater than total active sessions
-Dsession.threshold.timer	The frequency in minutes where utility monitors session threshold breach to start deletion of stale session. Default value is 5. Example: `-Dsession.threshold.timer=5` Possible Values: Integers
-Dsession.cache.update.timer	The frequency in minutes where utility updates the latest session ID in the local cache. This parameter should be in the multiple of `session.threshold.timer` value. Default value is 30. Example: `-Dsession.cache.update.timer=30` Possible Values: Integers
-Dnumber.of.shards	Total number of shards for the session replica-sets. Default value is 80. Example: `-Dnumber.of.shards=80` Possible Values: Integers

Parameter	Description
-Dlogback. configurationFile	The path to the log configuration file. Default value is `/etc/broadhop/logback-stale-session-cleaner.xml`. Example: `-Dlogback.configurationFile=` `/etc/broadhop/logback-stale-session-cleaner.xml` Possible Values: Any directory path with a logback file for the application.
-DdbPassword	Configure the database password if MongoDB Authentication is enabled. Example: `-DdbPassword=encryptedDbPassword` Make sure to restart the Stale session utility after mongo db password change procedure. For more information on MongoDB Authentication, see: • *MongoDB Authentication section in the CPS Installation Guide for VMware* • *MongoDB Authentication Process section in the CPS Installation Guide for OpenStack*

Memory and Performance Impact

- Logs require a maximum of 1.5 GB (stale-session-audit.log) and 1 GB (stale-session-cleaner.log) disk space.
- The utility JVM process requires 4 GB of additional memory over base pcrfclient VM requirement to run.
- You must configure a minimum and maximum value of -Xms4g and -Xmx8g for JVM memory in `/etc/broadhop/stale-session-cleaner/jvm.conf file`.
- Minimum four additional cores are required for the pcrfclient VM. This number of additional CPU cores depends on the number of shards and TPS per shard.

  For example, in a CPS setup, if there are 88 shards and each shard handles 200 TPS, so a total of 17600 TPS is being processed. Then, it is recommended to add 4 cores.
- Enabling the utility requires additional 15% of CPU usage on each sessionmgr VM.
- The utility requires requires additional 2 GB memory space and 10% of one CPU (pcrfclient) core for memcache.
- Memcache server memory allocation depends on the number of unique keys that are saved in memcache with 200 bytes needed for each such entry. When multiple memcache instances are specified then data is distribured among those and memory requirement for each instances must be calculated based on expected number of records that are saved in that instance. The default and minimum required memory

allocation for each memcache instance is 2 GB. Memory needed by memcache instance is in addition to the memory required for VMs.

Configuration and Restrictions

Note

- It is recommended to set the value for `session.count.threshold` to be greater than total number of active sessions.
- Log rotation for `/var/log/broadhop/stale-session-audit.log or /var/log/broadhop}/stale-session-cleaner.log` is controlled by logback, whereas the service logs are controlled by logrotate. It is similar to qns log and service-qns logs.

Starting and Stopping the Service

- Execute the following command in the pcrfclient where the application is running (and arbitervip is present) to stop the application:

  ```
  monit stop stale-session-cleaner-helper
  ```

- Execute the following command in the pcrfclient where the application (and arbitervip is present) is not running to restart the application:

  ```
  monit restart stale-session-cleaner-helper
  ```

Diameter Stack Configuration

This section allows for the creation of the stacks that handle the diameter traffic. Depending on your particular requirements one or more stacks can be created.

At System Level

In order to define a Diameter stack at system level you need to perform the following steps:

1. Login into Policy Builder.
2. Select **Reference Data** tab.
3. From the left pane, select **Systems**.
4. Select and expand your *system name*.
5. Select and expand **Plugin Configurations**.
6. Select **Diameter Configuration**.
7. From the right pane, click **Diameter Stack** under **Create Child**.

At Cluster Level

In order to define a Diameter stack at cluster level you need to perform the following steps:

1. Login into Policy Builder.
2. Select **Reference Data** tab.
3. From the left pane, select **Systems**.
4. Select and expand your *system name*.
5. Select and expand your *cluster name*.
6. Select and expand **Plugin Configurations**.
7. Select **Diameter Configuration**.
8. From the right pane, click **Diameter Stack** under **Create Child**.

The following parameters can be configured under Diameter Stack:

Table 39: Diameter Stack Parameters

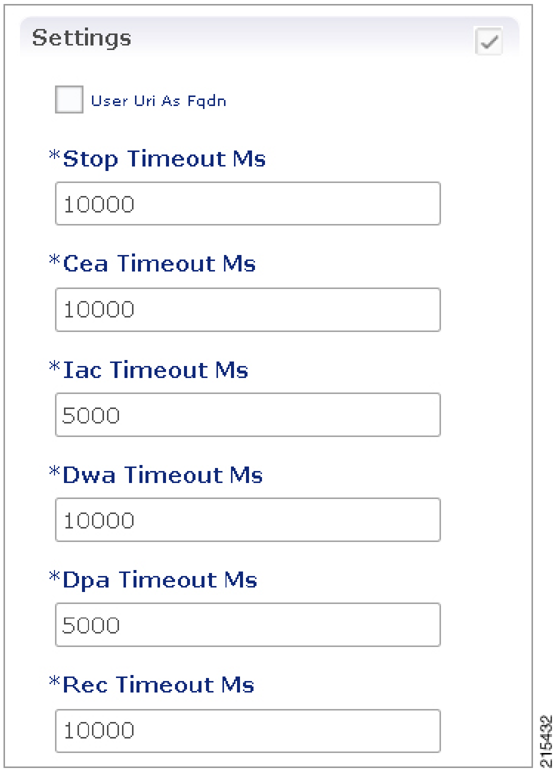
Parameter	Description
Name	Local stack name. This is only used within the Policy Builder GUI to identify the diameter stack.
Realm	Local realm for the diameter stack. This value is going to set as Origin-Realm AVP value in all the diameter messages originated from this stack. For example, volte.pcrf.cisco.com
Accept Undefined Peer	This allows for any incoming diameter peer connection request to be accepted by the stack provided the peer realm is provisioned under inbound realms. For more details on Inbound Peers check Inbound Peers, on page 112. Default value is checked. **Note** If this is unchecked, then the Inbound Peers and Outbound Peers table must be defined. Note that using this option opens a security hole into the system. Therefore, Cisco does not recommend using this option (uncheck the flag) in production environments.
Local End Points	This configures other stack parameters.
Local Host Name	The host local name where this stack is going to be created. **Note** If Local Host Name value does not map to a valid IP the stack binds to localhost (127.0.0.1).
Instance Number	Indicates the Instance number of the Policy Server process on Policy Director for which this entry applies. On a Policy Director each Policy Server process is assigned an Instance Number.

Parameter	Description
Advertised Diameter FQDN	This value is going to be set as Origin-Host AVP value in all the diameter messages originated from this stack. The Advertised Diameter FQDN value needs to map to a valid IP address because that IP address is going to be set as Host-IP-Address AVP value in CER/CEA. As per RFC 3588 Host-IP-Address is a mandatory AVP in CER/CEA.
Listening Port	The port the stack is listening to on the host identified by Local Host Name attribute. Default value is 3868.
Local Bind Ip	Allows the stack to bind to a different IP than the one that Local Host Name value maps to. When provisioned Local Bind Ip value overrides the Local Host Name value.
Transport Protocol	Allows you to select either 'TCP' or 'SCTP' for the selected diameter endpoint. Default value is TCP.
Multi Homing Hosts	This is a comma separated list of IP addresses that CPS uses to start the diameter stack with multi-homing enabled for SCTP transport. Diameter stack with TCP transport still uses the existing 'Local Bind Ip' field to specify any specific IP address for TCP stack. CPS uses the 'Local Bind Ip' to bring up SCTP stack and use it along with the ‘Multi Homing Hosts' to start the SCTP transport with multi-homing support. **Note** While using SCTP multi-homing functionality review the Linux network and gateway configurations for supporting multiple networks on different subnets. CPS supports Centos 6 release and reverse path filtering kernel parameter (rp_filter) values can be set for allowing packets from different subnets on Policy Director VMs. The default behavior in Centos 6 is to discard the packets in such scenarios.

Settings

You can provision different timers that are available at the diameter stack level.

Figure 42: Settings



Settings ✓

□ User Uri As Fqdn

*Stop Timeout Ms: 10000

*Cea Timeout Ms: 10000

*Iac Timeout Ms: 5000

*Dwa Timeout Ms: 10000

*Dpa Timeout Ms: 5000

*Rec Timeout Ms: 10000

The following parameters can be configured under Settings:

Table 40: Settings Parameters

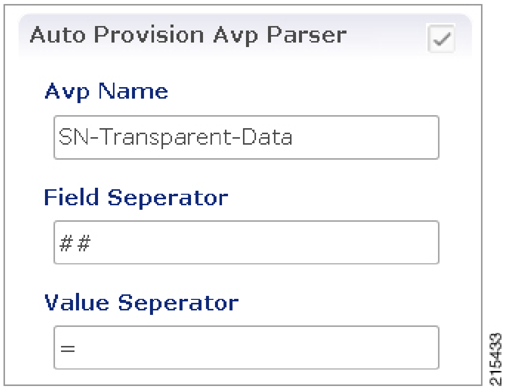
Parameter	Description
User Uri As Fqdn	Sets the Origin-Host AVP value in CER/CEA to the user URI value instead of FQDn value. Default value is not set.
Stop Timeout Ms	Sets the timeout duration for a stack to wait till all the resources stop. The delay is in milliseconds. Default value is 10000.
Cea Timeout Ms	Sets the CER or CEA exchange timeout duration in case of no response. The delay is in milliseconds. Default value is 10000.
Iac Timeout Ms	Sets the timeout duration for a waiting stack before retrying the communication with a peer that has stopped answering DWR messages. The delay is in milliseconds. Default value is 5000.

Parameter	Description
Dwa Timeout Ms	Sets the DWR or DWA exchange timeout duration in case of no response. The delay is in milliseconds. Default value is 10000.
Dpa Timeout Ms	Sets the DPR or DPA exchange timeout duration in case of no response. The delay is in milliseconds. Default value is 5000.
Rec Timeout Ms	Sets the timeout duration for reconnection procedure. The delay is in milliseconds. Default value is 10000.

Auto Provision Avp Parser

This section allows for provisioning of the necessary information needed to parse the Cisco vendor specific SN-Transparent-Data AVP value.

Figure 43: Auto Provision Avp Parser



Auto Provision Avp Parser ☑

Avp Name

SN-Transparent-Data

Field Seperator

##

Value Seperator

=

The following parameters can be configured under Auto Provision Avp Parser:

Table 41: Auto Provision Avp Parser

Parameter	Description
AVP Name	The AVP name whose value needs to be parsed using the field separator and value separator. For example “abcd=xyz##lmno=pqrst”
Field Separator	String value used as a token to split pairs of attribute and values. In the above example # is the field separator.
Value Separator	String value used as a token to split pairs of attribute and values. In the above example = is the value separator.

Inbound Peers

This section allows for the provisioning of the diameter peers that are allowed to initiate connections towards PCRF. The PCRF does not initiate diameter connections with these peers.

Peer name and peer realm are independently checked against the two tables.

The following parameters can be configured under Inbound Peers:

Table 42: Inbound Peers Parameters

Parameter	Description
Peers	Defines which peer names are allowed to initiate connections towards PCRF.
Local Host Name	Identifies the local host name of the Policy Director (load balancer) that identifies and allows an incoming connection from the Peer.
Instance Number	Indicates the assigned number of the Policy Server (QNS) process that initiates a connection with the Outbound Peer. **Note** Local Host Name and Instance Number should be specified if the intention is for only a single Policy Server (QNS) process on Policy Builder (load balancer) to allow/initiate a connection with the said peer else Instance number can be kept as “0”. In which case all the Policy Server (QNS) processes on Policy Director (load balancer) shall attempt/allow connection with the peer. Default value is 0.
Rating	Priority assigned to this peer for delivering a PCRF initiated request. The higher the rating value the higher is the priority assigned to the peer. Default value is 1.
Port Range	Should be specified only when the underlying transport connection Is SCTP and not required when the same is TCP.
Response Timeout	Cisco recommends not to use this parameter.
Name Pattern	Origin-Host AVP value in CER needs to validate against this pattern in order for the connection to be established. If that does not happen the CER is silently discarded and the TCP connection is reset by PCRF. Name pattern check does not happen if Accept Undefined Peer option described in Diameter Stack Configuration, on page 107 is checked. The Name Pattern needs to follow the standard Java regular expression syntax described here.

Table 43: Inbound Realms Parameters

Parameter	Description
Realms	Defines which peer realms are allowed to initiate connections towards PCRF.

Parameter	Description
Peer Type	Not used with inbound realms.
Processing Protocol	Mapping between the realm name and the specific PCRF logic that should be applied for the message. For more information on processing protocol refer to Table 27: Protocols, on page 85. **Note** When a Diameter Stack with a diameter realm is imported with no protocol assigned, it takes the default value as GX_TGPP.
Rating	Priority assigned to this realm for delivering a PCRF initiated request. This is only used with SY_PRIME processing protocol. Default value is 0. **Note** The lower the rating value, the higher is the priority assigned to the realm. For example, a realm having Rating=10 is used after a realm having Rating=1.
Stats Alias	Whatever the statistics that gets generated for the respective realm gets the name that is configured in “Stats Alias” appended to those statistics. This is applicable for com.broadhop.message mbean statistics only.
Name Pattern	Origin-Realm AVP value in CER needs to validate against this pattern in order for the incoming message to be processed. If that does not happen the message is silently discarded and the TCP connection is reset by PCRF. The Name Pattern needs to follow the standard Java regular expression syntax described here.

Important In **Message Timeout and Retry Configuration**, diameter response timeout is defined using the combination of **Application Id** and **Command Code** parameters.

When PCRF is configured to work with a DRA the actual system's host name does not need to be provisioned in the Peers table for the message to be answered.

When PCRF is configured to work with a DRA the actual system's origin realm name does need to be provisioned in the Peers table for the message to be processed. If it is not provisioned then PCRF shall send an error response containing the Result-Code AVP with value DIAMETER_APPLICATION_UNSUPPORTED (3007).

Outbound Peers

This section allows for the provisioning of the diameter peers to which the PCRF initiates the diameter connections.

Peer name and peer realm are independently checked against the two tables.

The following parameters can be configured under Outbound Peers:

Table 44: Outbound Peers Parameters

Parameter	Description
Peers	Defines the peers to which CPS can initiate connections.
Local Host Name	Identifies the local host name of the Policy Director (load balancer) that initiates a connection with the said Peer.
Instance Number	Indicates the assigned number of the Policy Server (QNS) process that allows an incoming connection from the Peer. Default: 0
Rating	Priority assigned to this peer for delivering a PCRF initiated request. The higher the rating value the higher is the priority assigned to the peer. Default: 1
Port Range	Should be specified only when the underlying transport connection is SCTP and not required when the same is TCP. However in mixed mode where both SCTP and TCP co-exist then it is mandatory to provide port range values for both TCP and SCTP peers in order to avoid any conflicts on using local ports on same host.
Response Timeout	Cisco recommends not to use this parameter.
Name	Peer host name. Peer host name needs to be mapped to a valid IP address or the diameter connection is not initiated. By default the connection is initiated on the standard diameter port (3868). If a different port needs to be used than the peer name shall be defined using the host:port format. Default value is “default”. **Note** We recommend that the peer names (Name) should match the Origin-Host AVP value in the incoming CER/CEA message.
Transport Protocol	Allows you to select either 'TCP' or 'SCTP' for the selected diameter stack instance. Default value is TCP.
Multi Homing Hosts	This is a comma separated IP addresses list that CPS uses to start the client connections towards external diameter peer. If either TCP/SCTP or both TCP and SCTP are configured in the Outbound Peers (Peers) table then client connections to the peers are initiated based on whether the PD instance is started as a ‘SCTP’ or ‘TCP’ stack. Mixed mode of client and stack running on both ‘TCP’ and ‘SCTP’ is not currently supported by diameter. **Note** While using SCTP multi-homing functionality review the Linux network and gateway configurations for supporting multiple networks on different subnets. CPS supports Centos 6 release and reverse path filtering kernel parameter (rp_filter) values can be set for allowing packets from different subnets on Policy Director (load balancer) VMs. The default behavior in Centos 6 is to discard the packets in such scenarios.

Table 45: Outbound Realms Parameters

Parameter	Description
Realms	Defines the realms to which CPS can initiate connections.
Peer Type	This indicates which diameter server to use when there are multiple target servers for the same protocol. This is only used with SY_PRIME processing protocol.
Processing Protocol	Mapping between the realm name and the specific PCRF logic that should be applied for the message. For more information on processing protocol refer to Table 27: Protocols, on page 85.
Rating	Priority assigned to this realm for delivering a PCRF initiated request. This is only used with SY_PRIME processing protocol. Default value is 0. **Note** The lower the rating value, the higher is the priority assigned to the realm. For example, a realm having Rating=10 is used after a realm having Rating=1. **Note** This rating is used only for next hop based routing with SY_PRIME.
Stats Alias	Whatever the statistics that gets generated for the respective realm gets the name that is configured in “Stats Alias” appended to those statistics. This is applicable for com.broadhop.message mbean statistics only.
Name	Origin-Realm AVP value in CER needs to validate against this pattern in order for the incoming message to be processed. If that doesn't happen the message is silently discarded and the TCP connection is reset by PCRF. The Name Pattern needs to follow the standard Java regular expression syntax described here.

Important In **Message Timeout and Retry Configuration**, diameter response timeout is defined using the combination of **Application Id** and **Command Code** parameters.

Note Outbound Realms table is not used when Next Hop Routing table is defined. For more information on next hop routing table, refer to Next Hop Routing, on page 87.

When PCRF is configured to work with a DRA the actual system's host name does not need to be provisioned in the Peers table for the message to be answered.

When PCRF is configured to work with a DRA the actual system's origin realm name does need to be provisioned in the Peers table for the message to be processed. If it is not provisioned than PCRF shall send an error response containing the Result-Code AVP with value DIAMETER_APPLICATION_UNSUPPORTED (3007).

The following restrictions are applicable while configuring CPS for SCTP:

When using SCTP as a transport protocol, CPS selects the 'Multi Homing Hosts' values along with the 'local bind ip' defined in local endpoints. But for TCP transport protocol CPS ignores the 'Multi home hosts' value.

When using SCTP as a transport protocol, CPS selects the 'Multi Homing Hosts' values along with 'Outbound Peers' defined in 'Peers' table. But for TCP transport protocol CPS ignores the 'Multi Homing Hosts' value.

Configuring Port-Range for SCTP outbound peers is mandatory. We also recommend using non-overlapping port ranges across different PDs within same Policy Director (load balancer) node while configuring multiple PDs.

For example:

PD1 (qns-2 process in the Policy Director (load balancer) VM) 12000-12500

PD2 (qns-3 process in the Policy Director (load balancer) VM) 13000-13500

PD3 (qns-4 process in the Policy Director (load balancer) VM) 14000-14500

Diameter Agents

The Diameter Agent in CPS currently supports only the PROXY mode of operation (for more information, see RFC 6733 – Diameter Base Protocol at https://tools.ietf.org/html/rfc6733). In Proxy mode, all relevant messages that are received by the CPS node (based on the applied filter on which the message is to be proxied) are forwarded to the given agent.

Policy Builder currently supports proxy functionality for Gx, Gy, and Rx interfaces. Messages reaching CPS may be proxied to an alternate realm based on the "Application-ID" and/or the "Command-Code" within the incoming message. As part of the Diameter agent's configuration (described in Diameter Agent Configuration, on page 116), the specified realm translates to a destination realm, and a destination node is selected based on outbound peers and priority/rating.

The filter information on which the Application/message needs to be proxied by CPS is provided by configuring a Use Case Template containing the DiameterAgentInfo service configuration (described in DiameterAgentInfo Service Configuration Object Setup, on page 117) as part of the configured service.

Diameter Agent Configuration

A diameter agent is defined with a name and an associated realm, and is then used when configuring the DiameterAgentInfo service configuration object.

Step 1 Log in to Policy Builder.

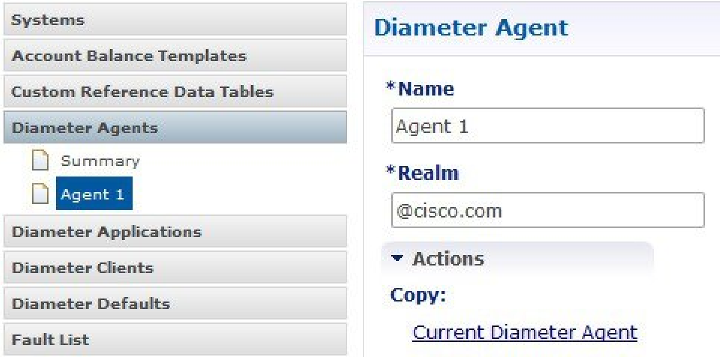
Step 2 Select the **Reference Data** tab.

Step 3 In the left pane, select **Diameter Agents**.

Step 4 In the **Summary** pane, click **Diameter Agent** under **Create Child**.

Step 5 In the **Diameter Agent** pane, type the **Name** and the **Realm** for the agent.

Figure 44: Diameter Agent Configuration



*Name: Agent 1

*Realm: @cisco.com

DiameterAgentInfo Service Configuration Object Setup

This section describes how to configure the DiameterAgentInfo service configuration object.

Step 1 In Policy Builder, select the **Services** tab.

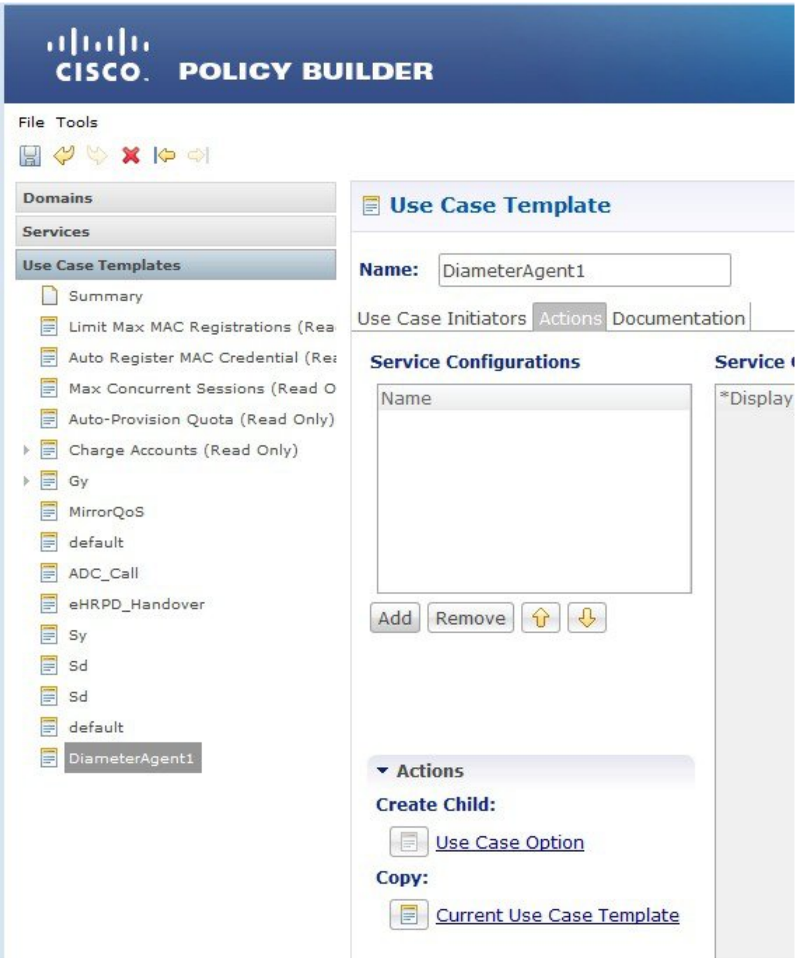
Step 2 In the left pane, select **Use Case Templates**.

Step 3 Select **Summary** and from right side pane, click **Use Case Template** under **Create Child**.

Step 4 In the **Name** field, type a name for the template.

Step 5 select the **Actions** tab, and then click **Add** under **Service Configurations**.

Figure 45: Use Case Template Actions Tab



Step 6 In the **Select Service Configuration** dialog box, scroll down to the proxy section, select **DiameterAgentInfo**, and click **OK**.

Step 7 Configure the DiameterAgentInfo parameters as described in the following table:

Table 46: DiameterAgentInfo Parameters

Parameter	Description
Diameter Agent Name	Click in the **Value** column beside **Diameter Agent Name**, and type the name that you supplied when you configured the Diameter agent.
Diameter Agent Type	**Proxy** is the only agent type that has been implemented.

Parameter	Description
Proxy Protocol	Select one of the following protocols from the drop-down list: • GX_TGPP • GY_V8 • RX_TGPP The other protocols in the list are not currently supported.
Proxy Request A V Ps (List)	In this section, you can define additional AVPs to add to the proxy request. The following parameters can be configured: **Command Code** – **Request Type** – **Code** – Type a code for the AVP. **Value** – Type a value for the AVP. **Type** – Select the AVP type from the drop-down list. **Operation** – Select the Operation from the drop-down list. **Vendor** – Select the AVP Vendor from the drop-down list.
Proxy Response A V Ps (List)	In this section, you can define additional AVPs to add to the proxy response. The following parameters can be configured: **Command Code** – **Request Type** – **Code** – Type a code for the AVP. **Value** – Type a value for the AVP. **Type** – Select the AVP type from the drop-down list. **Operation** – Select the Operation from the drop-down list. **Vendor** – Select the AVP Vendor from the drop-down list.

Diameter Clients

The Diameter Clients section allows for the creation of different clients identified by their realm. The clients defined in this section can be further used while configuring a policy so that different clients get different service configuration objects.

In order to define a Diameter Client you need to perform the following steps:

1. Login into Policy Builder.
2. Select **Reference Data** tab.

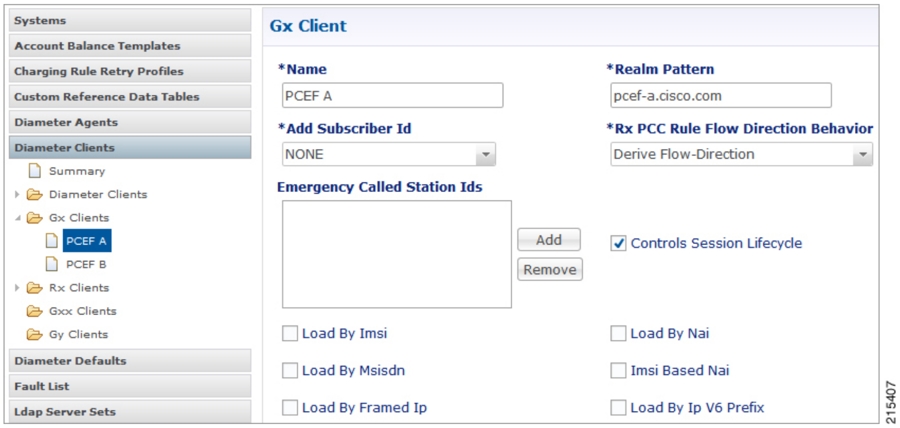
3. From the left pane, select **Diameter Clients**.

4. Select **Summary**.

5. Create the specific client that corresponds to your interface. If there is no specific client for your interface select the generic Diameter Clients.

6. Provide values for at least the mandatory attributes.

Figure 46: Gx Client



Gx Client

*Name: PCEF A

*Realm Pattern: pcef-a.cisco.com

*Add Subscriber Id: NONE

*Rx PCC Rule Flow Direction Behavior: Derive Flow-Direction

Emergency Called Station Ids

☑ Controls Session Lifecycle

□ Load By Imsi

□ Load By Nai

□ Load By Msisdn

□ Imsi Based Nai

□ Load By Framed Ip

□ Load By Ip V6 Prefix

Note The mandatory fields are marked with a “*” on the upper left corner of the field name label.

Once you have done that you can use the diameter client to filter the service objects that are going to be used in a policy.

More details about each client field and attribute will be provided in the following sections dedicated to each type of client.

In order to filter a Service Option based on the Diameter Client you need to perform the following steps:

1. Login into Policy Builder.

2. Select **Services** tab

3. From the left pane, select **Services**.

4. Expand Service Options tree.

5. Select and expand your service option.

6. Select the service option object.

7. Select the Value cell corresponding to the Diameter Client Display Name.

8. Click the “…” button.

9. Select the Diameter Client from the popup window.

10. Click **OK**.

For more details about how to define a service option refer to Services, on page 229.

Note If your service configuration object does not have a Diameter Client attribute it means it is not diameter related and it cannot be filtered out based on diameter client.

Currently, the following diameter client types are supported:

- Diameter Clients
- Gx Clients
- Rx Clients
- Gy Clients

Note The diameter client feature is mainly for use with inbound realms. No validation is done as to whether a realm is unique for a specific client type. If multiple clients are defined for the same realm the behavior may be unpredictable. The interface specific diameter clients are built on top of the generic Diameter Clients. They add specific behavior and this is why they should always be used in the context of the specific interface.

Diameter Clients

This generic diameter client object is supposed to be used for any interface that does not have a matching specific diameter client.

The following parameters can be configured under generic Diameter Client:

Table 47: Diameter Client Parameters

Parameter	Description
Name	The client name that is going to be used to reference this particular client in the service configuration object.
Realm Pattern	The pattern that peer realm name should match in order for this diameter client to be used. The pattern needs to follow the standard Java regular expression syntax described here. The first choice for Realm Pattern value should always be the exact peer realm name whenever possible.
Extract Avps	See Extract Avps, on page 135
Override Supported Features	Currently, not supported. **Note** This table is only supported for Gx and Rx client.

Parameter	Description
Copy Current Diameter Client	This action creates a new diameter client that is an exact copy of the current diameter client. The only difference between the original and the copy is that "-Copy" is appended to the name of the copy. The Copy action works exactly the same for all types of diameter clients.

Gx Clients

This specific diameter client object is supposed to be used only in relation with the Gx interface. It adds Gx specific features to the generic diameter client already described in Diameter Clients, on page 121.

Basic Options

The following parameters can be configured for Basic Options under Gx Client:

Table 48: Gx Client Parameters - Basic Options

Parameter	Description
Add Subscriber Id	Adds Subscription-Id grouped AVP in Gx CCA-i message with one of the following Subscription-Id-Type AVP value and Subscription-Id-Data AVP value depending on the selection. The values will be copied from the incoming Gx CCR-i message if available. • NONE (default): No Subscription-Id grouped AVP in Gx CCA • IMSI: END_USER_IMSI (1) • MSISDN: END_USER_E164 (0) • NAI: END_USER_NAI (3)
Rx PCC Rule Flow Direction Behavior	Controls how the Flow-Direction AVP value under Flow-Information grouped AVP is derived. This option is only used for Rx dedicated bearers. • Derive Flow-Direction: Flow-Direction AVP is derived based on Flow-Description AVP value and Flow-Status AVP value. This option is used only in case the PCEF advertised support for Rel10 feature under Supported-Features AVP. For more information refer to Table 49: Flow-Direction AVP Values, on page 126. • 3GPP Gx Rel11 Compliant: Flow-Direction AVP is derived as per 3GPP TS 29.212 v11 • Exclude Flow-Direction (default): Flow-Direction AVP is not set.
Sending Delayed Message Wait Time Ms	This parameter specifies the amount of time the Gx RAR is delayed after Gx CCA is sent when "Gx Triggered Session-Release-Cause in RAR" is enabled. Default value is 500 milliseconds.

Parameter	Description
Max Num of Dynamic Rule Supported	This parameter specifies the maximum number of dynamic rules supported per Gx session. Default value is 100. Allowed value > 10
Max Number of PRA Identifiers Supported	This parameter indicates the maximum number of PRA identifiers CPS supports. When PresenceReportingAreaConfiguration service configuration is configured with number of PRA Identifiers more than the this value, the PRA Identifiers configured beyond this value are ignored. Default value is 8.
Emergency Called Station Ids	The list of APNs that are allowed to initiate IMS emergency calls as per procedures described in 3GPP TS 29.212.
Controls Session Lifecycle	Decides whether all the other sessions bound to the current Gx session get terminated upon Gx session termination. Default value is checked.
Load By Imsi	If checked, attempts to load the session by IMSI (Subscription-Id-Data AVP value under Subscription-Id grouped AVP where Subscription-Id-Type AVP value is END_USER_IMSI (1)). Default value is unchecked.
Load By Nai	If checked, attempts to load the session by NAI (Subscription-Id-Data AVP value under Subscription-Id grouped AVP where Subscription-Id-Type AVP value is END_USER_NAI (3)). Default value is unchecked.
Load By Msisdn	If checked, attempts to load the session by MSISDN (Subscription-Id-Data AVP value under Subscription-Id grouped AVP where Subscription-Id-Type AVP value is END_USER_E164 (0)). Default value is unchecked.
Imsi Based Nai	If checked, the subscriber is identified by PCRF using “IMSI based NAI”, where the identity is represented in NAI form as specified in RFC 4282 [5], and formatted as defined in 3GPP TS 23.003 [6], clause 19.3.2. The IMSI based NAI is sent within the Subscription-Id AVP with the Subscription-Id-Type set to END_USER_NAI at IP-CAN session establishment. Default value is unchecked.
Load By Framed Ip	If checked, attempts to load the session by IPv4 address (Framed-IP-Address AVP value). Default value is unchecked.

Parameter	Description
Load By Ip V6 Prefix	If checked, attempts to load the session by IPv6 address (Framed-IPv6-Prefix AVp value). Default value is unchecked.
Session Chained	If checked, it does not attempt to terminate the Gx session by sending a Gx RAR to PCEF. Default value is unchecked.
Remove Realm In User Id Mapping	If checked, removes the realm from the NAI (if present) before attempting to load the session by username. For more details on NAI see RFC 2486. Default value is unchecked.
Exclude Sponsor Identity Avp	If checked, it does not add the Sponsor-Identity AVP to the Charging-Rule-Definition grouped AVP. This option is used only in case the PCEF advertised support for SponsoredConnectivity feature under Supported-Features AVP. Default value is unchecked.
Load By Called Station Id	If checked, attempts to load the session by IMSI and APN. In order for this option to be effectively used 'Load By Imsi' option (described above) needs to be checked. Default value is unchecked.
Re-install Rule on Monitoring Key Change	If checked, attempts to reinstall a charging rule in case the only AVP value that changed for a PreConfiguredRule is the monitoring key value.
Limit with Requested QoS on modification failure	If checked, authorizes bound QoS between retained and calculated QoS after CPS has received QoS modification failure event from PCEF. Default value is checked.
Enforce Missing Avp Check	The default value of this new attribute is TRUE (checked); that is, CPS will perform missing Enforce Missing AVP Check, on page 127 validations and send DIAMETER_MISSING_AVP (5005) result in the answer message. However, if this attribute is FALSE (unchecked), CPS will not perform the missing AVP validation.

Parameter	Description
One Gx Rule Per Flow	This parameter applies only to the dynamic charging rules over Gx that are generated by CPS due to the APPLICATION_START event trigger received over the Sd interface for ADC rules. If checked, CPS creates one dynamic charging rule over Gx per flow information received in the Application-Detection-Info AVP over the Sd interface. CPS also creates a unique TDF-Application-Identifier over Gx for each of these rules. So, each generated rule has a unique TDF-Application-Identifier and only one Flow-Information AVP. If unchecked, CPS generates only one rule per TDF-Application-Identifier received over the Sd interface. This one rule has all the Flow-Information AVPs. The TDF-Application-Identifier over Gx is same as over Sd. By default, the check box is unchecked.
Selective Muting	If checked, CPS selectively mutes the flow corresponding to a TDF-Application-Identifier on the dedicated bearer after it receives the first Application_Start event trigger on the dedicated bearer from PCEF. For default bearer, CPS selectively mutes the flow corresponding to a TDF-Application-Identifier after it receives the Application_Start event trigger on the default bearer from PCEF and maximum limit is reached on the dedicated bearer. **Note** Limit on number of flows on a given dedicated bearer is based on a unique combination of QCI and ARP Priority Level. This value is configurable in Policy Builder. After CPS receives Application_Stop event trigger from PCEF for a specific TDF-Application-Identifier (with TDF-App-Instance-ID=0), CPS removes that rule from the dedicated bearer and installs the rule on the default bearer and unmutes all the rules related to that Sd TDF-Application-Identifier on the default bearer. **Note** PCEF sends the TDF-App-Instance-ID as 0 only after all applications related to a TDF-Application-Identifier are stopped.
Re-Install Predefined Rules on Rulebase Change	Indicates whether all the existing predefined rules that are applicable for the session are re-installed if there is a Rule-Base change. Select this option if you want all the predefined rules (that are applicable to the session) to be re-installed if the Rule-Base changes due to any reason. If unchecked, whenever there is a Rule-Base change, CPS only notifies the changes (if any) in predefined rules to PCEF and does not re-install all the existing predefined rules. **Note** The rules that are not applicable are removed. This option does not apply to preconfigured or dynamic rules from Rx/Sd. **Restriction** Use this checkbox only in consultation with Cisco Technical Representative.

Parameter	Description
Gx triggered Session-Release-Cause in RAR	If checked (enabled), any Gx initiated session termination is responded to with a RAR immediately after CCR/CCA exchange with the PCEF. The RAR contains the Session-Release-Cause AVP. If unchecked (disabled), any Gx initiated session termination response from the PCRF in the CCA-U contains the Session-Release-Cause AVP. This is the default behavior. **Note** When the Gx RAR option is enabled, it is sent after the number of milliseconds specified under "Sending Delayed Message Wait Time Ms" field.
Enhanced Logic for Preconfigure Rule Redirection Support	If checked, Redirect-Support as disabled is only sent when enable was sent previously. By default, the check box is unchecked.
Enhanced Gx-RAR Behavior	If checked (enabled), the desired behavior is exhibited for call flows. By default, the check box is unchecked for backward compatibility.
Save Session State	If checked (enabled), Gx session state is restored following a failed Gx RAA (Result-Code AVP value not equal to DIAMETER_SUCCESS (2001)) to the state it was before the Gx RAR was sent. The behavior is same for both sync and async Gx RAR. By default, the check box is unchecked to for backward compatibility.
Ignore IPME Rule On Handover	Indicates whether to use IPME rules during handover or not. If checked, CPS does not consider the IPME rules during handover. If unchecked, CPS considers IPME rules during handover. By default, the check box is selected.

Table 49: Flow-Direction AVP Values

Priority	Criteria	Flow-Direction AVP Values
1	Flow-Description AVP value contains “permit in”	UPLINK (2)
2	Flow-Description AVP value contains “permit out”	DOWNLINK (1)
3	FlowStatus AVP value is ENABLED (2)	BIDIRECTIONAL (3)
4	FlowStatus AVP value is ENABLED_UPLINK (0)	UPLINK (2)
5	FlowStatus AVP value is ENABLED_DOWNLINK (1)	DOWNLINK (1)

Enforce Missing AVP Check

The following is the list of AVPs for which CPS performs the missing AVP validation if **Enforce Missing Avp Check** check box is selected:

- Mandatory AVPs: Origin-Host, Destination-Realm, CC-Request-Type, CC-Request-Number
- Conditional AVPs for session establishment: Subscription-Id (Subscription-Id-Type, Subscription-Id-Data), IP-CAN-Type, RAT-Type , Framed-IP-Address OR Framed-IPv6-Prefix (one must be present), AN-GW-Address (If IP-CAN-TYPE = '3GPP-EPS' or '3GPP2')
- Conditional AVPs for session modification: These AVPs are required based on the event trigger type.
    - SGSN_CHANGE Event Trigger: 3GPP-SGSN-Address or 3GPP-SGSN-IPv6-Address

      Applicable only to 3GPP-GPRS access types and 3GPP-EPS access types with access to the P-GW using Gn/Gp.
    - QOS_CHANGE Event Trigger: Bearer-Identifier, QoS-Information

      When IP-CAN-Type is 3GPP-GPRS and if the PCRF performs bearer binding, the Bearer-Identifier AVP shall be provided to indicate the affected bearer. QoS-Information AVP is required to be provided in the same request with the new value.
    - RAT_CHANGE Event Trigger: RAT-Type

      The new RAT type must be provided in the RAT-Type AVP.
    - PLMN_CHANGE Event Trigger: 3GPP-SGSN-MCC-MNC
    - IP_CAN_CHANGE Event Trigger: IP-CAN-Type

      The RAT-Type AVP must also be provided when applicable to the specific IP-CAN Type (for example, 3GPP IP-CAN Type).
    - RAI_CHANGE Event Trigger: RAI

      Applicable only to 3GPP-GPRS and 3GPP-EPS access types.
    - USER_LOCATION_CHANGE Event Trigger: 3GPP-User-Location-Info

      Applicable only to 3GPP-GPRS and 3GPP-EPS access types.
    - USER_LOCATION_CHANGE Event Trigger: 3GPP2-BSID

      Applicable only to 3GPP2 access types.
    - OUT_OF_CREDIT Event Trigger: Charging-Rule-Report, Final-Unit-Action
    - REALLOCATION_OF_CREDIT Event Trigger: Charging-Rule-Report
    - AN_GW_CHANGE Event Trigger: AN-GW-Address
    - UE_TIME_ZONE_CHANGE Event Trigger: 3GPP-MS-TimeZone
    - LOSS_OF_BEARER, RECOVERY_OF_BEARER, SUCCESSFUL_RESOURCE_ALLOCATION: Charging-Rule-Report
    - DEFAULT _EPS_BEARER_QOS_CHANGE: Default-EPS-Bearer-QoS
    - ECGI_CHANGE or TAI_CHANGE Event Trigger: 3GPP-User-Location-Info
    - ACCESS_NETWORK_INFO_REPORT Event Trigger:

3GPP-User-Location-Info, if Required-Access-Info = USER_LOCATION

3GPP-MS-Timezone, if Required-Access-Info = MS_TIMEZONE

- APPLICATION_START or APPLICATION_STOP Event Trigger over Gx: TDF-Application-Identifier

Advanced Options

Default Flow Description

The **Default Flow Description** field helps in configuring the flow description AVP value corresponding to charging rule over Gx Message, when Media-Sub-Component AVP contains the Flow-Number AVP set to "0", and the rest of AVPs within the Media-Component-Description and Media-Sub-Component AVPs are not used.

By default, this field is disabled or unchecked. The corresponding Flow Description AVP value is set to charging rule **permit in ip from any * to any *** for inbound and **permit out ip from any * to any *** for outbound.

Select the **Default Flow Description** check box to configure the parameters.

Table 50: Default Flow Description Parameters

Parameter	Description
Is Inbound?	This is a check box field. This parameter denotes whether Flow Description configuration defined is for Inbound or Outbound call. Default value is checked.
Source IP	This parameter denotes the Source IP of the Flow-Description AVP received in the message. Default value is any.
Source Port	This parameter denotes the Source Port of the Flow-Description AVP received in the message. Default value is *.
Destination IP	This parameter denotes the Destination IP of the Flow-Description AVP received in the message. Default value is any.
Destination Port	This parameter denotes the Destination Port of the Flow-Description AVP received in the message. Default value is *.

Cisco Pending Transaction Retry

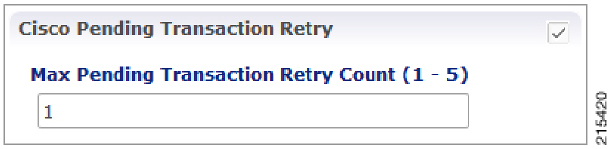
StarOS 16 introduces optional custom behavior for handling overlapping Gx transactions so that the potential race conditions that can occur on Gx interface are to be handled deterministically.

This feature introduces a new error indication to allow the transaction originator to determine if a re-attempt of the transaction is appropriate. The PCRF shall send an error response to the PCEF containing the Experimental-Result-Code AVP with Cisco specific value DIAMETER_PENDING_TRANSACTION (4198) if the PCRF expects a response to a pending request that it initiated. The PCRF shall also have the ability to retry the request message for which it received an error response containing the Experimental-Result-Code AVP with Cisco specific value DIAMETER_PENDING_TRANSACTION (4198).

Refer to the CISCO StarOS 16 and CISCO ASR5500 documentation for more details.

Default value (if enabled) is 1.

Figure 47: Cisco Pending Transaction Retry



Cisco Pending Transaction Retry ☑

Max Pending Transaction Retry Count (1 - 5)

1

Max Pending Transaction Retry Count does not include the initial request. For example, in the above case the system will send a initial message and if it fails, it will send the same message 1 more time (retry).

Note PCRF will cache and retry only one message per Gx session. If due to Rx IMS session interaction multiple Gx RAR messages are being evaluated while another Gx RAR message is already pending than PCRF will not reply on the Rx IMS session.

Sponsored Profile

The default monitoring key name format used to track the usage when the AF provides sponsored data connectivity to the subscriber is:

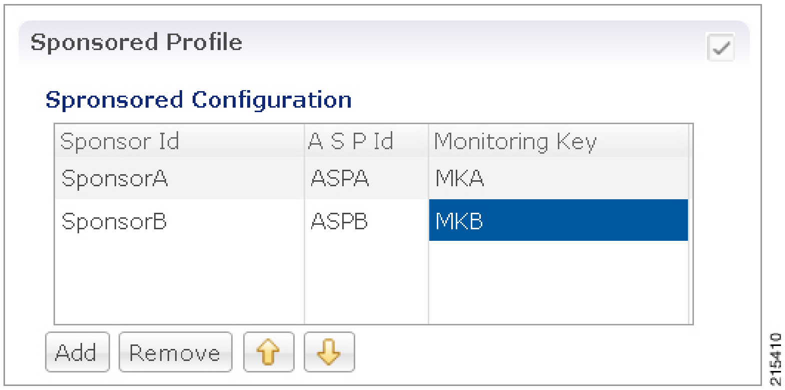
<Sponsor-Id>< Rx-Session-No>

where:

- <Sponsor-Id>: Sponsor-Identity AVP value under the Sponsored-Connectivity-Data grouped AVP.
- <Rx-Session-No>: Counts how many Rx sessions have bound so far to the Gx session by the time the current Rx session is created. This is an attribute of the Rx session stored on PCRF side and it doesn't change during the Rx session lifetime. The value starts from zero and it increases with one for each new Rx session that binds.

This feature allows for customization of the monitoring key name. The monitoring key name matching the Sponsor-Identity AVP value and Application-Service-Provider-Identity AVP value will be used instead of the default one.

Figure 48: Sponsored Profile



Sponsored Profile ☑

Spronsored Configuration

Sponsor Id	A S P Id	Monitoring Key
SponsorA	ASPA	MKA
SponsorB	ASPB	MKB

This option is used only in case the PCEF advertised support for SponsoredConnectivity feature under Supported-Features AVP.

Rx Based QoS Upgrade of Default Bearer

- **Override Boost with Throttle for Similar Priority:** This provides an option to over-ride Throttle with Boost for same priority values received in Dynamic-PCC-Request-QoS.

Restriction

- This feature is applicable for QoS uplift on Default Bearer only.
- This feature overrides the earlier implementation of QoS uplift done in CPS 7.0.5 and earlier versions.

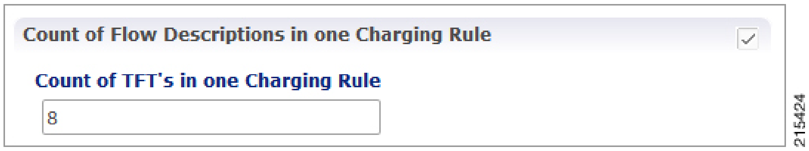
- **Atomic Update of QCI and ARP:** This check box has been added to support QCI and ARP atomicity. When checked, on receiving boost request, ARP gets modified only when QCI is modified.

Count of Flow Description in one Charging Rule

CPS now supports the ability to split Flow Information received from the Traffic Detection Function (TDF) in a CCR-Update across multiple Charging Rules and sent over the Gx interface.

This release provides the ability for CPS to distribute the TFTs across multiple CRNs. The distribution of TFTs keeps the Uplink and Downlink flows together in the same CRN. The number of TFTs per CRN is configurable. By default, CPS is configured to allow 8 TFTs per CRN.

Figure 49: Count of Flow



Count of Flow Descriptions in one Charging Rule ☑

Count of TFT's in one Charging Rule

8

The following parameter can be configured:

Table 51: Count of Flow Descriptions in one Charging Rule Parameters

Parameter	Description
Count of TFT’s in one Charging Rule	One TFT is equivalent to or denotes one Flow-Description AVP received in the message.

Max Number of Flow Descriptions on a bearer (per QCI)

Here, you can set the maximum number of flows that can be configured on the default and dedicated bearer (per QCI).

The following parameters can be configured:

Note These parameters apply only to the dynamic charging rules over Gx that are generated by CPS due to the APPLICATION_START event trigger received over the Sd interface for ADC rules.

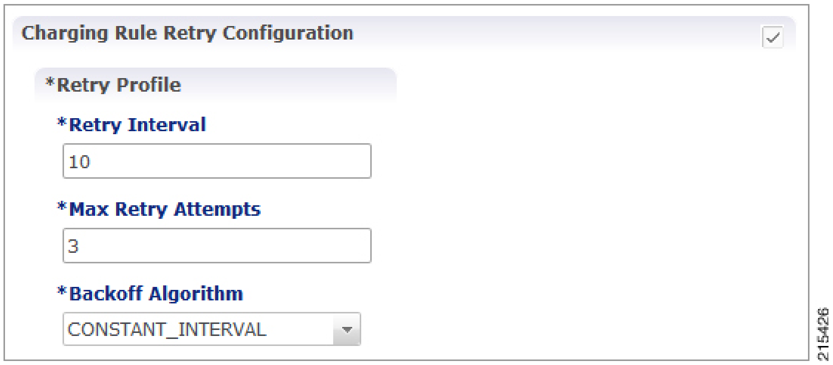
Table 52: Max Number of Flow Descriptions on a bearer (per QCI) Parameters

Parameter	Description
Max Number of Flow Descriptions on a default bearer (per QCI)	This parameter defines the maximum number of flows that can be installed on a default bearer per QCI. So, on receiving the APPLICATION_START event trigger over the Sd interface, CPS installs the corresponding flows over the Gx interface and QCI maps to that of the default bearer. Essentially, this is the limit of flows per QCI that CPS can accept from TDF over the Sd interface. Once this limit is reached, CPS ignores any more flows received from TDF, that is, CPS does not install any rules for those flows. Default value is 64.
Max Number of Flow Descriptions on a dedicated bearer (per QCI)	On receiving the APPLICATION_START event trigger from PCEF, CPS removes the default bearer rule and installs the dedicated bearer rule for the received Gx TDF-Application-Identifier. So, QCI for the new rule maps to a dedicated bearer. This parameter defines the the maximum number of flows per QCI that can be installed on a dedicated bearer. Once this limit is reached, CPS ignores the APPLICATION_START event trigger received over the Gx interface and there is no rule or flow installed on the dedicated bearer. Default value is 16.

Charging Rule Retry Configuration

Upon failure of installation of any/all of the TFTs across one or both CRNs, a configurable retry timer is activated with a configurable number of retries for the TFTs marked as “INACTIVE”. The number of retries and the timer interval between each retry is configurable.

Figure 50: Charging Rule Retry Configuration



Charging Rule Retry Configuration

*Retry Profile

*Retry Interval
10

*Max Retry Attempts
3

*Backoff Algorithm
CONSTANT_INTERVAL

The following parameters can be configured under Charging Rule Retry:

Table 53: Charging Rule Retry Parameters

Parameter	Description
Retry Interval	The delay between retry attempts. The default interval is 10 seconds. Also, by default, the value is capped at 15 secs (configurable). If value is less that 15 seconds, then the retries will be scheduled at second level granularity. If value is greater than 15 seconds, then granularity is of 1 minute (overdue retry events are checked every minute rather than each second).
Max Retry Attempts	The maximum times retry is attempted for a rule. Default value is 3 attempts.
Backoff Algorithm	The back-off algorithm used while determining the actual delay between retry attempts. Currently only one option is supported: Constant Interval: Causes the configured retry interval to be used (without any change) for delay for all retry attempts (other options like exponential back-off where retry interval increases exponentially are currently not supported/implemented).

Upon failure to install TFTs even after retry, all remaining flows are removed (if there were any successfully installed)followed by termination of the Sd Session. After a refresh, CPS attempts to re-establish the Sd-Session. CPS also marks the failed flows as INACTIVE.

Redirect Requests

CPS can reject incoming CCR-I messages with DIAMETER_REDIRECT_INDICATION (3006) error by acting as a redirect agent (RFC 3588). This decision to redirect a request is configured using an STG or CRD. CPS expects the STG or CRD to include a **Redirect Request Column** (of type **True** or **False**). There is no restriction on the condition that determines the redirect behavior.

The following parameters can be configured under Redirect Requests:

Table 54: Redirect Requests Parameters

Parameter	Description
Redirect Request Column	The result column (True/False) from the CRD used to determine if the session needs to be redirected. If result column specified here evaluates to True, session is redirected, else it continues as usual.
Redirect Host	The list of Redirect-Host AVP values to be included in the response. If there are more than one hosts listed, all the hosts are included in the response.
Redirect Max Cache Time (in seconds)	The Redirect-Max-Cache-Time AVP value (in seconds) to be included in the response.
Redirect Host Usage	The Redirect-Host-Usage AVP value (in seconds) to be included in the response. Redirect-Host-Usage AVP supports the following values: • DONT_CACHE: The host specified in the Redirect-Host AVP should not be cached. This is the default value. • ALL_SESSION: All messages within the same session, as defined by the same value of the Session-ID AVP may be sent to the host specified in the Redirect-Host AVP. That is, there is no need to consult the redirect agent for all the messages associated in the session. Identity received is stored until the session terminates. • ALL_REALM: All messages destined for the realm requested may be sent to the host specified in the Redirect-Host AVP. • REALM_AND_APPLICATION: All messages for the application requested to the realm specified may be sent to the host specified in the Redirect-Host AVP. • ALL_APPLICATION: All messages for the application requested may be sent to the host specified in the Redirect-Host AVP. • ALL_HOST: All messages that would be sent to the host that generated the Redirect-Host may be sent to the host specified in the Redirect- Host AVP. • ALL_USER: All messages for the user requested may be sent to the host specified in the Redirect-Host AVP.

Creating an STG to Redirect Requests

You must configure an STG to determine whether an incoming CCR-I needs to be rejected or not. The steps to configure the decision table are as follows:

Note The below procedure is a sample configuration based on APN and Billing plan.

Step 1 Log into Policy Builder.

Step 2 Select the **Reference Data** tab.

Step 3 Click **Custom Reference Data Tables** and select **Search Table Groups**.

Step 4 Under **Actions**, click **Search Table Groups**.

Step 5 Enter a name for the STG.

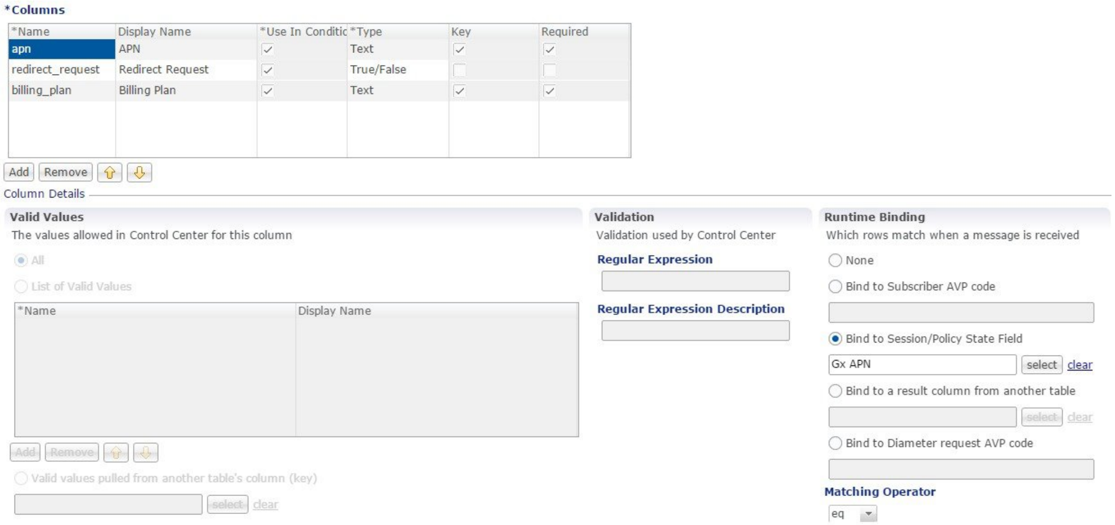
Step 6 Under **Result Columns**, click **Add** and enter a **Name**, **Display Name**, and select the check box under **Use In Condition**.

Step 7 Click **Custom Reference Data Table** under **Actions** > **Create Child**.

Step 8 Enter a **Name** and **Display Name** for the CRD Table.

Step 9 Under **Columns**, click **Add** and enter the following parameters as shown in the following figure:

Figure 51: Custom Reference Data Table Parameters



*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
apn	APN	☑	Text	☑	☑
redirect_request	Redirect Request	☑	True/False	□	□
billing_plan	Billing Plan	☑	Text	☑	☑

Column Details

Valid Values
The values allowed in Control Center for this column
● All
○ List of Valid Values

*Name	Display Name

○ Valid values pulled from another table's column (key)

Validation
Validation used by Control Center
Regular Expression:
Regular Expression Description:

Runtime Binding
Which rows match when a message is received
○ None
○ Bind to Subscriber AVP code
● Bind to Session/Policy State Field: Gx APN
○ Bind to a result column from another table
○ Bind to Diameter request AVP code
Matching Operator: eq

For **apn**, make sure you select **Bind to Session/Policy State Field**, click select and select **Gx APN**. Similarly, for **billing_plan**, select **Bind to Subscriber AVP code** and enter the name or code for the AVP that represents the subscriber's billing plan (for example, **billingplan**).

Step 10 Save the PB configuration.

Pending Transaction Retry

When a Gx session is established, the Supported-Features AVP value is checked for Pending Transactions bit in accordance with 3GPP TS 29.212. The AVP value is stored in the Gx session.

This feature is disabled by default. Select the Pending Transaction Retry check box to enable the feature.

Important On enabling this feature, make sure to disable the Cisco Pending Transaction Retry feature.

If the Pending Transaction Retry check box is unchecked (that is, disabled) in Policy Builder, the system defaults to 3GPP handling of race conditions or pending transactions.

The following parameters can be configured under Pending Transaction Retry:

Table 55: Pending Transaction Retry Parameters

Parameter	Description
Back Off Algorithm	• Constant_Interval: The configured retry Interval is used (without any change) for all retry attempts. • Linear_Interval: Retry interval is derived by multiplying the attempt number with the retry interval. This is applicable only when RAR messages are retried due to pending transactions. Default value is Constant_Interval.
RAR Retry Interval (MilliSeconds)	Retry time interval (milliseconds) after which same RAR is retried after receipt of Pending Transactions (4144) Experimental Result code in RAA. Default value is 1000 milliseconds.
Time (MilliSeconds) to hold CCR-U processing	Time interval (milliseconds) during which CCR-U processing is withheld till pending RAA is received from PCEF. Default value is 1000 milliseconds.
Time (MilliSeconds) to wait for CCR-U retry	Time interval (milliseconds) during which CPS should wait for PCEF to initiate a CCR-U retry after sending a RAA with Pending Transactions (4144) Experimental Result code. Default value is 1000 milliseconds.
Max No of additional RAR's to be stored	Number of RARs generated during pending transactions situations that need to be held and retried in sequence. Additional maximum RARs that can be stored is three. If this value is more that three, Policy Builder displays configuration violation error message. Default value is 1. If set to 0, additional RAR's are discarded.

Extract Avps

AVPs that are required for policy decisions are extracted from the diameter message. The AVPs are specified by their path within the diameter message. Additionally, nested AVPs (each level delimited with ".") can also be extracted with or without qualifiers.

Once extracted, the AVPs are then available for use in Initiator conditions or as key AVP in CRD tables for policy decisions. The AVPs are not stored with the session. Thus, if some policy is enabled because of a received message, and if there is a subsequent trigger message that does not contain that AVP, the initiator conditions will fail and the policy is reverted.

If the AVP to be extracted appears multiple times, each of the instance will be extracted and made available as a policy AVP. Initiator conditions can be written for one or more of these instances. Each condition will check all the available instances for evaluation. Thus if there are multiple instances, multiple conditions (if configured) can be true for the same AVP but with different values.

The **Extract Avps** table lists the AVPs that must be extracted from the diameter message.

- **Name**: Enter a logical name for the extracted AVP. This name will be used in Initiator conditions and CRD tables to identify the extracted AVP. This is a mandatory parameter.
- **Avp Path**: Enter the complete AVP path. This is a mandatory parameter.
- **Command Code**: If Command Code is specified, CPS attempts to extract the AVPs from only that command (and skip the rest). This is an optional parameter.

For example:

- Name: Event-Trigger
- Avp Path: Event-Trigger
- Command Code: 272

For the above example, given a CCR with Event-Trigger AVPs, CPS extracts each Event-Trigger AVP instance and adds it to the current policy state.

Override Supported Features

CPS supports override of Supported-Features with configured value (instead of internally calculated value). The override Supported-Features value can be defined in a CRD table. If the value is configured, CPS compares (bitwise AND) the incoming PCEF advertised value with the configured value and uses the result as the negotiated value. This negotiated value is included in the response message.

If the Override functionality is not enabled or table evaluation provided under the Override Supported-Features does not return a result, CPS falls back to the internal Supported-Features calculation.

Note CPS does not validate the configured Feature-List value. If wrong value is configured, CPS still evaluates negotiated features based on this wrong value and can enable features which CPS does not actually support.

The following parameters can be configured:

Table 56: Override Supported Features Parameters

Parameter	Description
Search Table Group	The STG to lookup for determining the configured Supported-Features (for override).
Vendor Id	The Result column from the selected STG that corresponds to Vendor-Id AVP value.

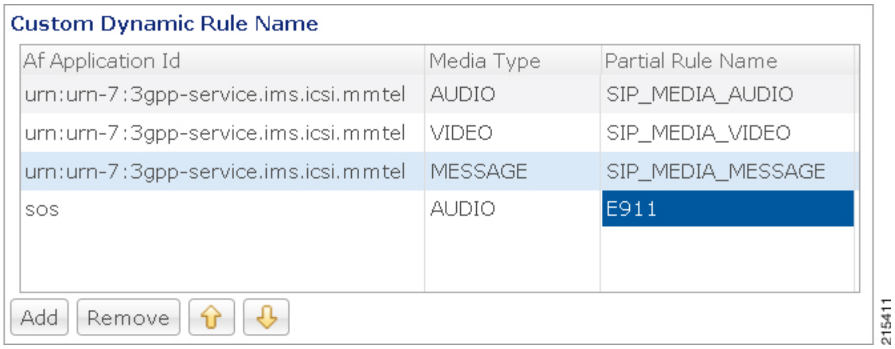
Parameter	Description
Feature List Id	The Result column from the selected STG that corresponds to Feature-List-Id AVP value.
Feature List	The Result column from the selected STG that corresponds to Feature-List AVP value.

Note Multiple entries can be configured, which are evaluated in order.

Custom Dynamic Rule Name

For an Rx call a different Rx dedicated bearer is created for each Media-Sub-Component grouped AVP in the incoming Rx AAR message. This feature allows for customization of the Rx dedicated bearer name based on the AF-Application-Identifier AVP value and Media-Type AVP value received in Rx AAR message.

Figure 52: Custom Dynamic Rule Name



Custom Dynamic Rule Name

Af Application Id	Media Type	Partial Rule Name
urn:urn-7:3gpp-service.ims.icsi.mmtel	AUDIO	SIP_MEDIA_AUDIO
urn:urn-7:3gpp-service.ims.icsi.mmtel	VIDEO	SIP_MEDIA_VIDEO
urn:urn-7:3gpp-service.ims.icsi.mmtel	MESSAGE	SIP_MEDIA_MESSAGE
sos	AUDIO	E911

The default Rx dedicated bearer name format is:
<Rx-Session-No><MCD-No>_<Flow-Number>_<partialRulename>_<Media-Type>

where:

- <Rx-Session-No>: Counts how many Rx sessions have bound so far to the Gx session by the time the current Rx session is created. This is an attribute of the Rx session stored on PCRF side and it doesn't change during the Rx session lifetime. The value starts from zero and it increases with one for each new Rx session that binds.
- <MCD-No>: Media-Component-Number AVP value under Media-Component-Description grouped AVP for the current Media-Sub-Component grouped AVP.
- <Flow-Number>: Flow-Number AVP value for the current Media-Sub-Component grouped AVP.
- <partialRulename>: Partial Rule Name value matching the current Af Application Id and Media Type values for the current Media-Sub-Component grouped AVP or “AF” if no match.
- <Media-Type>: Media-Type AVP value for the current Media-Sub-Component grouped AVP.

Note Only the <partialRulename> part can be customized.

Rx Clients

This specific diameter client object is supposed to be used only in relation with the Rx interface. It adds Rx specific features to the generic diameter client already described in Diameter Clients, on page 119.

The parameters described in the following table can be configured for the Rx client:

Table 57: Rx Client Parameters

Parameters	Description
Session Binding Attribute	Allows the Rx sessions initiated by this client to bind to the Gx session by other attribute than the IP address as per 3GPP TS 29.214. For more information refer to Table 58: Session Binding Attribute Values, on page 144.
Flow Description Source Ip Evaluation	• None: When selected, CPS does not take any action on source IP. • Replace with 'any': When selected, CPS replaces the flow description source IP with ‘any’. • Replace with UE IP: When selected, CPS replaces flow description source IP with UE framed IP.
STA Hold Time Ms	This parameter is used to define the timer by which the STA is held back. Once the timer expires even if the CCR-U is not received, STA is sent to the AF and the rxSession is removed. Default value is 4000 milliseconds.

Parameters	Description
CCR-U Wait Time (in seconds)	CCR-U Timer is the time to wait for CCR-U from PGW when the AF started a request and Specific-Action CUSTOM_DPCC_STATUS_REPORT was armed in AAR. CCR-U timer is started for every request (default bearer boost/spawning of dedicated bearer) from AF if the CCR-U is configured in Policy Builder and CUSTOM_DPCC_STATUS_REPORT(200) is armed in AAR request. There is a separate timer event for different Rx client. This timer is stopped by PCRF when CCR-U is received from P-GW. Also in case when P-GW does not respond to Gx-RAR then CCR-U timer is stopped on receiving internal Gx-RAA (result-code=7000) message. CCR-U timer is helpful in informing AF if the QoS requested through AF is updated on P-GW. In case of default bearer QoS boost/throttle request from AF, there is no notification sent by the P-GW to PCRF. In this case PCRF internally runs this CCR-U time which on expiry sends an update (through Rx_RAR having DPCC-Status AVP) to AF that QoS request is served. There is no default value for this timer. If you want to start CCR-U timer, then you need to configure through Policy Builder. The maximum value is 15 seconds.
Sending Delayed Message Wait Time Ms	This parameter is used to configure wait timer for sending delayed messages. Default value is 500 milliseconds. In case of multiple Media-Component-Descriptions being received in an AAR message by CPS, where one of them is rejected after evaluating for Rx Authorization, CPS sends a successful AAA for the accepted Media-Component-Descriptions and also creates a scheduled event for sending a delayed Rx RAR for rejected Media component. This Rx RAR is sent to AF based on **Sending Delayed Message Wait Time** configured.
Emergency URN List	The list of URNs that are used to indicate that a AF session relates to emergency traffic as per procedures described in 3GPP TS 29.214. For more information refer to Wildcard URN. See Emergency URN List, on page 144.
Override AF App Id with URN for Emergency sessions	When selected, CPS overrides the AF-Application-Identifier AVP value with the Service-URN AVP value for emergency calls. This option is provided in order to overcome the lack of AF-Application-Identifier AVP value in Rx AAR in case of IMS emergency calls. The default setting is unchecked.

Parameters	Description
Validate Flow-Description AVP Value	When selected, CPS validates the Flow-Description AVP values received as part of Media-Sub-Component based on restrictions provided in the 3GPP 29.214 Release 11 specification. If the Flow-Description value does not comply with the format specified then the AAR request is rejected with FILTER_RESTRICTIONS (5062) value in Experimental-Result-Code. When unchecked, CPS does not validate the Flow-Description AVP value and simply forwards it is as is to PCEF as part of generated rules. The default setting is unchecked.
29.213 standard QoS for preliminary service	When checked, CPS supports the QoS handling for Preliminary Service Status. So, on receiving Service-Info-Status AVP as preliminary service information from AF, CPS generates the dynamic PCC rule and assign QCI and ARP values of the default bearer to these PCC rule to avoid signaling to the UE. When unchecked, CPS ignores the Service-Info-Status AVP value and derive the ARP and QCI values as per the QoS derivation algorithm defined in 3GPP TS 29.213 specification. The default setting is unchecked.
NetLoc: Report ANI on rule failure	When checked, CPS always sends the ANI to AF on receiving ANI event from the PCEF. So, in case of bearer release that is either in Rx_RAR (when few rules are impacted) or in Rx_STA when all the rules are impacted, PCRF adds the ANI (access network information) towards AF. When unchecked, CPS does not report ANI to the AF every time the ANI event is received from PCEF. In case of Rx session termination by PCRF that is, when PCRF sends Rx ASR to the AF; PCRF sends the ANI in the Rx STA message even if AF has not asserted the Required-Access-Info AVP for ANI in the Rx STR message. **Note** The checkbox can be used only when NetLoc feature has been negotiated over Gx and Rx and the AF has requested for ANI in the Rx AAR message. The default setting is unchecked.
Hold STA if RAN-NAS-Cause enabled	When RAN-NAS-Cause feature is enabled, CPS sends access network information and RAN-NAS-Release-Cause to AF in STA. So, when this check box is selected, CPS waits for this information from the PCEF and does not send STA till it receives the CCR-U from the PCEF. The default setting is checked (TRUE). **Note** The check box is only applicable when RAN-NAS-Cause feature has been negotiated over Gx and Rx.

Parameters	Description
Auto Increment Precedence Avp	When selected, CPS automatically increments the precedence AVP value by 1 for every Rx charging rule that is installed as part of any Rx session that is using this Rx client within the same Gx session. For example, Gx session (Gx1) has one Rx session (Rx1). When Rx1 is created, two charging rules are installed and they are assigned precedence values 1 and 2. A second Rx session (Rx2) starts for Gx1 and also installs two Rx charging rules. These rules are assigned precedence values 3 and 4. The precedence values are stored in the Gx session in the rxPrecedenceCounter attribute. Using this option overrides any other Rx charging rule precedence settings (for example, any that may have been configured for the RxSponsoredDataChargingParameters service option). **Note** When this option is enabled, existing VoLTE deployments may be impacted. After upgrading to CPS 11.0.0, make sure that the gateway's configuration is changed to consider precedence values. You can use the **Precedence Start Value** and **Precedence End Value** options to set lower and upper limits for the precedence AVP values. If you do not set these options, the starting precedence value is set to 1 and is incremented to 9223372036854775807. The default setting is unchecked.
Remove Rule On Rule Deactivation	When selected, CPS manages the expiration of Rule-Deactivation time triggers. On expiration of the installed Rule-Deactivation time, CPS initiates removal of the inactive dynamic rules and tear-down of the existing Rx session. The default setting is unchecked (false).
Authorize Sponsor Data Connectivity	When selected, CPS validates the sponsor ID received in AAR request. If the received sponsor ID is unauthorized, CPS returns UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY (5067) code in AAA. The default setting is unchecked (false).
Enforce Unique AF-Charging-Identifier	When selected, CPS enforces a unique AF-Charging-Identifier across all Rx sessions within a given subscriber or network session. During an Rx session establishment, if there is already an Rx session (within the subscriber or network session) containing the same AF-Charging-Identifier value, CPS rejects the new Rx session with DUPLICATED_AF_SESSION (5064) experimental result code. The default setting is unchecked.

Parameters	Description
Prefer command level AF-Application-Identifier	The AF-Application-Identifier AVP present in the AAR message indicates the particular service that the AF session belongs to. This AVP can be present at the command level and within the Media-Component-Description AVP. When selected, and if the AF-Application-Identifier is sent both at command level and within the Media-Component-Description AVP, the AF-Application-Identifier AVP value present at the command level is considered. The default setting is unchecked, that is, the AF-Application Identifier provided within the Media-Component-Description AVP is considered.
Send timezone and location info	When selected, CPS sends time zone and location information in Rx AAA, STA, and Rx RAR response messages provided that 3GPP-MS-TimeZone AVP and 3GPP-User-Location-Info AVP are already received in the CCR message. To receive the updated time zone and location information in the messages, CPS should arm the UE_TIME_ZONE_CHANGE event trigger and USER_LOCATION_CHANGE event trigger in the service option under Event-Trigger configuration. **Note** CPS does not report this information until it is received in a CCR message from PCEF.
Trigger RAR when all rules fail (for SRVCC)	When selected, CPS can trigger RAR instead of ASR when all rules fail with rule failure code PS_TO_CS_HANDOVER. The default setting is unchecked.
Reject AAR with Invalid Service Info for missing Media-Type	When selected, if Media-Type is found to be missing in any Media-Component-Descriptions in Rx_AAR, CPS rejects the Rx_AAR with Experimental-Result-Code= INVALID_SERVICE_INFORMATION (5061). The default setting is unchecked.
Precedence Avp Lower And Upper	
Precedence Start Value	When selected, CPS automatically increments the precedence AVP value by 1 for every Rx charging rule that is installed as part of any Rx session using this Rx Client, within the same Gx session. The precedence values are stored in the Gx session in the rxPrecedenceCounter attribute. This value is optional, but when used, must be greater than 0 and less than the **Precedence End Value**.
Precedence End Value	The upper limit of the precedence values for Rx charging rules that are installed. When this value is reached, the rxPrecedenceCounter is reset to the **Precedence Start Value**. This value is required when using the **Precedence Start Value**. It must be greater than the start value.

Parameters	Description
Netloc Access Not Supported Configuration	See Netloc Access Not Supported Configuration, on page 145.
Session Binding Overriding	See Table 58: Session Binding Attribute Values, on page 144.
Rule Failure Mapping Table	By default, the table is empty and unchecked (for backward compatibility) but if you want to override the default behavior, then you need to configure all the error codes received over Gx via CCR-U or RAA message for which Rx RAR needs to be sent. You can create two tables for mapping rule-failure-code to specific-action (for sending in Rx RAR) and rule-failure-code to abort-cause (for sending in Rx ASR). If you have checked **Rule Failure Mapping Table** checkbox and did not configure any mappings then neither default Specific Action nor Abort Cause is applied for any of the Failure Code. If you have not checked **Rule Failure Mapping Table** checkbox then default Specific Action and Abort Cause is applied. • For mapping rule-failure-code to specific-action: **Table Name:** Gx Rule Failure To Rx Specific Action Mapping • For mapping rule-failure-code to abort-cause: **Table Name:** Gx Rule Failure To Rx Abort Cause Mapping **Note** In order to successfully map the rule-failure-code to specific-action, the P-CSCF/AF must have the corresponding specific-action on CPS.
Request Gx RAA for Event-Triggers	By default, the table is empty and unchecked (for backward compatibility). This configuration is used to determine the Gx event triggers that CPS should subscribe in Gx RAR (dummy RAR) before it processes the media information that it has received in Rx AAR message. The event triggers are determined based on a CRD table (dummy RAR table) whose input columns are bound to Rx media details (for example, Media-Type, AF-Application-Id, and so on) and output columns specify the event-trigger numbers that are to be subscribed/enabled on PCEF. The evaluation of this CRD table per media (Media-Component-Description) is defined through **Rx STG lookup binding** configuration under Rx Profile. The **Rx CRD AVP names to extract Event-Triggers** list is used to specify the Rx CRD AVP names. These Rx CRD AVPs are created based on the output column mapping defined for the CRD table (dummy RAR table) under **Rx STG lookup binding** (AVP name defined under Output column AVP pairs).
Extract Avps	See Extract Avps, on page 135.
Override Supported Features	See Override Supported Features, on page 136.

Table 58: Session Binding Attribute Values

Session Binding Attribute value	Description
IP Address (default)	Attempts to bind by • 1 Framed-IP-Address • 2 Framed-IPv6-Prefix
IMSI and APN	IMSI value and APN value from incoming request.
MSISDN and APN	MSISDN value and APN value from incoming request.
IMSI And IP Address	IMSI value, IP address value, and IPv6-Prefix value from incoming request. On receiving Rx session request, keys are generated for IMSI and IP Address or IMSI and IPv6-Prefix combination to load the session based on these keys.

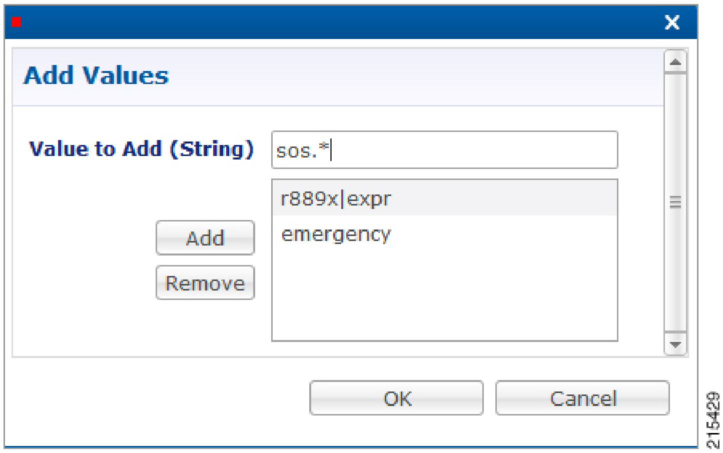
"IMSI and APN" and "MSISDN and APN" session binding attribute values are provided in order to support non 3GPP TS 29.214 compliant Rx clients.

Emergency URN List

CPS supports wildcard service URN. For example if sos.* is configured under Emergency URN List in Policy Builder and when Service-URN is received from AF with "sos" "sos.fire" "sos.police" and "sos.ambulance" and so on. indicating an emergency session CPS applies special policies that are configured for Emergency sessions.

1. Select the Rx Client name created.
2. Click **Add** near the **Emergency URN List** box. A new window **Add Values** is displayed.

Figure 53: Add Values



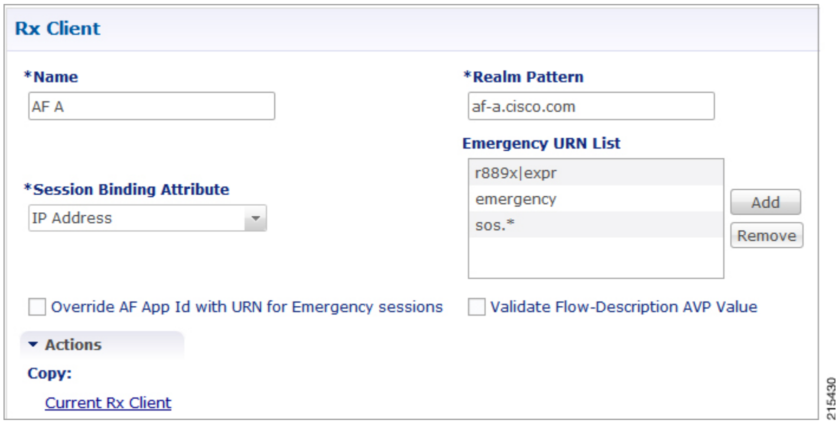
Add Values

Value to Add (String): sos.*

r889x|expr
emergency

3. Type the name of the emergency URN that you want to add in the **Value to Add (String)** text box and click **Add**.
4. Click **OK**. In the example shown below, three URNs entries are added. To remove an URN from this list select the URN to be removed and click **Remove**.

Figure 54: Add/Remove URN



Rx Client

*Name: AF A

*Realm Pattern: af-a.cisco.com

Emergency URN List:

- r889x|expr
- emergency
- sos.*

*Session Binding Attribute: IP Address

□ Override AF App Id with URN for Emergency sessions

□ Validate Flow-Description AVP Value

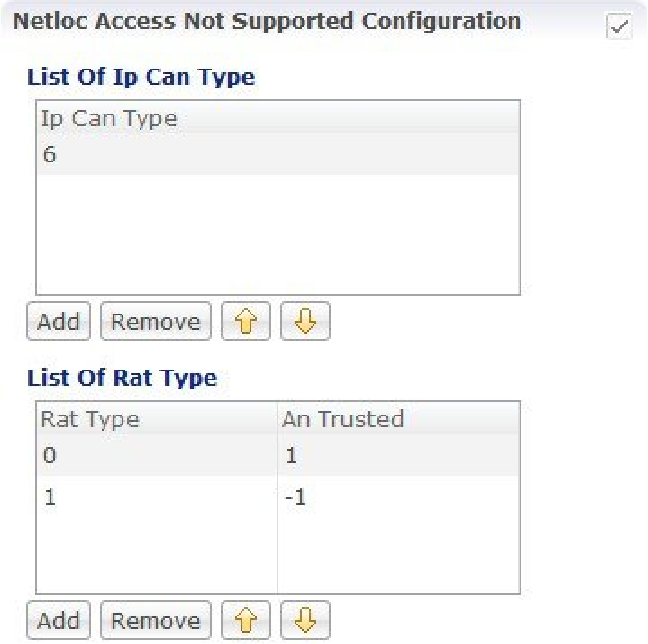
Note As shown in the example, '*' has been used for wildcarding. CPS uses standard Java pattern characters for Emergency URNs. The pattern needs to follow the standard Java regular expression syntax described here.

Netloc Access Not Supported Configuration

CPS supports to send NetLoc-Access-Support AVP in Rx AAA or STA message based on the current IP-CAN-Type or the values of Rat-Type AVP and AN-Trusted AVP. This is in accordance with the section 4.4.6.7 of the 3GPP 29.214.

To enable this, **Netloc Access Not Supported Configuration** has been added under **Rx Client**.

Figure 55: Netloc Access Not Supported Configuration



Netloc Access Not Supported Configuration ☑

List Of Ip Can Type

Ip Can Type
6

List Of Rat Type

Rat Type	An Trusted
0	1
1	-1

By default, this configuration is disabled. This means that PCRF will not check for NetLoc access support based on IP-CAN-Type or Rat-Type AVP and AN-Trusted AVP.

If this configuration is enabled but there are no entries in the two tables associated with it, then PCRF will not check for NetLoc access support based on IP-CAN-Type or Rat-Type AVP and AN-Trusted AVP.

The following table provides description related to the two tables under this configuration:

Table 59: Netloc Access Not Supported Configuration Tables

Table Name	Description
List Of Ip Can Type	This is the list of IP-CAN-Type values for which NetLoc access is not supported. For valid values of the IP-CAN-Type, refer the 3GPP specification 29.212. This table only takes integer values as input. Default value is -1. An entry with value = -1 must not be used for validation of NetLoc access.
List Of Rat Type	This is the list of Rat-Type AVP & AN-Trusted AVP values for which NetLoc access is not supported. For valid values of the Rat-Type & AN-Trusted, refer the 3GPP specification 29.212. This table only takes integer values as input. Default value is -1. *Rat Type* entry with value = -1 must not be used for validation of NetLoc access. *An Trusted* entry with value = -1 means that the AN-Trusted value does not care for this entry.

When the PCRF receives a request to report the access network information from the AF in an AAR command or in an STR command triggered by the AF, the PCRF tries to determine whether the access network supports the access network information reporting based on the currently used IP-CAN type or the values of RAT-Type AVP and AN-Trusted AVP.

PCRF first searches the list of configured IP-CAN-Type and if no match is found in the IP-CAN-Type list, then it searches the list of Rat-Type and AN-Trusted. If there is a match in any one list i.e. either the currently used IP-CAN-Type matches or current value of the Rat-Type and AN-Trusted matches, then the PCRF responds to AF with an AAA or STA command including the NetLoc-Access-Surpport AVP set to the value of 0 (NETLOC_ACCESS_NOT_SUPPORTED); otherwise, it immediately configures the PCEF to provide such access network information.

Gy Clients

This specific diameter client object is supposed to be used only in relation with the Gy interface. It adds Gy specific features to the generic diameter client already described in Diameter Clients, on page 119.

The following parameters can be configured under Gy Client:

Table 60: Gy Client Parameters

Parameters	Description
Load By Realm And User Id	If checked attempts to load the session by realm (Origin-Realm AVP value) and User Id. Default value is unchecked.
Load By Apn And User Id	If checked attempts to load the session by APN (Called-Station-Id AVP value) and User Id. Default value is unchecked.
Gy As Primary	This check box controls whether you want to run the Gy as primary (for example, for Gy only call model) or secondary (for example, Gx + Gy call model). `gyAsPK` parameter in `qns.conf` file is also used to run Gy as primary or secondary. This flag is system wide parameter. In case you want to run Gy only call model and Gx + Gy call model both on the same system, the `qns.conf` parameter cannot be used. The new check box field added under Gy Client is backward compatible with `qns.conf` parameter settings. For example, if `-DgyAsPK=true` parameter is configured in `qns.conf` file, the check box is overwritten with the value configured in `qns.conf` file. To run both Gy only and Gx + Gy call model on same system: • First delete the parameter (`-DgyAsPK=true`) if it is already configured in `qns.conf` file. • In Policy Builder, create separate Gy Clients for primary Gy and secondary Gy. • Next check the "Gy As Primary" check box in this Gy Client, if you want Gy as primary. • Uncheck the "Gy As Primary" check box in this Gy client, if you do not want Gy as primary.
Extract Avps	See Extract Avps, on page 135
Override Supported Features	Currently, not supported. **Note** This table is only supported for Gx and Rx client.

Both of the above mentioned flags help in binding the Gy session to correct Gx session when multiple Gx sessions exist for the same user.

In both cases User Id is:

User Id	AVP Value
IMSI	Subscription-Id-Data AVP value under Subscription-Id grouped AVP where Subscription-Id-Type AVP value is END_USER_IMSI (1)

User Id	AVP Value
MSISDN	Subscription-Id-Data AVP value under Subscription-Id grouped AVP where Subscription-Id-Type AVP value is END_USER_E164 (0)
NAI	Subscription-Id-Data AVP value under Subscription-Id grouped AVP where Subscription-Id-Type AVP value is END_USER_NAI (3)

Note When `gyAsPK` flag set to true in `qns.conf` file (`/etc/broadhop`), it loads the Gy session using the Gy session ID as the primary key. In CPS 12.1.0, CPS 13.1.0, and CPS 14.0.0 and higher releases, this parameter is enforced on all Gy messages. In other CPS releases, the parameter is ignored on CCR-I's, and the session is loaded by secondary keys specified in the Gy client. If there are no keys configured for the Gy client, CPS uses the default: IMSI and MSISDN from the Gy message. Default value is false.

Sy Clients

This specific diameter client object is supposed to be used to access the Sy Server.

The following parameters can be configured under Sy Client:

Table 61: Sy Client Parameters

Parameter	Description
Name	The client name that is going to be used to reference this particular client in the service configuration object.
Realm Pattern	The pattern that peer realm name should match in order for this diameter client to be used. The pattern needs to follow the standard Java regular expression syntax described here. The first choice for Realm Pattern value should always be the exact peer realm name whenever possible.
Counter Lookahead Interval	Dynamic calculation of policy counters events that are subjected to an update for the interval specified. If the look ahead interval is specified, CPS evaluates all policy counters and if a policy counter is about to expire before the interval, CPS sends the policy-counter-stats. Default value is 180 minutes.
Extract Avps	See Extract Avps, on page 135

Diameter Defaults

The Diameter Defaults section provides global default values for different modules of the system.

In order to define a Diameter Default you need to perform the following steps:

1. Login into Policy Builder.
2. Select **Reference Data** tab.
3. From the left pane select **Diameter Defaults**.
4. Select **Summary**.
5. Create the specific default object according to your needs.
6. Provide values for at least the mandatory fields.

Note

- The mandatory fields are marked with a "*" on the upper left corner of the field name label.
- There should be at most one object for each diameter default type or the results will be unpredictable. The Policy Builder GUI does not enforce this restriction though.

Custom AVP Profile

This feature allows the Service Provider to extend the Diameter dictionary with new vendor specific AVPs along with a source for that AVP and a destination where the AVP is going to be used.

The feature consists of two components:

- Custom Avp Table
- Avp Mappings

Custom Avp Table

This table allows for the definition of the custom AVP with all the standard attributes of an AVP.

The following parameters can be configured under Custom Avp Table:

Table 62: Custom Avp Table Parameters

Parameter	Description
AVP Name	Any string that is used to identify this custom AVP.
Avp Code	AVP Code combined with Vendor Id field identifies the attribute uniquely. • 1 - 255 Backward compatibility with Radius without setting the Vendor Id field. **Note** RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface. • 256 - above Used for Diameter and are allocated by IANA.

Parameter	Description
Vendor Id	It indicates the Vendor Id of the AVP. The following are the supported Vendor Ids: • base (0) • ciscoSystems (9) • Ericsson (193) • Tekelec (323) • TGPP2 (5535) • Openet (7898) • Starent (8164) • TGPP (10415) • ETSI (13019) • NSN (28458) • Nokia (34326) • Lucent (1751) • Verizon (12951) • Camiant (21274) • Huawei (2011)
Vendor Code	Vendor Id value as assigned by IANA. The Vendor Id bit known as the Vendor-Specific bit indicates whether the optional Vendor Code field is present in the AVP header. When set the AVP Code belongs to the specific vendor code address space.
Mandatory Bit	Indicates whether support of the AVP is required. If this Bit is checked then Diameter Client Server Proxy and Translation Agent must support the handling of this AVP.
Protected Bit	Indicates the need for encryption for end-to-end security. If this bit is checked indicates that AVP data is encrypted for end-to-end security.
Vendor Id Bit	Indicates whether the optional Vendor-ID field is present in the AVP header.

Parameter	Description
Data Type	Any valid basic AVP data format • Float32Avp • Float64Avp • Integer32Avp • Integer64Avp • OctetStringAvp • Unsigned32Avp • Unsigned64Avp • UTF8String

Avp Mappings

This table allows for the mapping between the source and the destination for the custom AVP (defined in the previous section). Multiple attributes can be used to identify both the source for the custom AVP value as well as the destination where the AVP is going to be used.

The following mappings are supported:

- Custom AVP to Custom AVP Mapping Maps a custom AVP to another custom AVP.
- 3gpp / spr AVP to 3gpp AVP Mapping Maps a 3GPP AVP or a SPR attribute to a 3GPP AVP.
- 3GPP / SPR AVP to Custom AVP Mapping Maps a 3GPP AVP or a SPR attribute to a custom AVP.

Custom AVP to Custom AVP Mapping

The following parameters can be configured under Custom AVP to Custom AVP Mapping:

Table 63: Custom AVP to Custom AVP Mapping Table Parameters

Parameter	Description
Source Avp	Name of AVP that has to be looked up for possible mapping.
Source App Id	The Application Interface Id (Gx) in numeric format (16777238) on which the Source AVP is received.
Source Cmd Code	The command code of the message on interface Source APPID that contains the Source AVP.
Source Cmd Type	The message indicated by Source Command Code is a request or response. Types: • Request • Response
Origin Host	This field contains the identification of the source point of the operation.

Parameter	Description
Origin Realm	This field contains the identification of the realm of the operation originator.
Target Avp	AVP Name that is actually mapped to Source AVP.
Target App Id	Target Application Identifier (Sy - 16777302 - for this release).
Target Cmd Code	The command code of the message that goes on Target APPID and have Target AVP.
Target Cmd Type	The message having Target Command Code request or a response. Types: • Request • Response
Destination Host	This field contains the identification of the destination point of the operation.
Destination Realm	This field contains the realm of the operation destination.

Response value for Source Cmd Type and Target Cmd Type is not currently supported.

3gpp / spr AVP to 3gpp AVP Mapping

The following parameters can be configured under 3gpp / spr AVP to 3gpp AVP Mapping:

Table 64: 3gpp / spr AVP to 3gpp AVP Mapping Table Parameters

Parameter	Description
Source Avp	Name of AVP that has to be looked up for possible mapping.
Is SPR AVP?	Check if the source is an SPR attribute. The Source AVP originates from a Source Command or from Subscriber profile in Subscriber Profile Repository. Default value is unchecked.
Source App Id	The Application Interface Id (Gx) in numeric format (16777238) on which the Source AVP is received.
Source Cmd Code	The command code of the message on interface Source APPID that contains the Source AVP.
Source Cmd Type	The message indicated by Source Command Code is a request or response. Types: • None • Request • Response
Origin Host	This field contains the identification of the source point of the operation.

Parameter	Description
Origin Realm	This field contains the identification of the realm of the operation originator.
Target Avp	AVP Name that is actually mapped to Source AVP.
Target App Id	Target Application Identifier (Sy - 16777302 - for this release).
Target Cmd Code	The command code of the message that goes on Target APPID and have Target AVP.
Target Cmd Type	The message having Target Command Code request or a response. Types: • Request • Response
Destination Host	This field contains the identification of the destination point of the operation.
Destination Realm	This field contains the realm of the operation destination.

Response value for Source Cmd Type and Target Cmd Type is not currently supported.

3GPP / SPR AVP to Custom AVP Mapping

The following parameters can be configured under 3GPP / SPR AVP to Custom AVP Mapping:

Table 65: 3GPP / SPR AVP to Custom AVP Mapping Table Parameters

Parameter	Description
Source Avp	Name of AVP that has to be looked up for possible mapping.
Is SPR AVP?	Check if the source is an SPR attribute. The Source AVP originates from a Source Command or from Subscriber profile in Subscriber Profile Repository. Default value is unchecked.
Source App Id	The Application Interface Id (Gx) in numeric format (16777238) on which the Source AVP is received.
Source Cmd Code	The command code of the message on interface Source APPID that contains the Source AVP.
Source Cmd Type	The message indicated by Source Command Code is a request or response. Types: • None • Request • Response
Origin Host	This field contains the identification of the source point of the operation.

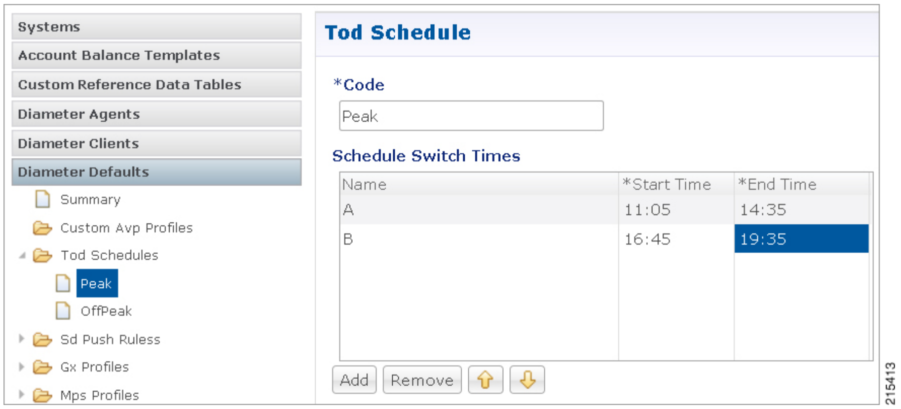
Parameter	Description
Origin Realm	This field contains the identification of the realm of the operation originator.
Target Avp	AVP Name that is actually mapped to Source AVP.
Target App Id	Target Application Identifier (Sy - 16777302 - for this release).
Target Cmd Code	The command code of the message that goes on Target APPID and have Target AVP.
Target Cmd Type	The message having Target Command Code request or a response. Types: • Request • Response
Destination Host	This field contains the identification of the destination point of the operation.
Destination Realm	This field contains the realm of the operation destination.

Response value for Source Cmd Type and Target Cmd Type is not currently supported.

ToD Schedule

This feature allows for different PCC rules to be installed on a per time-of-day basis. Based on the defined schedules PCRF will look ahead one scheduled interval every time the policy is re-evaluated and will schedule for each PCC rule an activation time using the Rule-Activation-Time AVP and de-activation time using the Rule-Deactivation-Time AVP.

Figure 56: ToD Schedule



Tod Schedule

*Code: Peak

Schedule Switch Times

Name	*Start Time	*End Time
A	11:05	14:35
B	16:45	19:35

- Both Start Time and End Time need to be defined in hhmm 24hr format.
- UE time zone (3GPP-MS-TimeZone AVP) if available takes precedence over PCRF time-zone.
- ToD schedule should be complete for 24 hours.
- There should be no overlapping between the different schedule Switch Times.

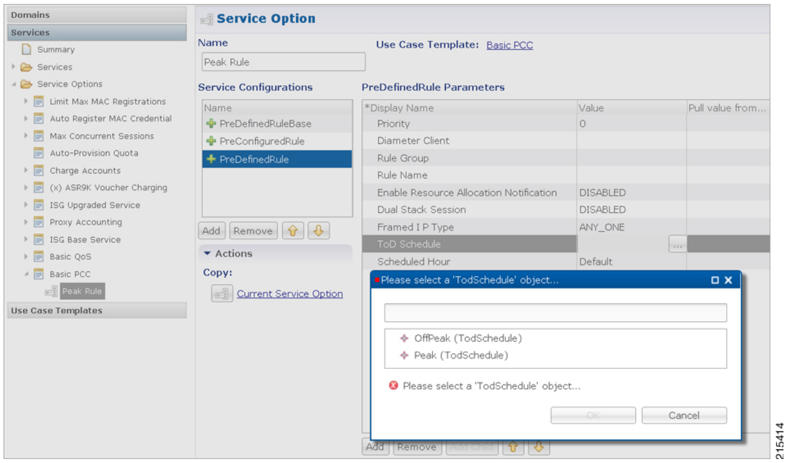
- First charging schedule should start at mid-night with start-time value as 0000 and last schedule should end on next mid-night with end-time value as 2359. Time entry with 2359 is rounded up to the next minute to complete the 24 hour schedule.

The ToD Schedule can be referenced only from a **PreDefinedRule**, **PreDefinedRuleBase** or a **PreConfiguredRule** service configuration object.

In order to use a ToD Schedule in a Service Option you need to perform the following steps

1. Login into Policy Builder.
2. Select **Services** tab.
3. From the left pane select **Services**.
4. Expand **Service Options** tree.
5. Select and expand your service option.
6. Select the service option object.
7. Select the **Value** cell corresponding to the ToD Schedule.
8. Push the "…" button.
9. Select the ToD Schedule from the popup window.
10. Click **OK**.

Figure 57: ToD Schedule - Service Option



Name: Peak Rule

Use Case Template: Basic PCC

PreDefinedRule Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Rule Group		
Rule Name		
Enable Resource Allocation Notification	DISABLED	
Dual Stack Session	DISABLED	
Framed I P Type	ANY_ONE	
ToD Schedule		
Scheduled Hour	Default	

Please select a 'TodSchedule' object...

OffPeak (TodSchedule)
Peak (TodSchedule)

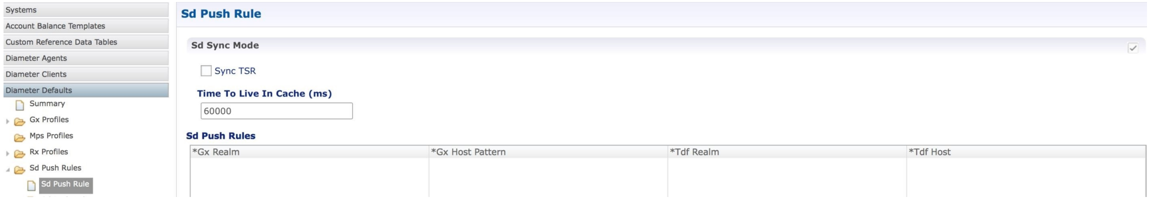
Please select a 'TodSchedule' object...

For more details about how to define a service option refer to Services, on page 229.

Sd Push Rules

This section supports the Sd solicited reporting scenario when the TDF-Information grouped AVP is not sent from the PCEF to the PCRF in a Gx CCR-i. For more information on Sd solicited reporting refer to *3GPP TS 29.212*.

Figure 58: Sd Push Rules



Sd Push Rule

Sd Sync Mode

□ Sync TSR

Time To Live In Cache (ms)

60000

Sd Push Rules

*Gx Realm	*Gx Host Pattern	*Tdf Realm	*Tdf Host

The following parameters can be configured under **Sd Push Rules**:

Table 66: Sd Sync Mode

Parameters	Description
Sync TSR	Select to enable TSR in sync mode.
Time To Live in Cache (ms)	When Sd Sync mode is enabled, determines how long the Gx CCA-I response is stored in the session before retracting the stored response to be sent to PGW after Sd TSR/TSA exchange occurs between PCRF and TDF. This value is recommended to be higher than the PGW timeout.

Table 67: Sd Push Rules

Parameter Type	Message	Attribute	AVP
Input	Gx CCR-i	Gx Realm	Origin-Realm
		Gx Host Pattern	Origin-Host
Output	Sd TSR	TDF Realm	Destination-Realm
		TDF Host	Destination-Host

Note

- The first choice for Gx Host Pattern value should always be the exact peer realm name whenever possible.
- No Sd session is initiated if there's no match for the input columns in the Sd Push Rules table.

Gx Profile

This section provides default values to be used for Gx default bearer QoS parameters as well as some specific behavior related to default bearer QoS.

The following parameters can be configured under Gx Profile:

Table 68: Gx Profile Parameters

Parameter	Description
Push Pre Configured Rule Options	Controls whether the configured default bearer QoS will be installed on the default bearer or on the secondary bearers. • PushOnDefaultBearerQoS (default) • PushWithUpgradedDefaultBearerQoS
Logical Apn	Allows for a default APN name to be defined. This APN name is going to be further used as an input into the AF Application Id Validation feature described below. The APN value will be set based on the available data and the priorities described below. • 1 - A policy derived AVP having the same value as the Logical Apn • 2 - Called-Station-Id AVP from incoming Rx AAR • 3 - Called-Station-Id AVP from Gx session
Gx Client QoS Exclusion List	Gx client names that are allowed not to have a default bearer QoS installed. In case a default bearer QoS has not been configured in the policy and the Gx client name has not been added to this list an error response will be sent to the PCEF containing the Result-Code AVP value DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143).
Grant Requested QoS	Controls whether the requested QoS should be granted or not as the default bearer QoS. Default value is unchecked.
Grant Requested Qos Over Global Qos	If this option is selected then the requested QoS should be granted even if the global QoS is provisioned. There are three type of QoS first is taken from service second is from default QoS and third one is from request. If this flag is checked then requested QoS will take priority over default QoS. Default value is unchecked.
Global Default Granted QoS	
Qci	The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0 10 – 255 are divided for usage as follows • 0 - Reserved • 10-127 - Reserved • 128-254 - Operator specific • 255 - Reserved
Max Req Bandwidth UL	It defines the maximum bit rate allowed for the uplink direction.
Max Req Bandwidth DL	It defines the maximum bit rate allowed for the downlink direction.

Parameter	Description
Guaranteed Bit Rate UL	It defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bit Rate DL	It defines the guaranteed bit rate allowed for the downlink direction.
Apn Agg Max Bit Rate UL	It defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN.
Apn Agg Max Bit Rate DL	It defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN.
Enable Pending Policy Evaluation	When selected, pending policy calculation is enabled for one look ahead in advance. Default value is unchecked.

ARP

Select the Arp type from the drop-down list to open parameters for the corresponding selection. ARP is used to indicate the priority of allocation and retention.

The following parameters can be configured under **Arp**:

Table 69: ARP Parameters

Selection	Parameters	Description
Allocation Retention Priority	Priority Level	The priority level is used to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined with value 1 as the highest level of priority. • Values 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. • Values 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.
	Preemption Capability	If it is provided within the QoS-Information AVP the AVP defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. If it is provided within the Default-EPS-Bearer-QoS AVP the AVP defines whether the default bearer can get resources that were already assigned to another bearer with a lower priority level. • 0 This value indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. • 1 This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.
	Preemption Vulnerability	If it is provided within the QoS-Information AVP the AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. If it is provided within the Default-EPS-Bearer-QoS AVP the AVP defines whether the default bearer can lose the resources assigned to it in order to admit a pre-emption capable bearer with a higher priority level. • 0 This value indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied. • 1 This value indicates that the resources assigned to the service data flow or bearer shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level.

Selection	Parameters	Description
Application QoS Policy	AF Application Identifier Pattern	It contains information that identifies the particular service that the AF service session belongs to. This information may be used by the PCRF to differentiate QoS for different application services. You can specify regular expressions for this parameter as needed.
	Media Type	Applicable Media-Type (session level or specific to Media-Component-Description). The list includes Audio Video Data Application Control Text Message and Other.
Reservation Priority QoS Policy	Reservation Priority	The Reservation Priority includes the priority value of the related priority service. The Reservation Priority is populated with a default value if the priority value is unknown.
Base MPS QoS/Base MPS QoS Gx	Qci	The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS excluding the applicable bit rates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0 10 – 255 are divided for usage as follows: • 0 Reserved • 10-127 Reserved • 128-254 Operator specific • 255 Reserved
MPS QoS	MPS Id	The MPS Id contains the national variant for MPS service name indicating an MPS session.
	Media Type	Applicable Media-Type (session level or specific to Media-Component-Description). Select from drop-down list. The list includes Audio Video Data Application Control Text Message and Other.

Relaxed USAGE_REPORT Event-Trigger Handling

Use this checkbox to enable the functionality for supporting old event-trigger value (26) for the usage report. This configuration will be applicable only when CPS is configured to use R10 event-trigger values by unchecking the '**Use V9 Event Trigger Mapping**' flag in Diameter Configuration.

Peers using Event-Trigger value (26) for USAGE_REPORT

The following table contains the list of realm and host entries for which CPS will support old event-trigger value (26) for USAGE_REPORT.

The parameters can be configured under **Relaxed USAGE_REPORT Event-Trigger Handling**:

Table 70: Relaxed USAGE_REPORT Event-Trigger Handling Parameters

Parameter	Description
Realm Pattern	The pattern that peer realm name should match in order for this diameter client to be used. The pattern needs to follow the standard Java regular expression syntax described here.

Parameter	Description
Host Pattern	Host name pattern as received in Origin-Host AVP in AAR message. The pattern needs to follow standard Java pattern conventions. The pattern needs to follow the standard Java regular expression syntax described here.

QoS Retry on APN-AMBR_FAILURE_MODIFICATION

Use this check box to receive APN-AMBR_FAILURE_MODIFICATION events from PCEF.

The following parameters can be configured under **QoS retry on APN-AMBR_FAILURE_MODIFICATION**:

Table 71: QoS retry on APN-AMBR_FAILURE_MODIFICATION Parameters

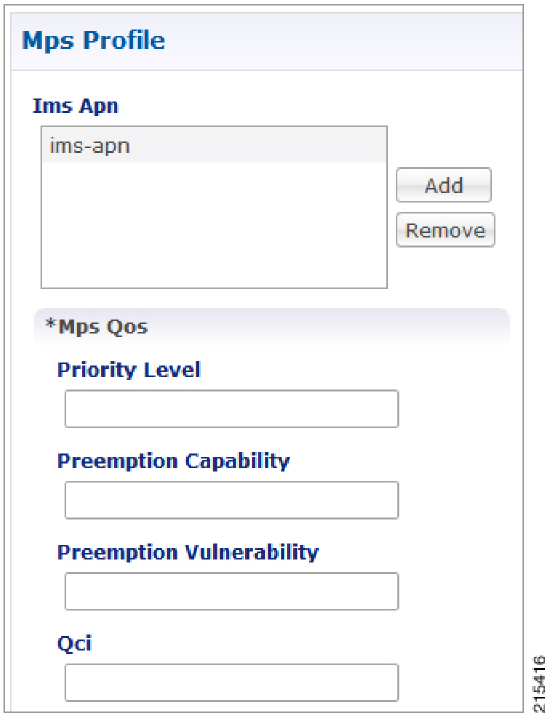
Parameter	Description
Number Of Retry	Number of retries to push calculated QoS information.
QoS Retry Options	In the case GGSN sends APN-AMBR_FAILURE_MODIFICATION report to CPS, following are the retry options in which CPS sends the QoS information: • Immediate Retry: CPS calculates QoS based on the configured policy and sends it immediately in a CCA message. • Delayed Retry: CPS responds to CCA-U without any QoS information unless there is difference between the current derived QoS and previously sent QoS. CPS sends the QoS information in the next RAR or CCA-U message.
Action On QoS Retry Exhaust	CPS retries sending the QoS information "n” times, to avoid looping. After exhaustion of the retries, following are the options: • Continue Session: CPS does not send same QoS information in subsequent CCA-U message unless there is a difference between the current calculated QoS and previously sent QoS. • Terminate Session: CPS sends RAR with Release Cause value as UNSPECIFIED_REASON after the time configured in Time To Trigger Release RAR expires. On receiving CCR-T, CPS terminates the session.
Time To Trigger Release RAR In Minutes	CPS sends RAR with Release Cause value as UNSPECIFIED_REASON after the time configured in Time To Trigger Release RAR expires.
Time To Reset QoS Retry Counter In Minutes	Once CPS receives APN-AMBR_FAILURE_MODIFICATION, CPS sets next reset timer to value configured in Time to Reset QoS Retry Counter. If CPS does not receive APN-AMBR_FAILURE_MODIFICATION within this specified time, CPS resets the retry count to 0.

MPS Profile

This section provides default values to be used if MPS feature is needed to support eMPS priority. The MPS Profile provides MPS attributes required for priority service provisioning. The priority level value from Service configuration takes precedence over MPS Profile value.

Note There must be at least one Mps Profile defined under **Mps Profiles**.

Figure 59: MPS Profile



The following parameters can be configured under **Mps Profile**:

Table 72: MPS Profile Parameters

Parameter	Description
Ims Apn	List of IMS APNs for which the MPS feature is supported. This field can accommodate several Ims Apn that are used to match with the incoming service request for priority service. The values that are received by the Default Bearer QoS are looked up for a suitable Ims Apn match. If the APN value of a Gx session request matches IMS APN IMS signaling priority from EMPS service is used as priority level.
Mps QoS	For information on parameters under Mps QoS refer to ARP Parameters.

For additional information on 3GPP specifications refer to http//www.3gpp.org/DynaReport/29212.htm.

The above link is compliant with Release 11.

Rx Profile

This section provides default and specific values to be used by the different QoS parameter mapping functions at PCRF as per 3GPP TS 29.213. This section also provides a mechanism to authorize the Rx IMS sessions.

Basic Options

Table 73: Rx Profile - Basic Options

Parameter	Description
Prefer answer Codec-Data	Select **Prefer answer Codec-Data** checkbox if you want the default priority to be given to the answer codec (when both answer and offer are present within the AAR). By default, this option is unchecked (not selected).
Disable Always On EMPS Service	If the checkbox is selected, then the feature **Always On EMPS Service** gets disabled otherwise the feature works by default (when the checkbox is not selected).
Disable Downgrade of Normalised ARP and QCI	If this checkbox is selected, the Normalised ARP and QCI is not downgraded till all the Rx sessions terminate. By default, this option is not selected. If this checkbox is not selected, the Normalised ARP and QCI is downgraded when RxSession with Priority ARP terminates. For more information and ARP and QCI Normalization, refer to ARP and QCI Normalization, on page 167.
Default QoS Policy	Provides the values to be used during the derivation of the Maximum Authorized Data Rates Authorized Guaranteed Data Rates Maximum Authorized QoS Class per IP flow or bidirectional combination of IP flows in the PCRF and for calculating the Maximum Authorized/Guaranteed Data Rates QCI and ARP in the PCRF whenever the "as set by the operator" phrase is used in the algorithm description. For description of different parameters under Default QoS Policy, refer to Table 68: Gx Profile Parameters, on page 157.
Rx Sync Mode	For description of different parameters under Rx Sync Mode parameters, refer to Table 74: Rx Sync Mode Parameters, on page 164.

Parameter	Description
MPS QoS Policy	Provides a way to derive QoS attributes for MPS sessions based on some other AVP values. For description of different parameters under MPS QoS Policy, refer to Table 69: ARP Parameters, on page 159. **Note** A Media-Type having an empty label shall be used only to get the output values to be used for default bearer QoS.
Codec QoS Policy	For more information, refer to Codec QoS Policy, on page 164
Reservation Priority QoS Policy	Provides a way to derive Rx dedicated bearers QoS attributes based on Reservation-Priority AVP value as per 3GPP TS 29.213. For description of different parameters under Reservation Priority QoS Policy refer to Table 68: Gx Profile Parameters, on page 157 and Table 69: ARP Parameters, on page 159.
AF Application Id Validation	For more information, refer to AF Application Id Validation, on page 166

Table 74: Rx Sync Mode Parameters

Parameters	Description
Sync AAR	Select to enable AAR in sync mode.
Sync STR	Select to enable STR in sync mode.
Time To Live in Cache Millis	When Rx Sync mode is enabled, determines how long the Rx AAR/STR response is stored in the session before retracting the stored response to be sent towards PCSCF after Gx RAR/RAA exchange occurs between PGW and PCRF. This value is recommended to be higher than the PCSCF timeout.

Codec QoS Policy

Provide a way to derive Rx dedicated bearers QoS attributes based on Codec-Data AVP value as per 3GPP TS 29.213.

For description of different parameters under Codec QoS Policy refer to Table 68: Gx Profile Parameters, on page 157 and Table 69: ARP Parameters, on page 159.

The additional parameters Codec Data Pattern and Codec Details Pattern contains codec related information known at the AF. This information is encoded as per 3GPP 29.214 specifications

The first line of the value of the Codec-Data AVP consists of either the word `uplink` or the word `downlink` (in ASCII) followed by a new-line character. The semantics of these words are the following:

- `uplink` indicates that the SDP was received from the UE and sent to the network.
- `downlink` indicates that the SDP was received from the network and sent to the UE.

The second line of the value of the Codec-Data AVP consists of either the word `offer`, the word `answer`, or the word `description`.

The rest of the value consists of the SDP line(s) in ASCII encoding separated by new-line characters, as specified in IETF RFC 4566. The first of these line(s) is an `m` line. The remaining lines are any available SDP `a` and `b` lines related to that `m` line.

Restriction

- You should not configure 'Codec QoS Policy' table with ambiguous entry. If multiple rows are configured which matches same 'Codec-Data' and 'Codec-Details' values then CPS will fetch first matched row.
- Codec-Data column value is mandatory in Policy Builder configuration while adding entry in the 'Codec QoS Policy' table.
- CPS considers the first Codec-Data AVP if AAR request has multiple 'Codec-Data' AVPs.
- By default, CPS uses the first Codec-Data AVP with `offer` or `answer` on the second line if the AAR request has multiple Codec-Data AVPs. If `Prefer Answer` is set to `true`, CPS uses the first Codec-Data AVP with `answer` on the second line, or the first Codec-Data AVP with `offer` if there is no Codec-Data AVP with `answer`.
- CPS considers only the first media format in the `m=` line.
- You should configure the 'Codec Data Pattern' and 'Codec Details Pattern' column values with wildcards as per the standard Java regular expression syntax described at the link.

  CPS supports leading middle and trailing wildcards. Multiple wildcards should be possible in a single string.
- Case sensitivity is supported for both 'Codec Data Pattern' and 'Codec Details Pattern' columns so you should provide the values accordingly.

If multiple Codec-Data AVPs are reported in multiple AAR messages for a single Rx session then CPS will consider the first Codec-Data AVP value received in first AAR message for selecting QoS policies.

The following sections provides few examples on how to configure the wildcards.

1. Codec Data value used as the search key in this table is the 4th group (of numbers) from the 3rd line of the Codec-Data AVP string value.

   In the following example, only the value 116 is going to be used as a search key in the Codec QoS Policy table.

   ```
   uplink
   offer
   m=audio 50000 RTP/AVP 116 107 97 115 111 110
   a=rtpmap116 AMR-WB/16000
   a=rtpmap107 AMR-WB/16000
   a=rtpmap97 AMR/8000
   a=rtpmap115 AMR/8000
   a=rtpmap111 telephone-event/16000
   a=rtpmap110 telephone-event/8000
   a=currqos local none
   a=currqos remote none
   a=desqos mandatory local sendrecv
   a=desqos optional remote sendrecv
   a=sendrecv
   a=ptime20
   a=maxptime240
   ```

2. Only the first Codec-Data AVP value is used.
3. You can configure Codec Details Pattern and Codec Data Pattern columns with wildcards as per java regular expressions (for example, .* $, and so on) so that CPS can compare the AVP values with this regex and fetch the appropriate QoS values.

   Example:

   Consider you want to configure “Codec Data Pattern 98" and “Codec Details Pattern AMR/8000”.

   There are multiple combination you can configure. Some examples are given below :

   With ExactMatch:

   - Codec Data Pattern 98 Codec Details Pattern AMR/8000.
   - Codec Data Pattern 98 Codec Details Pattern <No value specified>, that is, null

   With wildcards

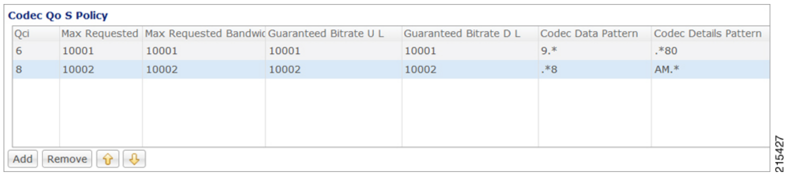
   - Codec Data Pattern .*8 Codec Details Pattern AM.*
   - Codec Data Pattern 9.* Codec Details Pattern .*80
   - Codec Data Pattern 9.* Codec Details Pattern AM.*80
   - Codec Data Pattern .* Codec Details Pattern ^AM.*80

   AM.*80 indicates that String that has AM and any number characters and 80. It does not mean that string should start with AM and end with 80.

   If you want to specify starting and ending characters explicitly then you should use '^' for starting (say ^77 value should start with 77) and '$' for ending (say AM.*80$ value should end with 80); you should configure the 'Codec Data Pattern' and 'Codec Details Pattern' column as per the standard Java regular expression syntax.

   Suppose you configure multiple rows matching the same values; for example, as shown in the following figure, both rows can be matched with values “Codec-Data 98 and Codec-Details AMR/8000." In this case, CPS will select the first matched row.

   Figure 60: Codec QoS Policy



Codec Qo S Policy

Qci	Max Requested	Max Requested Bandwic	Guaranteed Bitrate U L	Guaranteed Bitrate D L	Codec Data Pattern	Codec Details Pattern
6	10001	10001	10001	10001	9.*	.*80
8	10002	10002	10002	10002	.*8	AM.*

AF Application Id Validation

Provides a way to authorize the Rx IMS sessions. In case there's not a match between the AVP values below in the table the PCRF shall send an error response to the AF containing the Experimental-Result-Code AVP with value REQUESTED_SERVICE_NOT_AUTHORIZED (5063) as per 3GPP TS 29.214.

Interface	AVP Value
Gx	Refer to Logical APN attribute under Gx Profile, on page 156.

Interface	AVP Value
Rx	AF-Application-Identifier
	Media-Type

Note

- Called-Station-Id AVP value is retrieved from the Gx session the Rx session binds to.
- If the incoming Rx AAR message contains multiple flows having different AF-Application-Identifier AVP value or Media-Type AVP value and any of these flows is not authorized than the PCRF shall send an error response as described above.
- If no AF-Application-Identifier AVP is present in the incoming request the validation is skipped.

ARP and QCI Normalization

Apply Best/Normalized ARP across all PrioritySharing Rx sessions with same MediaType and AF-Application-Identifier. The ARP normalization is applied within multiple Media Sub Component within Media Component Description.

Elevate the Default bearer ARP to the best/normalized ARP across all QCI, Media Type and AF-Application-Identifiers.

There are two ways to enable the feature:

- Priority-Sharing-Indicator (PSI) AVP present in the Rx_AAR sent by P-CSCF/IMS "Priority-Sharing-Indicator".

  0 - enabled

  1 - disabled

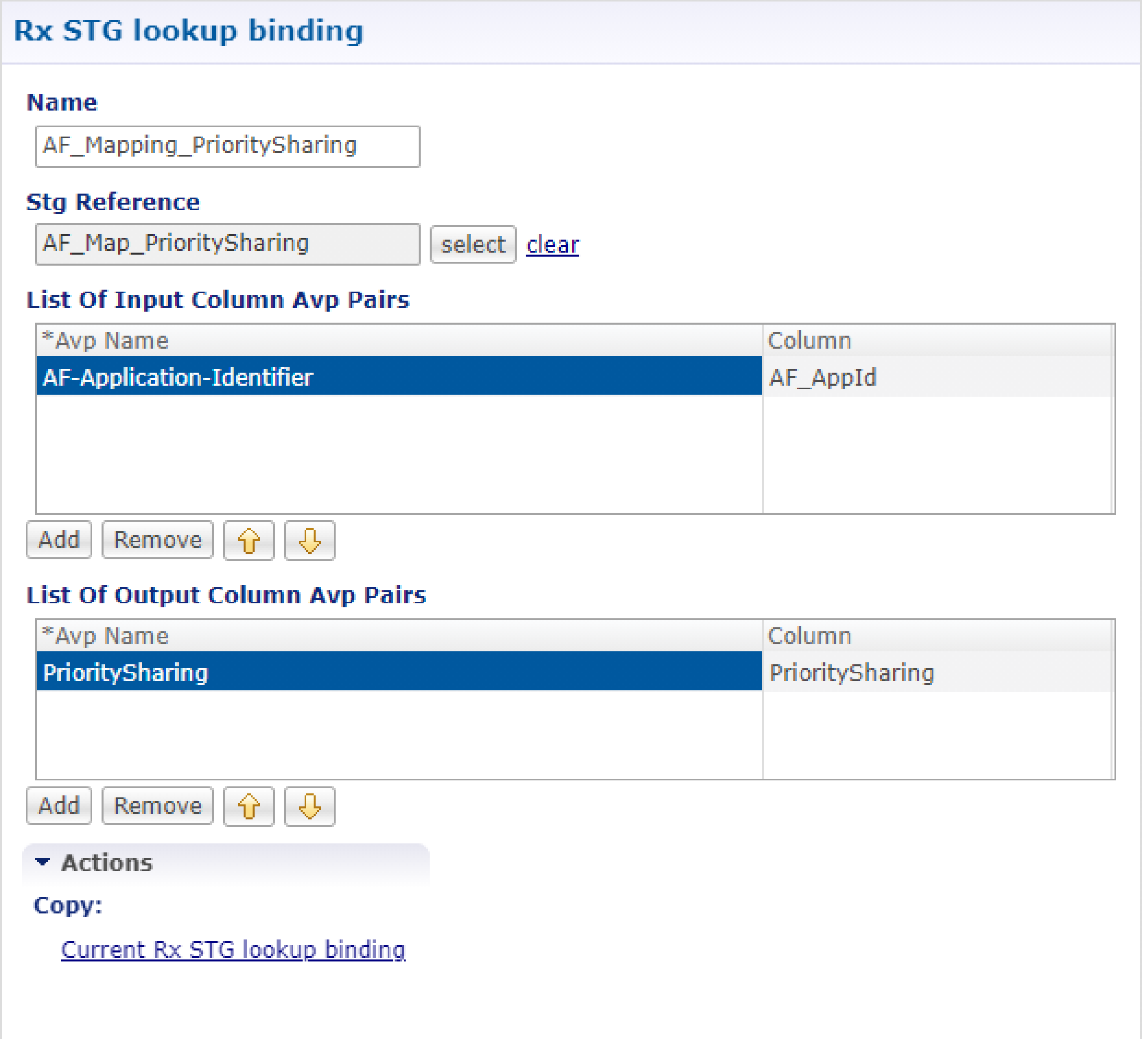
- PSI feature is enabled/disabled for specific AF-Application-Identifier via Policy Builder and CRD Configuration.

  Enable - set prioritySharing value as “0”

  Disable - set prioritySharing value as “1”

Policy Builder and CRD Configuration: Rx STG lookup binding for AF-Application-Identifier AVP to PrioritySharing Enable/Disable.

Figure 61: Rx STG lookup binding



Rx STG lookup binding

Name: AF_Mapping_PrioritySharing

Stg Reference: AF_Map_PrioritySharing

List Of Input Column Avp Pairs

*Avp Name	Column
AF-Application-Identifier	AF_AppId

List Of Output Column Avp Pairs

*Avp Name	Column
PrioritySharing	PrioritySharing

Actions

Copy:

Current Rx STG lookup binding

Advanced Options

You can get access to these features by creating child objects to your Rx profile object.

Note There should be at least one object of each type for any Rx profile object or the results will be unpredictable. The Policy Builder GUI does not enforce this restriction though.

Sponsored Data Charging Parameters

The Sponsored Data Charging Parameters allows you to configure specific charging parameters for the Sponsored Data scenarios depending on some AVPs from the incoming Rx AAR. These parameters are going to be set under Charging-Rule-Definition grouped AVP.

The required charging parameters are as follows:

- Rating-Group
- Reporting-Level
- Online
- Offline
- Metering-Method

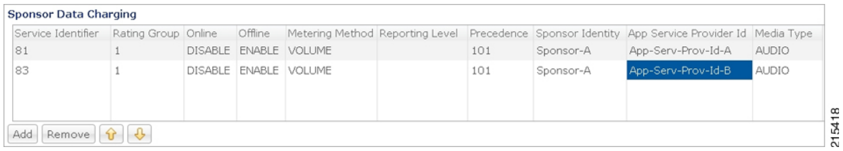
To map the above mentioned parameters the following keys are used:

- Sponsor-Id
- Application-Service-Provider-Identity
- Media Type

These keys are applicable for Sponsored Data Charging Parameters only.

The mapping configuration for the charging parameters is configured under **Policy Builder** > **Reference Data tab** > **Diameter Defaults** > **Rx Profile**.

Figure 62: Sponsor Data Charging



Sponsor Data Charging

Service Identifier	Rating Group	Online	Offline	Metering Method	Reporting Level	Precedence	Sponsor Identity	App Service Provider Id	Media Type
81	1	DISABLE	ENABLE	VOLUME		101	Sponsor-A	App-Serv-Prov-Id-A	AUDIO
83	1	DISABLE	ENABLE	VOLUME		101	Sponsor-A	App-Serv-Prov-Id-B	AUDIO

In the Sponsor Data Charging table, you can define the parameter values in all the columns including the values for the key parameters such as - Sponsor Identity App Service Provider Identity and Media Type.

Default Sponsor Data Charging

Defines the default values for the sponsor data charging parameters under Charging-Rule-Definition grouped AVP to be used in case there's no match in the Sponsor Data Charging. This configuration is optional. Default value is unchecked.

The following parameters can be configured under Sponsor Data Charging:

Table 75: Sponsor Data Charging Parameters

Parameter	Description
Service Identifier	The identity of the service or service component the service data flow in a PCC rule relates to.
Rating Group	The charging key for the PCC rule used for rating purposes.
Online	It defines whether the online charging interface from the PCEF for the associated PCC rule is enabled. The default charging method provided by the CPS takes precedence over any pre-configured default charging method at the PCEF. • Enable This value is used to indicate that the online charging interface for the associated PCC rule is enabled. • Disable This value is used to indicate that the online charging interface for the associated PCC rule is disabled.

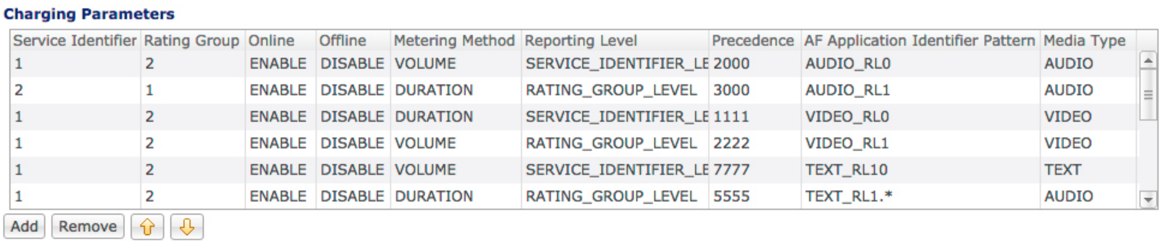
Parameter	Description
Offline	It defines whether the offline charging interface from the PCEF for the associated PCC rule is enabled.The default charging method provided by the CPS takes precedence over any pre-configured default charging method at the PCEF. • Enable This value is used to indicate that the offline charging interface for the associated PCC rule is enabled. • Disable This value is used to indicate that the offline charging interface for the associated PCC rule is disabled.
Metering Method	The Metering-Method AVP (AVP code 1007) is of type Enumerated and it defines what parameters shall be metered for offline charging. The PCEF may use the AVP for online charging in case of decentralized unit determination and having three values • DURATION (0) This value shall be used to indicate that the duration of the service data flow shall be metered. • VOLUME (1) This value shall be used to indicate that volume of the service data flow traffic shall be metered. • DURATION_VOLUME (2) This value shall be used to indicate that the duration and the volume of the service data flow traffic shall be metered.
Reporting Level	The Reporting-Level AVP is of type Enumerated and it defines on what level the PCEF reports the usage for the related PCC rule.There are three types of reporting levels • SERVICE_IDENTIFIER_LEVEL (0) This value shall be used to indicate that the usage shall be reported on service id and rating group combination level and is applicable when the Service-Identifier and Rating-Group have been provisioned within the Charging-Rule-Definition AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. • RATING_GROUP_LEVEL (1) This value shall be used to indicate that the usage shall be reported on rating group level and is applicable when the Rating-Group has been provisioned within the Charging-Rule-Definition AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. • SPONSORED_CONNECTIVITY_LEVEL (2) This value shall be used to indicate that the usage shall be reported on sponsor identity and rating group combination level and is applicable when the Sponsor-IdentityAVP Application-Service-Provider-Identity AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging.
Precedence	This determines the order in which the service data flow templates are applied at service data flow detection at the PCEF. A PCC rule with the Precedence AVP with lower value shall be applied before a PCC rule with the Precedence AVP with higher value.

Parameter	Description
Sponsor Identity	Sponsor-Identity AVP value under the Sponsored-Connectivity-Data grouped AVP.
App Service Provider	App Service Provider Id is same as Sponsor-Identity. It is an AVP under the Sponsored-Connectivity-Data grouped AVP.
Media Type	Applicable Media-Type (session level or specific to Media-Component-Description). Select from drop-down list. The list includes Audio Video Data Application Control Text Message and Other.

Dynamic Rule Charging Parameter

The Dynamic Rule Charging Parameters allows you to configure different charging parameters for the Rx dedicated bearers. Charging parameters are defined for dynamic PCC rules so that the service provider can properly charge for the traffic. For each Media-Sub-Component grouped AVP under Media-Component-Description grouped AVP in an AAR request PCRF installs a dynamic charging rule. The charging parameters for these dynamic PCC rules are not included in the AAR message so they are pulled out from the configuration.

Figure 63: Charging Parameters



Charging Parameters

Service Identifier	Rating Group	Online	Offline	Metering Method	Reporting Level	Precedence	AF Application Identifier Pattern	Media Type
1	2	ENABLE	DISABLE	VOLUME	SERVICE_IDENTIFIER_LE	2000	AUDIO_RL0	AUDIO
2	1	ENABLE	DISABLE	DURATION	RATING_GROUP_LEVEL	3000	AUDIO_RL1	AUDIO
1	2	ENABLE	DISABLE	DURATION	SERVICE_IDENTIFIER_LE	1111	VIDEO_RL0	VIDEO
1	2	ENABLE	DISABLE	VOLUME	RATING_GROUP_LEVEL	2222	VIDEO_RL1	VIDEO
1	2	ENABLE	DISABLE	VOLUME	SERVICE_IDENTIFIER_LE	7777	TEXT_RL10	TEXT
1	2	ENABLE	DISABLE	DURATION	RATING_GROUP_LEVEL	5555	TEXT_RL1.*	AUDIO

In the **Charging Parameters** table, you can define the parameter values in all the columns including the values for the key parameters such as - **AF Application Identifier Pattern** and **Media Type**.

The **AF Application Identifier Pattern** parameter contains information that identifies the particular service that the AF service session belongs to. This information may be used by the PCRF to differentiate QoS for different application services. You can specify regular expressions for this parameter as needed.

Default Charging Parameters

Defines the default values for the charging parameters under Charging-Rule-Definition grouped AVP to be used in case there's no match in the Charging Parameters table. This configuration is optional. Default value is unchecked.

For description of different parameters under Dynamic Rule Charging Parameters refer to Table 75: Sponsor Data Charging Parameters, on page 169.

Note

- An empty value being selected in either of Online Offline or Metering Method drop-boxes means no value is defined for that attribute so it will not be added to the Charging-Rule-Definition grouped AVP. Default value for all these three attributes is empty.
- The same parameters can be configured using an RxChargingParameterSTGConfiguration service configuration object.

Rx STG Lookup Binding

In the **Rx STG lookup binding** you can define the STG that is based on Rx media information (such as, media-type, af-application-id, and so on) and specify the mappings for binding the CRD columns to input and output AVPs.

CPS evaluates the CRD tables defined under **Rx STG lookup binding** using the media information available in the rx-sessions after the evaluation of all CRDs by the framework.

The following parameters can be configured under **Rx STG lookup binding**:

Table 76: Rx STG lookup binding Parameters

Parameter	Description
Name	The name of the Rx STG lookup binding.
Stg Reference	Reference to the Search Table Group containing the CRD tables that defines parameters for Rx specific media information.
List Of Input Column Avp Pairs	Defines the mapping between the AVP Names and the key Columns defined in the selected STG. These AVPs are inputs while evaluating the CRD table in STG. • Avp Name: Name of the diameter AVP (received in Media Component Description AVP of the AAR message) which is to be used as input for CRD table evaluation. For example, Media-Type, AF-Application-Identifier, and so on. • Column: Reference to the key column in STG corresponding to the specified AVP.
List Of Output Column Avp Pairs	Defines the mapping between the AVP Names and the output columns defined in the STG selected. These mapping indicate how the output column's values are mapped to AVPs after the CRD is evaluated. • Avp Name: The name/code of the Rx CRD AVP that is created for the output column. The Rx CRD AVP stores the information related to the media (media-type, mcd number, rx-session-id, and so on). There are multiple such AVPs with same code for the evaluated MCDs. • Column: Reference to the output column defined in the STG selected.

Evaluation of STGs defined in **Rx STG lookup binding** (evaluated for each media in the Rx session) creates multiple **Rx CRD result AVP** for each configured output column. Along with the code and CRD output value, this result AVP also stores the media component details such as, Media-Component-Number, Media-Type and Rx session-id. This information can be used for creating conditions (for example, An Rx CRD result Avp exists).

Rule Retry Profiles

CPS can be configured to selectively re-attempt to install rules that fail to install or activate. Upon receipt of a Charging-Rule-Report indicating the failure to install or activate one or more rules CPS will evaluate the failed rules and take further action.

CPS decides whether to reinstall a failed rule based on the Rule Retry Profile configured for the rule. The configuration of this Rule Retry behavior takes place in the Rule Retry Profile screen in Policy Builder.

- CPS will not re-attempt to install a failed rule unless the rule has a Rule Retry Profile associated with it. If no Rule Retry Profile is configured the rule status and failure code are updated immediately and no attempt to install the rules is made. This is the default behavior.
- If the Rule Retry Profile is configured but the reported rule failure code does not match any of the failure codes defined in the associated Rule Retry Profile the rule status and failure code are updated immediately and no attempt to install the rules is made regardless of the status of the other parameters.
- The rule status is not updated until the last retry fails.

Create a Rule Retry Profile

Step 1 Login to Policy Builder.

Step 2 Go to **Reference Data** > **Rule Retry Profiles**.

Step 3 From the right pane, click **Rule Retry Profile** under **Create Child** to open a Rule Retry Profile.

The following parameters can be configured for each Rule Retry Profile:

Table 77: Rule Retry Profile Parameters

Parameter	Description
Retry Interval	The number of seconds to wait before retrying to install a rule. See also Backoff Algorithm parameter. Default: 10 seconds **Note** If the value is less than 15 seconds, then the retries are scheduled at second level granularity. If the value is greater than 15 seconds, then granularity is in minutes. For example, if the interval is configured as 30 seconds, the timer may expire within 30 sec + 1 min approximately.

Parameter	Description
Max Retry Attempts	The maximum number of retry attempts to make. When CPS reaches this maximum retry value without successfully installing the rule the rule status and failure code are updated immediately and no further attempts are made to install the rule. Note This value does not include the initial installation attempt that is reported as failed but only the subsequent attempts. Default: 3
Backoff Algorithm	The algorithm to be used for calculating the time between retries. CONSTANT_INTERVAL Each retry is scheduled after an interval equal to Retry Interval seconds since the last report. LINEAR_INTERVAL Each retry is scheduled after an interval equal to Retry Interval x Current Attempt Number seconds since the last report. Default: CONSTANT_INTERVAL
Rule Failure Code	Select the failure codes for which CPS retries as specified in 3GPP TS29.212 v11.10 Section 5.3.38 Rule-Failure-Code AVP. Click **Add** then select one or more failure codes from the drop down menu. Click **Add** to include them to the list. Click **OK** when you are done. If no Rule Failure Code is specified, then CPS retries regardless of the failure code reported.
Name	Enter a unique name for this Rule Retry Profile. This name is used to associate Rules to this Rule Retry Profile.
Max Retry Interval	Enter the maximum time in seconds between the first and the last retry. If set to zero, the PCRF does not enforce a time limit for sending the retry messages. Default: 0 (zero)

Parameter	Description
Cisco Event Failure code	When a Cisco-CC-Failure-Type AVP is received to report Gy failure, CPS matches the Cisco-CC-Failure-Type AVP value in the diameter message CCR-Update with the Cisco Event Failure Code for the rule. If the value matches, then CPS retries the rule. Cisco Event Failure Code supports all values of type Unsigned32 from PGW. The following are some examples values for the Cisco Event Failure code: • 0 - CC_CONNECTION_FAILURE • 1 - CC_RESPONSE_TIMEOUT • 3* - 3xxx Protocol Error result-codes (For example, 3004 - DIAMETER_TOO_BUSY) • 4* - 4xxx Transient Failure result-codes (For example, 4002 - DIAMETER_OUT_OF_SPACE) • 5* - 5xxx Permanent Failure result-codes (For example, 5001 - DIAMETER_AVP_UNSUPPORTED) For more information on codes, refer to RFC 3588.
Enable Profiles Based On Failure Code	This check box is used to configure profiles based on failure codes. By default, this checkbox is not selected. For more information, refer to Profile Based On Failure Code, on page 175.

If there is still time to retry a rule installation (First Retry Time + Max Retry Interval <= Current Time) then the rule status and failure code are not updated immediately such that no policy change based on rule failure status is triggered.

Profile Based On Failure Code

This table is used to override the attributes Retry Interval, Backoff Algorithm, Max retry Attempts, and Max Retry Interval of generic profile which is already available.

CPS uses the following columns to select a row from this table:

- Cisco Event Failure Code
- Rule Failure Code
- Sy Realm

Note

- Cisco Event Failure Code or Rule Failure Code column value is mandatory to select the row. If both has Null values, then CPS ignores that row.
- If Sy session exist, then only CPS considers Sy Realm column value. There is no need to add a value if you do not want to consider SyRealm.
- If there is no value configured for Retry Interval, Backoff Algorithm, Max retry Attempts, and Max Retry Interval columns for a selected row in the table then CPS sets those attributes with already existing field values present under generic **Rule Rety Profile**.

Sy Realm Value

This parameter is used to derive SyRealm from CRD. User has to select CRD output column so that SyRealm value is pulled from the CRD table. If there is no Sy realm value derived from this field, then CPS tries to get the realm information from local Sy session.

The CRD output column values takes precedence over local Sy session.

Associate a Rule Retry Profile with a Rule

Each type of Service Configuration Object Rule in CPS (PreDefinedRule PreDefinedRuleBase PreConfiguredRule) can be associated with the Rule Retry Profile created in the previous section.

Step 1 In Policy Builder select the **Services** tab.

Step 2 From the left pane select **Services**.

Step 3 Expand **Service Options** tree.

Step 4 Select and expand your service option.

Step 5 Select the service option object.

Step 6 In the Service Option screen select the Service Configuration object. A Rule Retry Profile can be referenced only from a **PreDefinedRule**, **PreDefinedRuleBase** or a **PreConfiguredRule** service configuration object.

Step 7 Select the **Value** cell corresponding to the **Retry Profile**.

Step 8 Click the "…" button.

Step 9 Select the Rule Retry Profile from the popup window then click **OK**.

Step 10 Click **OK**.

For more details about how to define a service option refer to Services chapter.

CHAPTER 5

Interface Configuration

Gx Interface Configuration

This procedure describes how to create a Gx service in which the PCRF mirrors the QoS received from the PCEF/Gateway. When the PCRF receives a Credit-Control-Request (Initial) message, it sends the same QoS parameters back to the PCEF in the Credit-Control-Answer (Initial) message.

Step 1 Open Policy Builder, and select the **Services** tab.

Step 2 In the left-hand pane, select **Use Case Templates** > **Summary**.

Step 3 In the **Summary** pane, click **Use Case Template** under **Create Child**, and then do the following:

a) In the **Name** field, type `MirrorQoS` (using this name for example Use Case Template).

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.
The **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select **DefaultBearerQoS**.

e) Click **OK**.
The **Select Service Configuration** dialog box closes, and the DefaultBearerQoS object is displayed under **Service Configurations**.

f) Click **Add** again under **Service Configurations**.

g) In the **Select Service Configuration** dialog box, scroll down to the **gx** section, and select **DefaultBearerQoSActions**.

h) Click **OK**.

Now both added service configuration objects are displayed under **Service Configurations** pane.

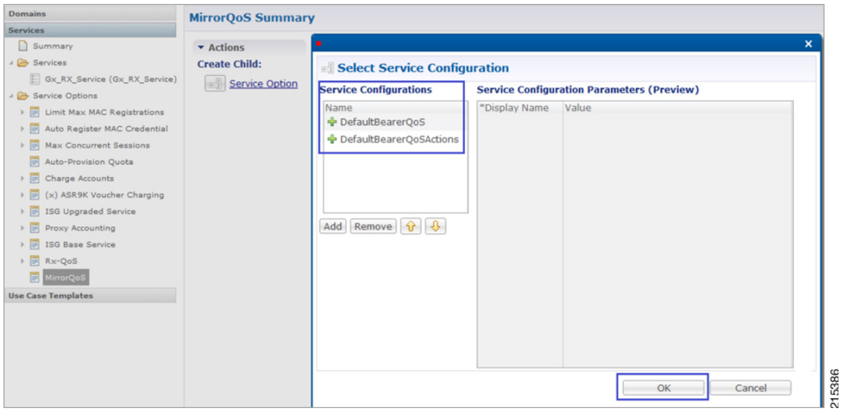
Step 4 From the left-hand pane, select **Services** > **Service Options**.

The new *MirrorQoS* option is displayed at the bottom of the list of service options.

Step 5 Select **MirrorQoS** in the **Service Options** list, and do the following:

a) In the **MirrorQoS Summary** pane, click **Service Option** under **Create Child**.
The **Select Service Configuration** dialog box opens. Both of the service configuration objects that you added are listed under **Service Configurations**.

Figure 64: Mirror QoS Summary



Name
DefaultBearerQoS
DefaultBearerQoSActions

*Display Name	Value

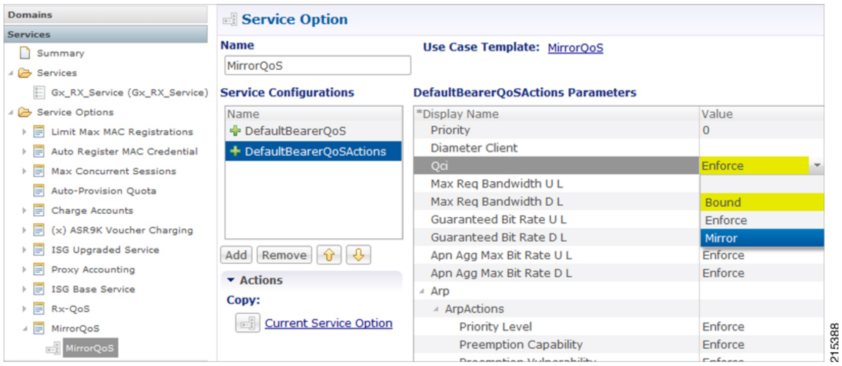
b) Click **OK**.

c) Type **`MirrorQoS`** in the **Name** field.

d) Under **Service Configurations**, select **DefaultBearerQoSActions**.
The DefaultBearerQoSActions parameters are displayed to the right.

e) In the **Value** column, select **Mirror** for all of the attribute value pairs.

Figure 65: Mirror QoS Summary - Service Option



Name: MirrorQoS

Use Case Template: MirrorQoS

Name
DefaultBearerQoS
DefaultBearerQoSActions

*Display Name	Value
Priority	0
Diameter Client	
Qci	Enforce
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guaranteed Bit Rate D L	
Apn Agg Max Bit Rate U L	Enforce
Apn Agg Max Bit Rate D L	Enforce
Arp	
ArpActions	
Priority Level	Enforce
Preemption Capability	Enforce

Step 6 In the left-hand pane, select **Services** > **Services**.

Step 7 In the **Services Summary** pane, click **Service** under **Create Child**, and do the following:

a) Type a descriptive code for the MirrorQoS service in the **Code** field.

b) Type **`MirrorQoS`** in the **Name** field.

c) Uncheck the **Balance Service** option.

d) Click **Add**.

e) In the **Select Service Configuration** dialog box, select the MirrorQoS service option, and click **OK**.

Step 8 Select **File** > **Publish to Runtime Environment**.

The new MirrorQoS service is now available to all Policy Server (QNS) nodes for processing.

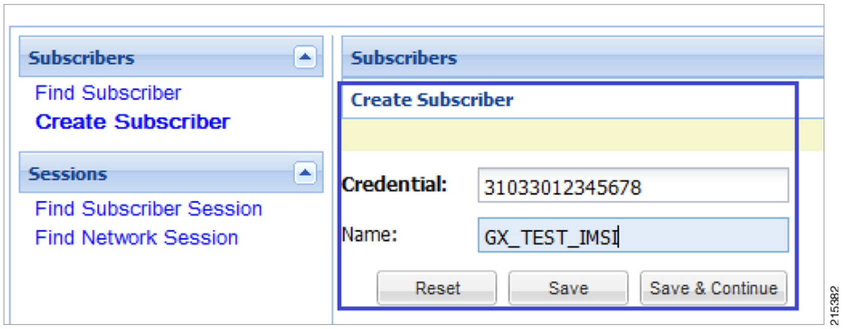
Step 9 Verify that the newly created service is available for use by doing the following:

a) Open the Control Center GUI and go to the **Subscribers** section.

b) Click **Create Subscriber**.

c) Enter the IMSI/MSISDN and the name of the subscriber, and then click **Save & Continue**.

Figure 66: Create Subscriber



Credential: 31033012345678

Name: GX_TEST_IMSI

d) Go to the **Services** section.

e) Click the **Add** section, which lists the available services, and select the new MirrorQoS service.

f) Click **Save** and run a test call to verify that the QoS parameters are mirrored by PCRF in Credit-Control-Answer(Initial) message back to the PCEF.

Gy Interface Configuration

The Diameter Gy reference point is located between the OCS and the PCEF. The CPS supports using the Gy reference point for usage monitoring of the on-board OCS known as the Multi-service Balance Manager (MsBM) against a PCEF.

CPS uses the Gy RatingGroup Service Configuration Object within the Use Case Templates to hold the configuration parameters for Gy. The following procedure describes how to set up a Gy RatingGroup that will be sent upon a CCR-i request from the PCEF. The Gy RatingGroup service option would then be added to a service along with a Gx rule or QoS.

For more information, see Gx Interface Configuration, on page 177 for details on how to create a valid Gx service.

The following procedure is based on the ASR5K acting as the PCEF supporting the Enhanced Charging Service (ECS) mechanism for Gy "Pull" Usage Monitoring. The RatingGroup configuration for Gy will work in a similar method with any supported PCEF using the Gy interface.

Step 1 Open the Policy Builder GUI, and select the **Services** tab.

Step 2 In the left-hand pane, select **Use Case Templates** > **Summary**.

Step 3 In the **Summary** pane, click **Use Case Template** under **Create Child**, and then do the following:

a) In the **Name** field, type **Gy**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.
The **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gy** area in the list of service configuration objects, and select **RatingGroup**.
The **Select Service Configuration** dialog box closes, and the RatingGroup object is displayed under **Service Configurations**.

Step 4 In the left-hand pane, select **Services** > **Service Options**.

The new Gy option is displayed at the bottom of the list of service options.

Step 5 Select **Gy** in the **Service Options** list, and do the following:

a) In the **Gy Summary** pane, click **Service Option** under **Create Child**.
The **Select Service Configuration** dialog box opens. The RatingGroup service configuration object is listed under **Service Configurations**.

b) Click **OK**.

c) Type `Gy` in the **Name** field.

d) Under **Service Configurations**, select **RatingGroup**.
The RatingGroup parameters display to the right.

The following table describes the parameters that are necessary to support the ASR5000 ECS Usage Monitoring for a volume quota service:

Table 78: RatingGroup Parameters

Parameter	Description
Rating Group	Corresponds to a value configured on the ASR5000 that represents which data should be monitored.
RG Type	Rating Group Type supports one of two values either “volume” or “time”.
Dosage	How much quota to initially give the client (in bytes).
Balance Code	
Final Unit Action	In this example, we will use TERMINATE as the default Final Unit Action on quota depletion, which will send a CCR-u with the final usage for the rating group. Other options supported include NONE (no action taken) RESTRICT_ACCESS (send a Restriction Filter Rule and Filter ID) and REDIRECT (send a Redirect Address of Redirect Address Type).
Validity Time	Sets a session timer for the Gy quota grant; even if quota is not exhausted the PCEF must check back in at the end of the validity time (in seconds).
Volume Quota Threshold	PCEF will check back in with OCS when the Volume Quota Threshold has been reached; value must be set as less than the overall Dosage (in bytes).
Quota Holding Time	The amount of time the quota should be available on the PCEF without activity from the user (in seconds)
Quota Consumption Time	Idle traffic threshold time (in seconds); only used with time quota rating groups.

Parameter	Description
Use Shared Bucket	Used in a shared quota use case in which the same account balance and rating group can be used within a shared group of users. Default: false

Priority and Diameter Client do not need to be set. Priority can be used to set the priority for the RatingGroup if multiple RatingGroups are on a service.

Tariff Switch Model and Tariff Change Time are outside the scope of this document.

Note If Tariff Switch Model is not set, any value set in Tariff Change Time is ignored.

Step 6 Validate the Gy service configuration as follows:

a) Create a new service in Policy Builder that contains a Gx rule service configuration and the Gy RatingGroup service configuration.

Note The Gx rule must be a rule defined on the PGW that is associated with a Gy service to the CPS as the OCS.

b) Per the Gy pull model, when the PCEF receives the appropriate Gx rule, it initiates a CCR-i to the OCS, which will reply back with the RatingGroup service option values in a CCA.

c) Using **tcpdump**, verify that the CCA contains the appropriate values as defined in the RatingGroup.

Sy Interface Configuration

The Sy reference point is located between the Policy and Charging Rules Function (PCRF) and the Online Charging System (OCS). The Sy reference point enables the transfer of information relating to subscriber spending from OCS to PCRF and supports the following functions:

- Request of policy counter status reporting from PCRF to OCS
- Notifications of policy counter status change from OCS to PCRF
- Cancellations of policy counter status reporting from PCRF to OCS

Since the Sy interface resides between PCRF and OCS in the HPLMN, roaming with home routed or visited access as well as non-roaming scenarios is supported in the same manner.

The following procedure describes how to subscribe to the OCS (Online charging system) counter status updates from the PRCF side by initiating a 'Spending Limit Request (SLR)' message:

Step 1 Open the Policy Builder GUI, and select the **Services** tab.

Step 2 Create a Gx service as described in Gx Interface Configuration, on page 177.

Now you are ready to create an Sy service as described in the following steps.

Step 3 In the left-hand pane, select **Use Case Templates** > **Summary**.

Step 4 In the **Summary** pane, click **Use Case Template** under **Create Child**, and then do the following:

a) In the **Name** field, type **`Sy`**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.
The **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **sy** area in the list of service configuration objects, and select **SpendingLimitReport**.

e) Click **OK**.
The **Select Service Configuration** dialog box closes, and the SpendingLimitReport object is displayed under **Service Configurations**.

Step 5 In the left-hand pane, select **Services** > **Service Options**.

The new Sy option is displayed at the bottom of the list of service options.

Step 6 Select **Sy** in the **Service Options** list, and do the following:

a) In the **Sy Summary** pane, click **Service Option** under **Create Child**.
The **Select Service Configuration** dialog box opens. The SpendingLimitReport service configuration object is listed under **Service Configurations**.

b) Click **OK**.

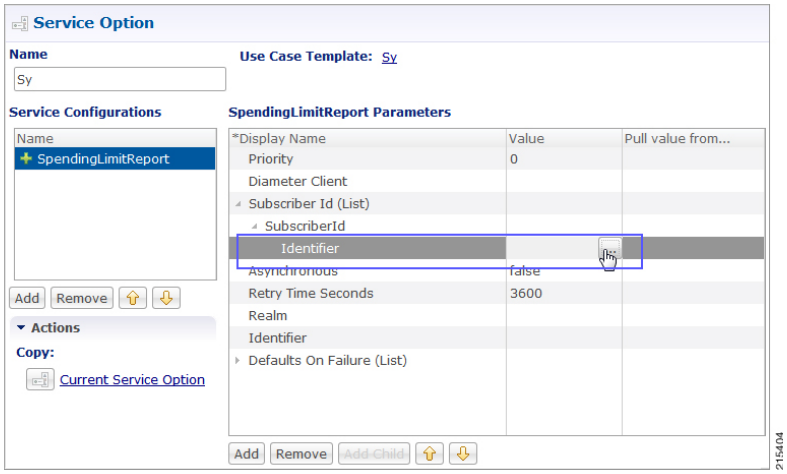
c) Type **`Sy`** in the **Name** field.

d) Under **Service Configurations**, select **SpendingLimitReport**.
The SpendingLimitReport parameters display to the right.

e) In the list of parameters, expand **Subscriber Id (List)** > **SubscriberId** parameter.
The **Identifier** parameter appears.

f) Click in the **Value** column beside the **Identifier** parameter, and then click the **...** button.

Figure 67: Identifier Parameter



Name: Sy

Service Configurations

Name
SpendingLimitReport

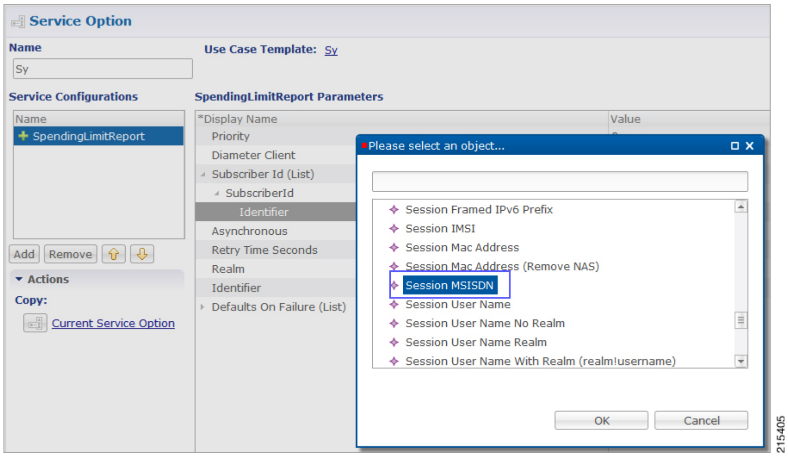
SpendingLimitReport Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Subscriber Id (List)		
SubscriberId		
Identifier	...	
Asynchronous	false	
Retry Time Seconds	3600	
Realm		
Identifier		
Defaults On Failure (List)		

A dialog box containing a list of identifiers opens.

g) Select **Session MSISDN** in the list, and click **OK**. Based on your requirements, you can also use other identifiers such as IMSI, and so on.

Figure 68: Session MSISDN Identifier



Service Option

Name: Sy

Use Case Template: Sy

Service Configurations

Name
SpendingLimitReport

SpendingLimitReport Parameters

*Display Name	Value
Priority	
Diameter Client	
Subscriber Id (List)	
SubscriberId	
Identifier	
Asynchronous	
Retry Time Seconds	
Realm	
Identifier	
Defaults On Failure (List)	

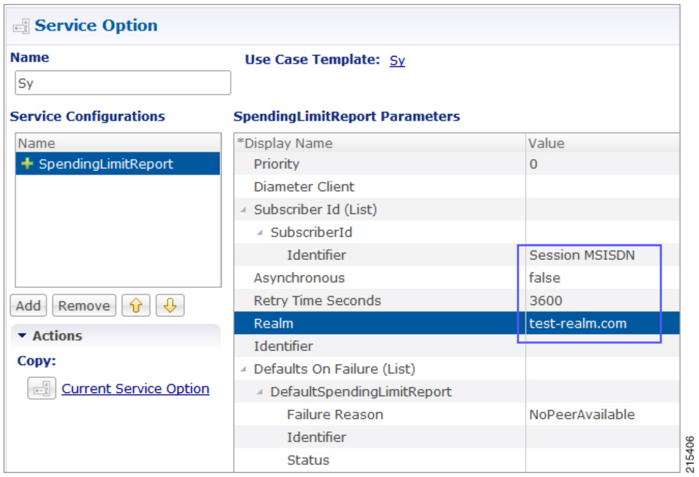
Please select an object...

- Session Framed IPv6 Prefix
- Session IMSI
- Session Mac Address
- Session Mac Address (Remove NAS)
- Session MSISDN
- Session User Name
- Session User Name No Realm
- Session User Name Realm
- Session User Name With Realm (realm!username)

h) Update the **Realm** parameter with the Sy peer realm (OCS Realm) where the message needs to be sent from PCRF.

In this configuration we are not specifying any counter name in the Identifier columns, which means that the PCRF subscribes to all the counter statuses available on the OCS for the subscriber.

Figure 69: Realm Parameter



Service Option

Name: Sy

Use Case Template: Sy

Service Configurations

Name
SpendingLimitReport

SpendingLimitReport Parameters

*Display Name	Value
Priority	0
Diameter Client	
Subscriber Id (List)	
SubscriberId	
Identifier	Session MSISDN
Asynchronous	false
Retry Time Seconds	3600
Realm	test-realm.com
Identifier	
Defaults On Failure (List)	
DefaultSpendingLimitReport	
Failure Reason	NoPeerAvailable
Identifier	
Status	

Step 7 In the left-hand pane, select **Services** > **Services**.

Step 8 In the **Services Summary** pane, click **Service** under **Create Child**, and do the following:

a) Type a descriptive code for the Sy service in the **Code** field.

b) Type `Sy` in the **Name** field.

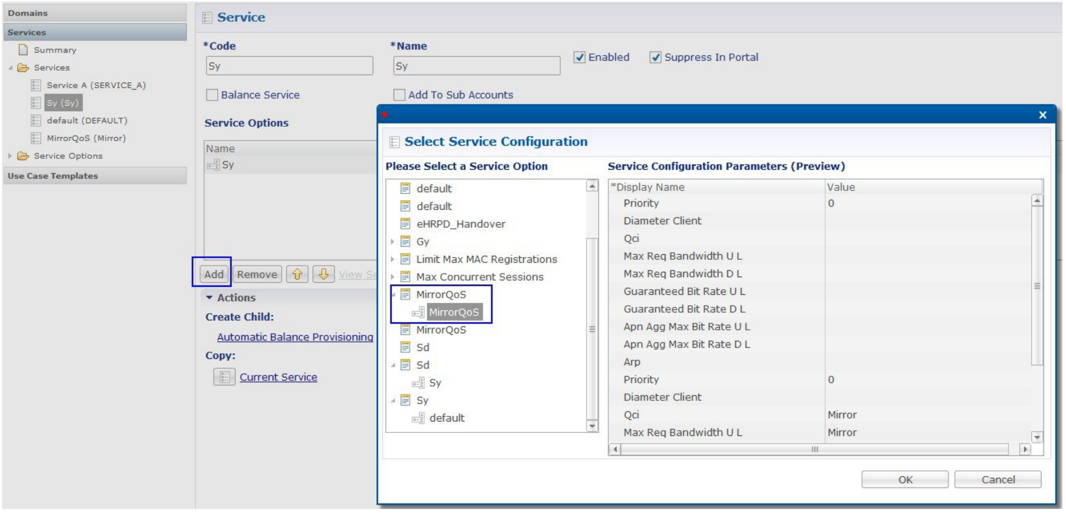
c) Uncheck the **Balance Service** option.

d) Click **Add**.

e) In the **Select Service Configuration** dialog box, select the Sy service option, and click **OK**.

f) Click **Add** again, select the MirrorQoS service option, and click **OK**.

Figure 70: Adding the Mirror QoS Service Option



Service

*Code: Sy

*Name: Sy

☑ Enabled ☑ Suppress In Portal

□ Balance Service □ Add To Sub Accounts

Service Options

Name
Sy

Select Service Configuration

Please Select a Service Option

Service Configuration Parameters (Preview)

*Display Name	Value
Priority	0
Diameter Client	
Qci	
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guaranteed Bit Rate D L	
Apn Agg Max Bit Rate U L	
Apn Agg Max Bit Rate D L	
Arp	
Priority	0
Diameter Client	
Qci	Mirror
Max Req Bandwidth U L	Mirror

- By adding the Gx interface 'MirrorQoS' service, PCRF will mirror the QoS for this subscriber.
- By adding the Sy interface 'Sy' service, PCRF will subscribe with OCS for all the counters per user.
- Both Gx/Sy service options together will generate a successful end-to-end subscriber call.

Step 9 Select **File** > **Publish to Runtime Environment**.

The new Sy service is now available to all Policy Server (QNS) nodes for processing.

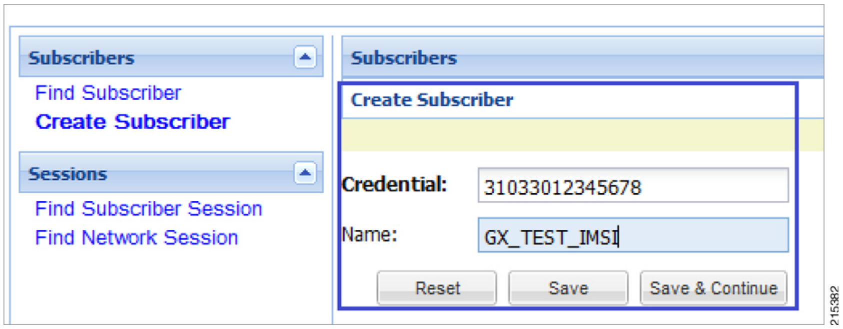
Step 10 Verify that the new Sy service is available for use by doing the following:

a) Open the Control Center GUI and go to the **Subscribers** section.

b) Click **Create Subscriber**.

c) Enter the IMSI/MSISDN and the name of the subscriber, and then click **Save & Continue**.

Figure 71: Create Subscriber



Credential: 31033012345678

Name: GX_TEST_IMSI

d) Go to the **Services** section.

e) Click **add** to open **Select Service** pop-up box which lists the available services. Select the new Sy service.

Figure 72: Select New Service - 1

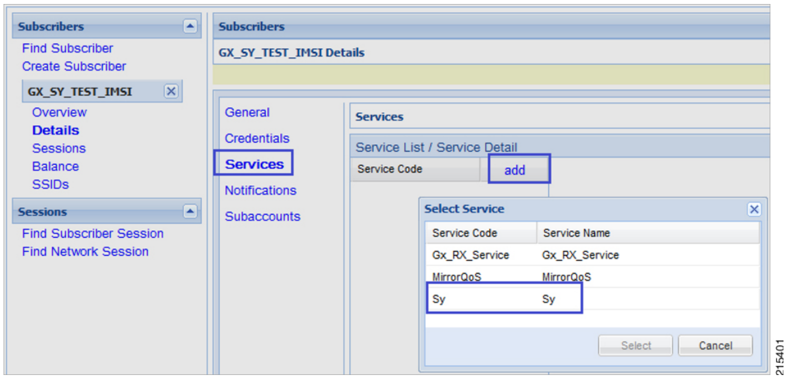
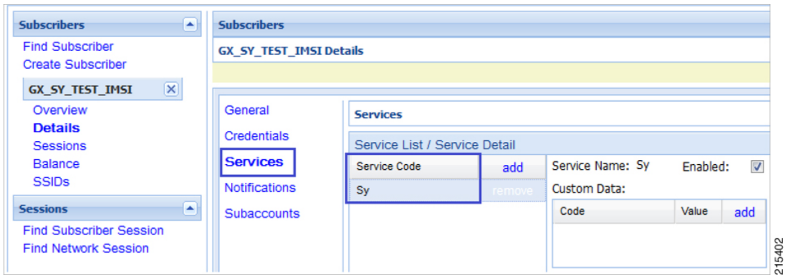


Figure 73: Select New Service - 2



f) Click **Save** and run a test call to verify the following:

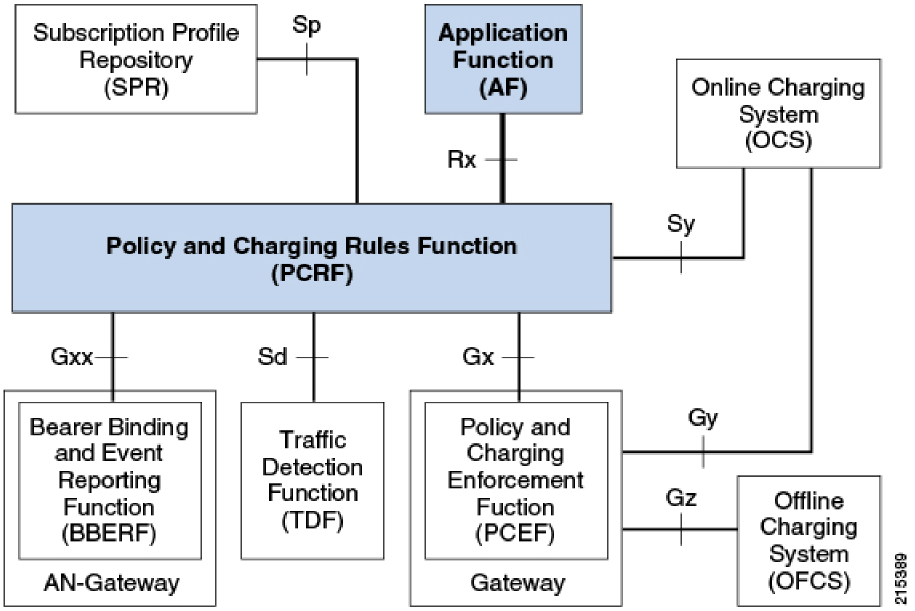
- QoS parameters are mirrored by PCRF in Credit-Control-Answer (Initial) message back to the PCEF.
- PCRF sends a Spending Limit Request message to the PCS on the Sy interface receives Spending Limit Answer message from the OCS.

Rx Interface Configuration

The Rx reference point is used to exchange application-level session information between the Policy and Charging Rules Function (PCRF) and the Application Function (AF). This information is part of the input used by the PCRF for the Policy and Charging Control (PCC) decisions.

The PCRF exchanges the PCC rules with the Policy and Charging Enforcement Function (PCEF) and QoS rules with the Bearer Binding and Event Reporting Function (BBERF).

Figure 74: Rx Reference Point


Subscription Profile Repository (SPR)
Sp
Application Function (AF)
Rx
Online Charging System (OCS)
Policy and Charging Rules Function (PCRF)
Sy
Gxx
Sd
Gx
Bearer Binding and Event Reporting Function (BBERF)
AN-Gateway
Traffic Detection Function (TDF)
Policy and Charging Enforcement Fuction (PCEF)
Gateway
Gy
Gz
Offline Charging System (OFCS)
215389

The PCRF provides network control regarding the service data flow detection gating QoS and flow based charging (except credit management) towards the PCEF. The PCRF receives session and media related information from the AF and informs AF of traffic plane events.

When a new AF session is being established and media information for this AF session is available at the AF and the related media require PCC supervision the AF shall open an Rx Diameter session with the PCRF for the AF session using an AA-Request command unless an Rx session has already been established for the AF session.

The AF shall provide the full IP address of the UE using either Framed-IP-Address AVP or Framed-Ipv6-Prefix AVP and the corresponding Service Information within Media-Component-Description AVP(s). The AF shall indicate to the PCRF as part of the Media-Component-Description whether the media IP flow(s) should be enabled or disabled with the Flow-Status AVP.

The AF may include the AF-Application-Identifier AVP into the AA-Request in order to indicate the particular service that the AF session belongs to. This AVP can be provided at both AF session level and Media-Component-Description level. When provided at both levels the AF-Application Identifier provided within the Media-Component-Description AVP will have precedence.

Use Case:

The following procedure describes how to configure the Rx parameters that are necessary for the establishment of a dedicated bearer and calculating/deriving the QoS for the Dynamic Charging rule names that PCRF sends to the PCEF using a Gx RARmessage:

Step 1 Open the Policy Builder GUI, and select the **Reference Data** tab.

Step 2 In the left-hand pane, select **Diameter Defaults**.

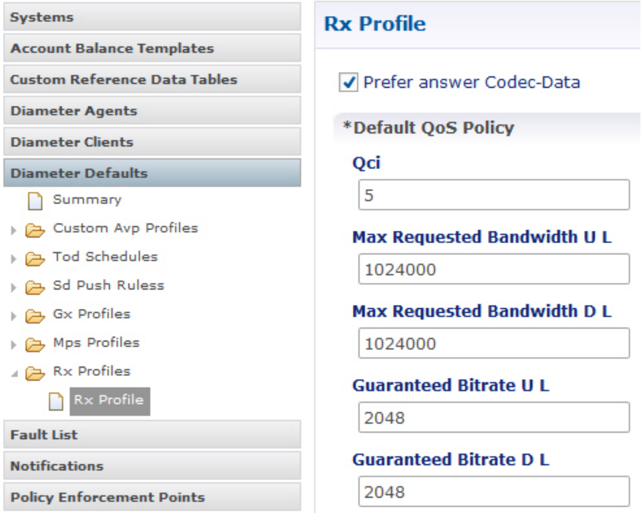
Step 3 In the **Summary** pane, click **Rx Profiles** under **Create Child**.

The Rx Profile configuration pane appears. When multiple Rx profiles are configured, the first profile should be configured as described in the following steps.

Step 4 Select **Prefer answer Codec-Data** if you want the default priority to be given to the answer codec (when both answer and offer are present within the AAR). This option is not selected by default.

Note CPS will by default select the first of offer or answer that is present in the sent XML. By selecting this checkbox, CPS will prefer answer regardless of the order sent by the Rx endpoint.

Figure 75: Rx Profile Configuration



Rx Profile

☑ Prefer answer Codec-Data

*Default QoS Policy

Qci: 5

Max Requested Bandwidth U L: 1024000

Max Requested Bandwidth D L: 1024000

Guaranteed Bitrate U L: 2048

Guaranteed Bitrate D L: 2048

Step 5 In the **Default QoS Policy** area, update the mandatory attribute value pairs as required.

Note The **Default QoS Policy** area is used when there is no Application QoS Policy or Codec QoS Policy defined, or when the incoming call doesn't match the configured values (with regard to AF ID or other parameters).

Note If AF Application Identifier (AF-ID)-specific QoS handling is needed, the Application QoS Policy table needs to be updated. If the AF-ID received in the AAR message from the AF matches the AF Application Identifier configured under the Application QoS Policy section, then the PCRF uses QoS attributes from this table to populate the dynamic rule QoS AVPs, which is then sent to the PCEF for dedicated bearer establishment.

Step 6 Scroll down to the **Actions** area in the **Rx Profile** pane, and click **Dynamic Rule Charging Parameters** under **Create Child**.

Step 7 Update the fields using one of the following methods as per requirements:

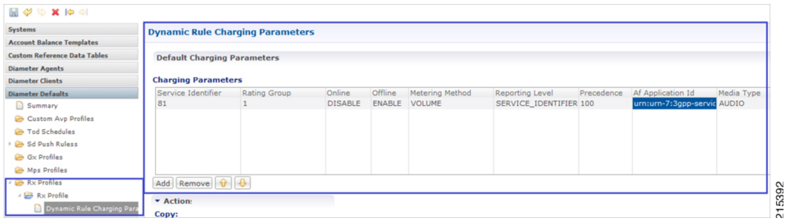
- Update the default Dynamic Rule Charging Parameters.

  Note This is used in case the provisioned values (AF Identifier based) do not match the incoming AAR message, essentially signifying that the AF ID in the AAR message is not provisioned or that the AAR message did not contain an AF Identifier.

- Update AF ID-specific Dynamic Rule Charging Parameters.

  Note This is used when the incoming AAR contains AF Identifier that is provisioned in the table shown in the following figure.

Figure 76: Dynamic Rule Charging Parameters



Dynamic Rule Charging Parameters

Default Charging Parameters

Charging Parameters

Service Identifier	Rating Group	Online	Offline	Metering Method	Reporting Level	Precedence	Af Application Id	Media Type
81	1	DISABLE	ENABLE	VOLUME	SERVICE_IDENTIFIER	100	urn:urn-7:3gpp-servic	AUDIO

Step 8 This configuration is applicable system wide or based on a particular Rx Client if needed. Validate the configuration by executing a basic VoLTE call with the standard Gx configuration. Verify that the CPS is able to handle the incoming AAR message on the Rx interface and can trigger dynamic charging rules on the Gx interface towards the PCEF using the RAR message.

Sd Interface Configuration

The Sd reference point is located between the Policy and Charging Rules Function (PCRF) and the Traffic Detection Function (TDF).

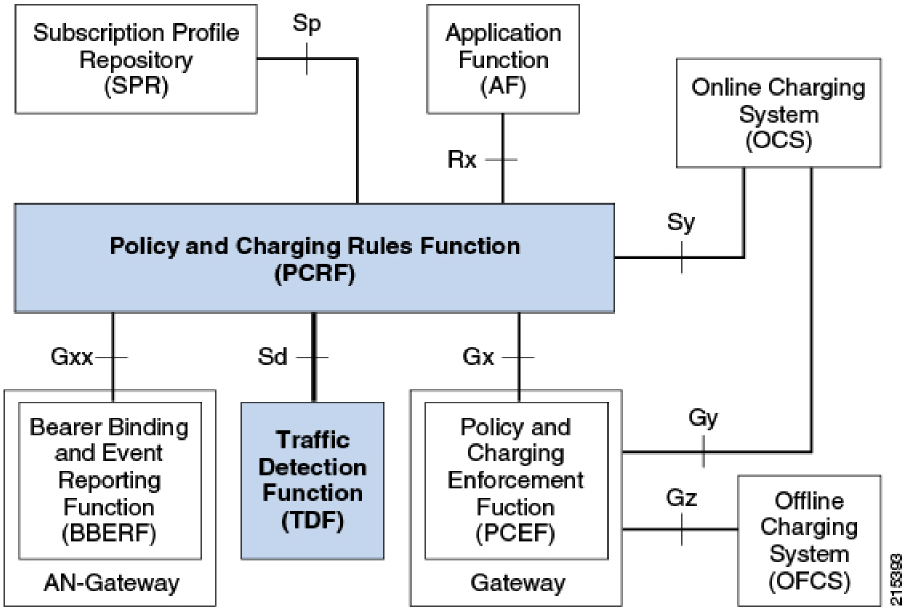
For the solicited application reporting the Sd reference point is used for:

- Establishment and termination of TDF session between PCRF and TDF.
- Provisioning of Application Detection and Control rules from the PCRF for the purpose of traffic detection and enforcement at the TDF.
- Usage monitoring control of TDF session and of detected applications and reporting of the start and the stop of a detected applications traffic and transfer of service data flow descriptions for detected applications if deducible from the TDF to the PCRF.

For the unsolicited reporting the Sd reference point is used for:

- Establishment and termination of TDF session between PCRF and TDF.
- Reporting of the start and the stop of a detected application's traffic and transfer of service data flow descriptions for detected applications if deducible and transfer of Application instance identifier if service data flow descriptions are deducible from the TDF to the PCRF.

Figure 77: Sd Reference Point


Subscription Profile Repository (SPR)
Sp
Application Function (AF)
Online Charging System (OCS)
Rx
Sy
Policy and Charging Rules Function (PCRF)
Gxx
Sd
Gx
Gy
Bearer Binding and Event Reporting Function (BBERF)
AN-Gateway
Traffic Detection Function (TDF)
Policy and Charging Enforcement Fuction (PCEF)
Gateway
Gz
Offline Charging System (OFCS)
215393

The PCRF may provide ADC Rules to the TDF by using Sd interface.

Once the start or stop of the application's traffic matching one of the ADC Rules is detected if PCRF has previously subscribed to the APPLICATION_START/APPLICATION_STOP Event-Triggers unless a request to mute such a notification (Mute-Notification AVP) is part of the corresponding ADC Rule the TDF shall report the information regarding the detected application's traffic to the PCRF and apply the enforcement actions if defined within the corresponding ADC Rule.

Use-Case:

The following procedure describes how to initiate an Sd session from PCRF towards the TDF by sending a Predefined ADC Rule using a TDF-Session-Request (TSR) message to the TDF and getting a successful TDF-Session-Answer (TSA) message on the PCRF:

Step 1 Open the Policy Builder GUI, and select the **Services** tab.

Step 2 Create a Gx service as described in Gx Interface Configuration, on page 177.

Now you are ready to create an Sd service as described in the following steps.

Step 3 In the left-hand pane, select **Use Case Templates** > **Summary**.

Step 4 In the **Summary** pane, click **Use Case Template** under **Create Child**, and then do the following:

a) In the **Name** field, type `Sd`.
b) Select **Actions** tab.
c) Click **Add** under **Service Configurations**.
The **Select Service Configuration** dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.
d) Scroll down to the **sd** area in the list of service configuration objects, and select **ADCPredefinedRule**.
e) Click **OK**.

The **Select Service Configuration** dialog box closes, and the ADCPredefinedRule object is displayed under **Service Configurations**.

Step 5 In the left-hand pane, select **Services** > **Service Options**.

The new Sd option is displayed at the bottom of the list of service options.

Step 6 Select **Sd** in the **Service Options** list, and do the following:

a) In the **Sd Summary** pane, click **Service Option** under **Create Child**.
The **Select Service Configuration** dialog box opens. The ADCPredefinedRule service configuration object is listed under **Service Configurations**.

b) Click **OK**.

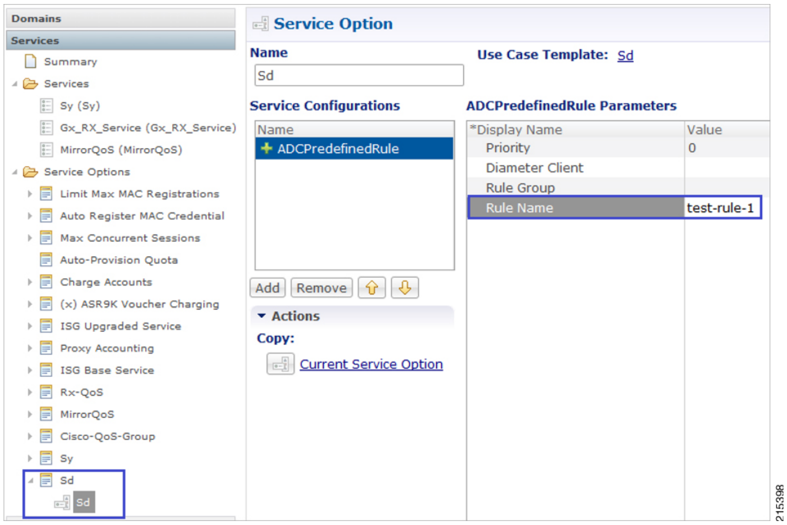
c) Type `Sd` in the **Name** field.

d) Under **Service Configurations**, select **ADCPredefinedRule**.
The ADCPredefinedRule parameters display to the right.

e) Click in the **Value** column beside the **Rule Name** parameter, and type the name of the ADC Rule that is provisioned on the TDF and that the PCRF needs the TDF to enforce. For this example, we used `test-rule-1`.

Note The rule that is being configured here MUST already be provisioned on the TDF, or the TDF will return an error (unknown rule name).

Figure 78: Rule Name parameter



Name: Sd

Use Case Template: Sd

Service Configurations

Name
ADCPredefinedRule

ADCPredefinedRule Parameters

*Display Name	Value
Priority	0
Diameter Client	
Rule Group	
Rule Name	test-rule-1

Step 7 In the left-hand pane, select **Services** > **Services**.

Step 8 In the **Services Summary** pane, click **Service** under **Create Child**, and do the following:

a) Type a descriptive code for the Sd service in the **Code** field.

b) Type `Sd` in the **Name** field.

c) Uncheck the **Balance Service** option (unless explicitly needed for the use case being developed).

d) Click **Add**.

e) In the **Select Service Configuration** dialog box, select the Sd service option, and click **OK**.

f) Click **Add** again, select the MirrorQoS service option, and click **OK**.

- By adding the Gx interface 'MirrorQoS' service, PCRF will mirror the QoS for this subscriber.

- By adding the Sd interface 'Sd' service, PCRF will trigger a TSR request with an ADC rule towards TDF.

- Both Gx/Sy service options together will generate a successful end-to-end subscriber call.

Step 9 Select **File** > **Publish to Runtime Environment**.
The new Sd service is now available to all Policy Server (QNS) nodes for processing.

Step 10 Select the **Reference Data** tab.

Step 11 In the left-hand pane, select **Diameter Defaults.** > **Summary**.

Step 12 In the **Summary** pane, click **Sd Push Rules** under **Create Child**.

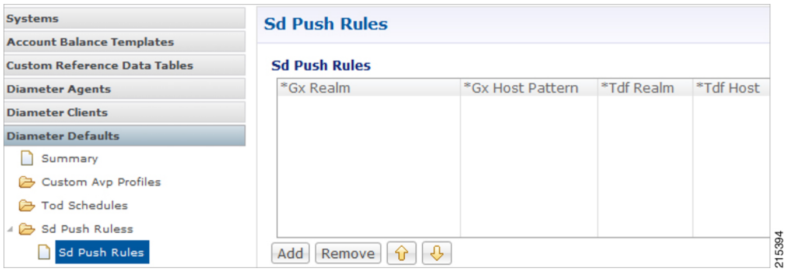
The **Sd Push Rules** pane appears.

In order to initiate connections toward the TDF on the Sd interface, the table shown in the following figure needs to be populated with the origin and remote Host/Realm configuration.

The Sd service/template will send messages to the TDF based on the host/realm configuration defined here.

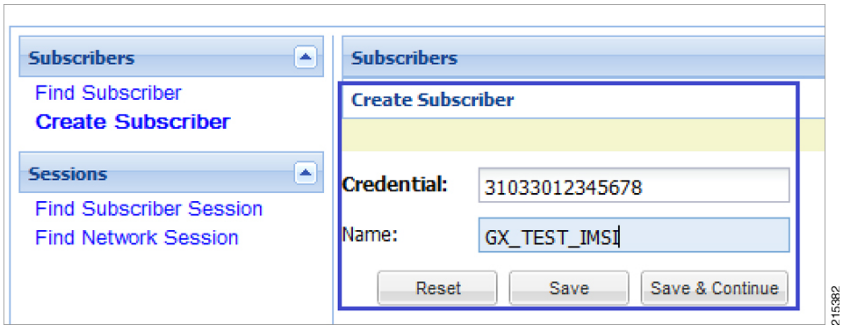
For more information on how to configure the parameters, see Diameter Defaults, on page 148.

Figure 79: Sd Push Rules Configuration Parameters



Step 13 Verify that the new Sd service is available for use by doing the following:

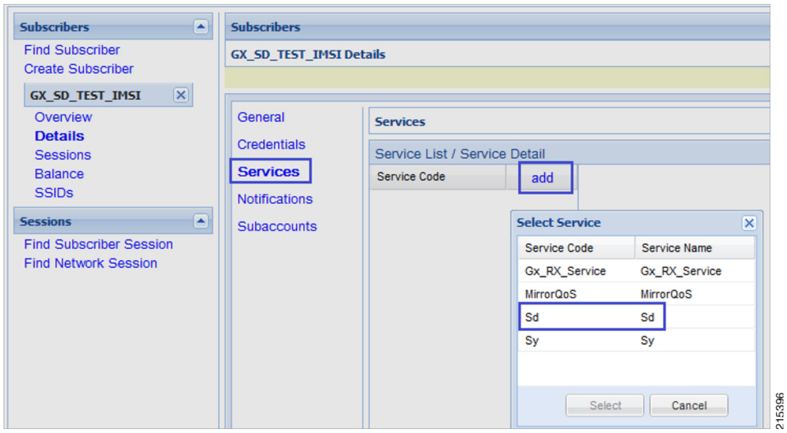
a) Open the control center GUI and go to the **Subscribers** section.
b) Click **Create Subscriber**.
c) Enter the IMSI/MSISDN and the name of the subscriber, and then click **Save & Continue**.



Credential: 31033012345678

Name: GX_TEST_IMSI

d) Go to the **Services** section.
e) Click **add** to open **Select Service** pop-up box which lists the available services, and select the new Sd service.



f) Click **Save** and run a test call to verify the following:

- QoS parameters are mirrored by PCRF in Credit-Control-Answer (Initial) message back to the PCEF.
- PCRF sends a TDF-Session-Request message to the TDF on the Sd interface (with the Predefined ADC rule), receives TDF-Session-Answer message from the TDF.

Sh Interface Configuration

CPS supports the ability to connect to the Home Subscriber Server (HSS) over the Sh interface to parse subscriber profile data in order to make policy decisions.

CPS queries the HSS on Gx session establishment and caches the subscriber data locally. CPS allows the operator to configure which attributes need to be extracted from the User-Data AVP and stored.

Create the Diameter Outbound Peer and Realm Connection to HSS

The connection to the HSS must be enabled by configuring it in the Outbound Peers section in the Diameter Stack configuration.

Refer to Outbound Peers, on page 113 for instructions.

Note When defining the Realm in the Realms table, enter the Processing Protocol as SH_TGPP.

Configure the Sh Domain

Sh interface connections in CPS are defined per domain and therefore are configured on the Domains screen in Policy Builder.

Refer to Domains, on page 197 for more information.

Note The following steps represent the most common way to configure an Sh interface connection, but other configuration options are available.

Step 1 Follow the steps in Defining the General Attributes of the Domain, on page 198 to create a new domain for the Sh Interface.

Step 2 On the **General** tab, set **Authorization** to **Allow all Users**.

Note While **Allow all Users** is the most common setting, CPS can be set to have subscribers in the SPR (USuM Authorization) and still use the Sh mechanism for additional profile data.

Step 3 On the **Provisioning** tab, set **Provisioning** to **<not set>**.

Step 4 On the **Advanced Rules** tab, select the appropriate service in the **Default Service** field. The default service applies to all subscribers' requests that hit the Sh domain.

Step 5 Continue with the instructions in Defining the Additional Profile Data of the Domain, on page 203.

Configure Multiple Sh Entitlements

Note Enabling this feature may result in CPS system performance degradation.

CPS can now receive and parse multiple values via Sh that use the same location in the data structure. These values are then resolved in conjunction with CRD tables to determine the service and appropriate AVPs to add to the session. This capability allows duplicate data structures to be processed and resolved rather than requiring unique data structures for all values, as was the case for CPS versions prior to 11.0.

The following example illustrates an incoming Sh response that contains multiple Entitlement and Custom AttributeName='4GPFO' values that are not unique. A maximum of five values from the incoming response will be used to determine a "bundled" result. The incoming values are processed against the CRD to compress them into a final result based on priorities.

```
<Sh-Data>
     <RepositoryData>
     <ServiceIndication>CamiantUserData</ServiceIndication>
     <SequenceNumber>0</SequenceNumber>
     <ServiceData><CamiantShUser xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xsi:noNamespaceSchemaLocation='CamiantShUser.xsd'>
     <![CDATA[<Version>1.0</Version>
     <AccountId>274500345196</AccountId>
     <Entitlement>RTA</Entitlement>
     <Entitlement>RTB</Entitlement>
     <Entitlement>RTC</Entitlement>
     <Custom AttributeName='BillingPlanCode'>L03</Custom>
     <Custom AttributeName='4GPFO'>THR200k200k</Custom>
     <Custom AttributeName='4GPFO'>THR200k300k</Custom>
     <UserId Type='E164' Scope='Public'>2345557890</UserId>
     <UserId Type='NAI'
Scope='Private'>0333444123456789@epc.mnc444.mcc333.3gpp.network.org</UserId>
     <EquipmentId Type='IMEISV' DeviceType='Phone'>35-209900-176148-23</EquipmentId>]]>
     </CamiantShUser>
```

```
        </ServiceData>
        </RepositoryData>
</Sh-Data>
```

This procedure describes how to configure Policy Builder to assign multiple entitlements to a subscriber, which allows services to be used in a more targeted manner.

Step 1 Log in to Policy Builder.

Step 2 Create a Search Table Group and a corresponding Custom Reference Data Table as follows:

a) Select the **Reference Data** tab.

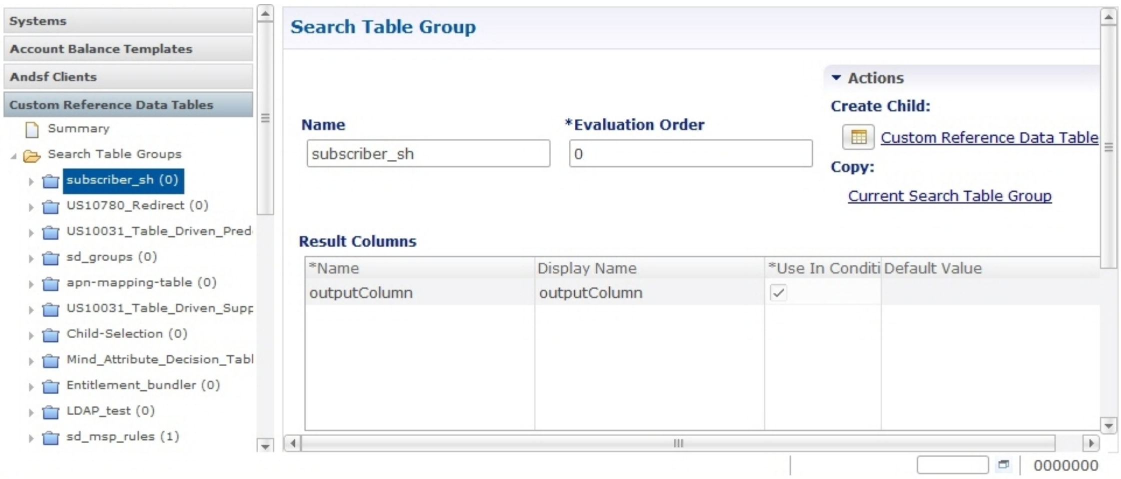
b) In the left pane, select **Custom Reference Data Tables**.

c) Click **Search Table Groups**.

d) In the **Search Table Groups Summary** pane, click **Search Table Group** under **Create Child**.

e) In the **Search Table Group** pane, type a name for the group; for example, **`subscriber_sh`**. An example is shown below:

Figure 80: Search Table Group



Name: subscriber_sh

*Evaluation Order: 0

Result Columns

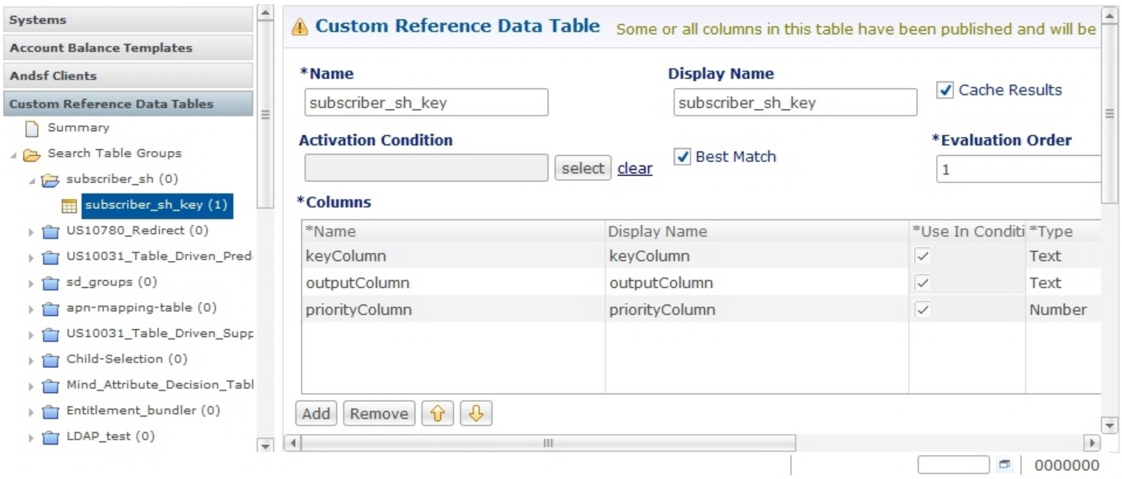
*Name	Display Name	*Use In Conditi	Default Value
outputColumn	outputColumn	✓	

f) Click **Custom Reference Data Table** under **Create Child**.

g) In the **Custom Reference Data** pane, type a **Name** for the CDR; for example, **`subscriber_sh_key`**.

h) Under **Columns**, add a key column, an output column, and a priority column. An example is shown below.

Figure 81: Custom Reference Data Table


Systems
Account Balance Templates
Andsf Clients
Custom Reference Data Tables
Summary
Search Table Groups
subscriber_sh (0)
subscriber_sh_key (1)
US10780_Redirect (0)
US10031_Table_Driven_Pred
sd_groups (0)
apn-mapping-table (0)
US10031_Table_Driven_Supp
Child-Selection (0)
Mind_Attribute_Decision_Tabl
Entitlement_bundler (0)
LDAP_test (0)
Custom Reference Data Table
Some or all columns in this table have been published and will be
select
clear
Add
Remove
0000000

*Name: subscriber_sh_key

Display Name: subscriber_sh_key

☑ Cache Results

Activation Condition:

☑ Best Match

*Evaluation Order: 1

*Columns

*Name	Display Name	*Use In Conditi	*Type
keyColumn	keyColumn	✓	Text
outputColumn	outputColumn	✓	Text
priorityColumn	priorityColumn	✓	Number

Step 3 Configure a bundle profile as follows:

a) Under **Custom Reference Data Tables** in the left pane, click **Bundle Profiles**.

b) In the **Bundle Profiles Summary** pane, click **Bundle Profile** under **Create Child**.

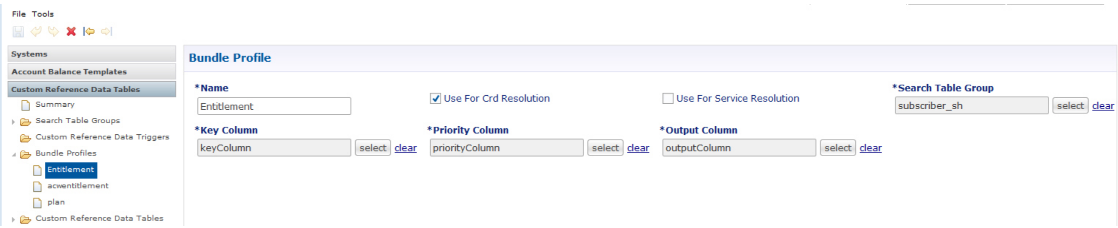
c) In the **Bundle Profile** pane, type a **Name** for the profile; for example, `Entitlement`.

d) If you want the bundle profile to apply to the CRD and/or Service Resolution processes, select **Use for Crd Resolution** and/or **Use for Service Resolution**.

e) In the **Search Table Group** field, type the name of the search table group.

f) In the **Key Column**, **Priority Column** and **Output Column** fields, use the **Select** button to select the names of the columns that were configured in the CRD table. An example is shown below:

Figure 82: Bundle Profile



*Name: Entitlement

☑ Use For Crd Resolution

□ Use For Service Resolution

*Search Table Group: subscriber_sh

*Key Column: keyColumn

*Priority Column: priorityColumn

*Output Column: outputColumn

Step 4 Configure the Sh Profile in a new domain or in an existing one:

a) Select the Policy Builder **Services** tab.

b) In the left pane, select **Domains**.

c) Select an existing domain under **Domains** to edit, or click **Domain** under **Create Child** in the **Service Reference Data Objects** pane to create a new one.

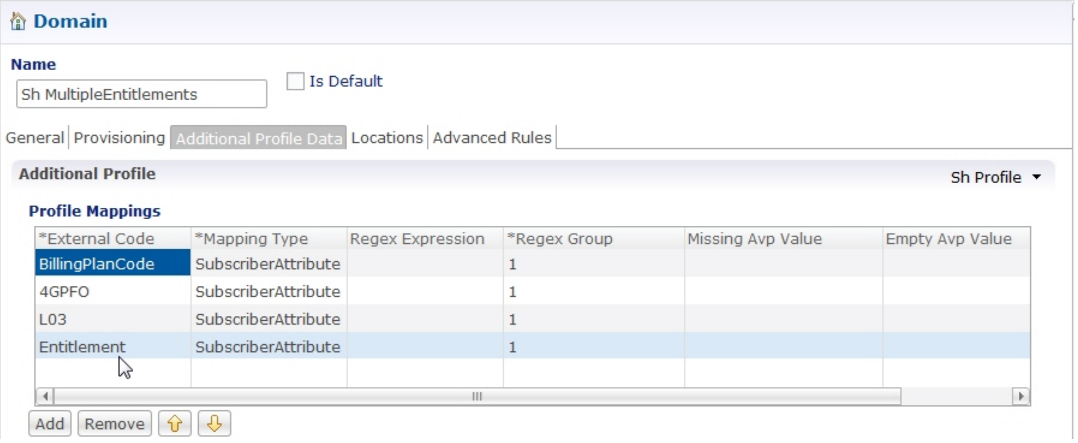
Note If this is a new domain type a name for it; for example, `Sh MultipleEntitlements`.

d) In the **Domain** pane, click the **Additional Profile Data** tab.

e) Select **Sh Profile** in the pull-down menu on the right-hand side of the **Additional Profile** section heading.

f) Under **Profile Mappings**, add a new **External Code** and name it using the bundle profile name; in our example, the bundle profile name is Entitlement. An example configuration is shown below:

Figure 83: External Code Configuration using Bundle Profile Name



Domain

Name

Sh MultipleEntitlements

□ Is Default

Additional Profile

Sh Profile ▾

Profile Mappings

*External Code	*Mapping Type	Regex Expression	*Regex Group	Missing Avp Value	Empty Avp Value
BillingPlanCode	SubscriberAttribute		1		
4GPFO	SubscriberAttribute		1		
L03	SubscriberAttribute		1		
Entitlement	SubscriberAttribute		1		

g) On rare occasions, you may want to select the **Use Service Indications For Service Resolution** option if you want the Service Indications to be put into the policy state for services resolution. Service Indications are used in the outgoing UDR/SNR to tell the HSS what data to send back to CPS.

Note If you decide to select this option, do so only after consulting with Cisco Advanced Services.

LDAP/Ud Interface Configuration

For more information on LDAP/Ud interface configuration, refer to Domains.

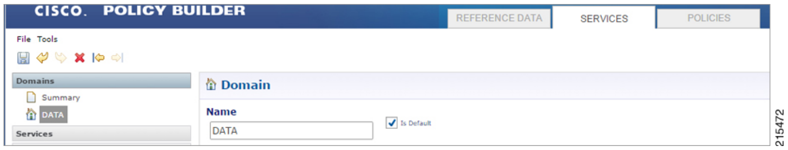
CHAPTER 6

Domains

Overview

The Access Point Network (APN) attribute is sent to the CPS PCRF on the diameter Gx CCR-I message or within the Gy CCR-I message. Generally, an operator will want to define specific subscriber profile rules and service definitions that apply to all subscribers that are attached to the given APN. Within CPS, the APN profile rules are defined in the Domains section of the Services tab is shown below:

Figure 84: APN Profile Rules



Name

DATA

☑ Is Default

The Domain definition within the system controls the following behavior:

- Retrieves the user profile from the CPS SPR database. This step is optional and depends upon whether the operator is storing subscriber profiles in the CPS SPR database.
- Retrieves a user profile from an external data source using the LDAP/Ud protocols or the Diameter Sh protocol.
- Defines the default service(s) that are assigned to a user's session under the given conditions. For information on services, Services, on page 229.

Strategies for Defining Domains

Two strategies can be used when creating Domains for APN profiles. These approaches are:

Step 1 Define one domain per logical APN. This approach is the most flexible and preferred approach for production deployments. The approach uses an APN mapping table to map the APN value to a logical APN. This allows all similar APNs to have the same profile. An example, is mapping "data_1" to "DATA".

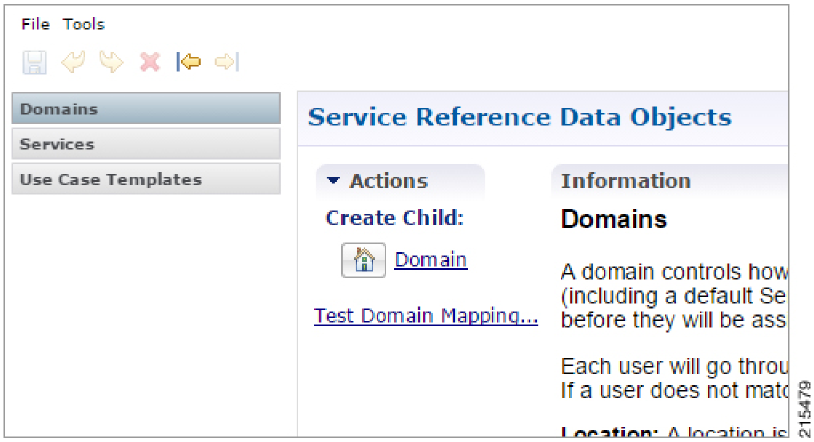
Note Definition of an APN to logical APN mapping table is required to utilize this strategy. Defining this mapping table is shown at the end of this chapter.

Step 2 Define one default domain for the system. This approach should only be used if multiple APNs are not defined or for proof of concept/demonstration environment systems.

Defining a Domain

Defining a domain requires selecting the **Domains** section on the **Services** tab and then clicking **Domain** in the right pane as shown below.

Figure 85: Defining a Domain



Domains

A domain controls how
(including a default Se
before they will be ass

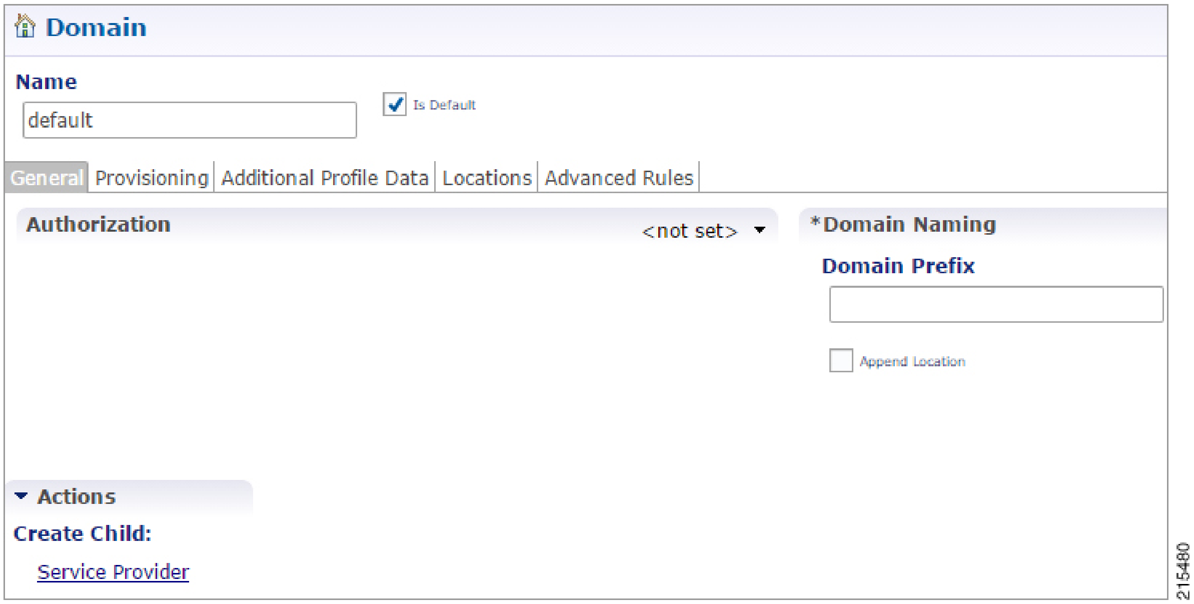
Each user will go throu
If a user does not matc

Location: A location is

Defining the General Attributes of the Domain

Once the **Create Child Domain** action is selected, the following screen appears for data entry:

Figure 86: Naming the Domain



Domain

Name

default

☑ Is Default

Authorization <not set>

*Domain Naming

Domain Prefix

□ Append Location

The following parameters can be configured on the **General** tab.

Table 79: General Tab Parameters

Parameter	Description
Name	This is a short textual name of the domain that describes the APN that is mapped into this domain node. For example, VoLTE would imply this domain contains all VoLTE sessions. This name should be short and descriptive for an end user to find the associated business rules. **Restriction** After a domain is defined changing the name of an APN invalidates all existing sessions attached to the APN. The system does not prevent name changes and as a result this restriction must be enforced as part of the business process in using the system. If a name change is required then impacted sessions must be deleted from the session data store manually.
Is Default	This indicates that this domain is the “default” domain if the incoming message does not map to any of the other domains. Restrictions The system must have at least one default domain to ensure that all new sessions map to a domain. The preferred approaches are (1) to create a default domain with a restricted service definition or (2) assign the default domain to the most common domain (for example, DATA).
Authorization	This section defines whether the local CPS SPR should be used for profile retrieval. There are a number of options that are available in this section to support non-mobile use cases. For more information, see Authorization, on page 200.

Authorization

The only valid options for use in a mobile configuration are:

- **USuM Authorization:** Select this option if a local CPS SPR lookup should be executed upon new session creation.

Figure 87: USuM Authorization Option

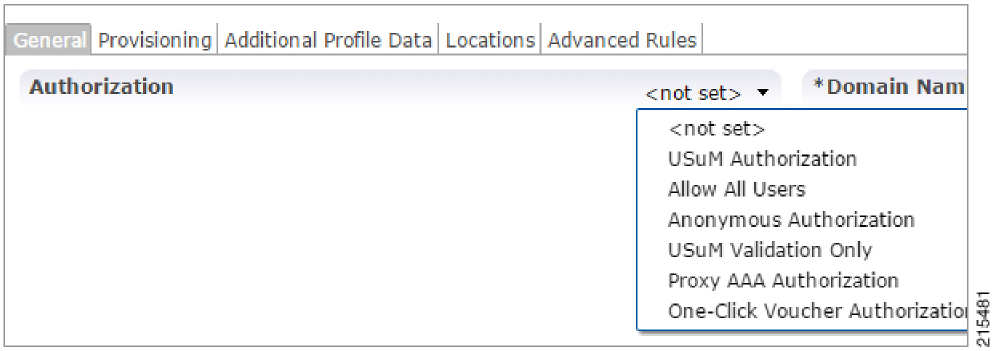
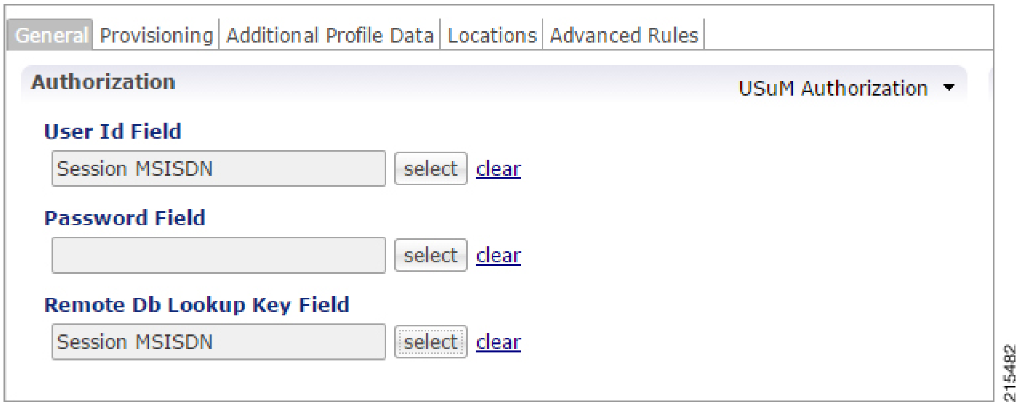


Figure 88: USuM Authorization Configuration



Authorization: USuM Authorization

User Id Field: Session MSISDN

Password Field:

Remote Db Lookup Key Field: Session MSISDN

The following parameters can be configured under **USuM Authorization**:

Parameter	Description
User ID Field	Set this to either **Session MSISDN** or **Session IMSI** depending on which credential is used to store the data in the SPR.
Password Field	Select the corresponding password for the User ID field selected.
Remove Db Lookup Key Field	This field is optional and should be used only in conjunction with USuM remote DB functionality. If this functionality is enabled, then the key field should match the user id field.

- **Allow All Users**: Select this option when defining an Sh interface Domain that will retrieve information from an HSS.

  See Configure the Sh Domain, on page 192 for more information.

All other options should not be used in a mobile configuration. One option must be selected.

Defining the Provisioning Attributes of the Domain

The **Provisioning** tab defines whether auto provisioning of subscribers within the SPR should occur. This method is generally used in scenarios where the system is configured to “auto-learn” subscribers and assign a default service profile.

For mobile configurations, set the attributes under the **Provisioning** tab as follows:

External Profile Cache

CPS uses the local SPR database (formerly referred to as the USuM database) to temporarily cache the subscriber profile fetched from an external data source (HSS/External-SPR) using the Diameter Sh interface. The cached subscriber record in the SPR database has the custom AVPs created for each attribute that is retrieved from HSS/External-SPR and mapped as per the Profile Mapping defined in the Sh Profile.

The following parameters can be configured:

- The **Primary Credential** field defines the primary key for the provisioned subscriber record (for example, IMSI, MSISDN, and so on.)
- The **Subscriber Validity Period (mins)** denotes the time (in minutes) for which the provisioned subscriber record is valid.

Note

- The **Subscriber Validity Period (mins)** is set only when the subscriber record is created the first time for that subscriber. This value is not changed if CCR-I (s) are received before the subscriber validity period expires. In case a CCR-I is received after the validity period has expired, the existing SPR cache record is deleted. Once the existing SPR record is deleted, a new UDR/UDA exchange happens and the subscriber validity period is updated along with the new SPR cache record.
- Since CPS creates a local CPS SPR to temporarily cache the subscriber's profile, and this impacts the overall response time. To reduce the impact, you need to configure Mongo database to use `tmpfs` for storage.
- You must consider the size of the database depending on the number or subscriber's profile to cache.
- For consistent profile updates across multiple sessions for the same subscriber, it is recommended to set the **DB Read Preference** drop-down list to **PrimaryPreferred** in **REFERENCE DATA** > **Systems** > **Plugin Configurations** > **USuM Configuration**.
- If the first session is created using UDR or UDA and the subscriber data is stored in the CPS SPR database, and if there is any change for the same subscriber's data in SPR/HSS, the change is not reflected for another Gx session for same subscriber. The new Gx session still refers to the cached subscriber profile.
- If this feature is enabled, you must not provision or delete the subscriber's profile using Control Center or Unified APIs.
- Domain naming configuration, if used, affects the subscriber's primary credential used for storing or accessing the profile in CPS SPR. Hence, you must configure it based on the desired unique identity for the subscriber.

- Select the **Use Remote SPR Databases** check box to enable CPS to use the remote SPR Mongo databases. CPS uses the primary credential (for example, IMSI/MSISDN extracted based on the retriever) and passes it as `remoteLookupKeyValue` when it performs the SPR look-up operation to create, update, or delete subscriber records in the CPS SPR databases for fetched external subscriber profiles.

Note

- This parameter takes effect only when **Remote Database Configuration** is configured in **USuM Configuration** under **Plugin Configuration**.

  See USuM Configuration, on page 58

- Enabling this parameter causes CPS to distribute the SPR operations across different SPR databases, thus using memory for each extra CPS SPR (remote) databases instance.
- If this feature is enabled for Geographic Redundancy deployment, the CPS SPR Mongo database must be local to each site and must not be replicated across sites. However, if additional SPR Mongo databases are present on a remote site, the latency between the two sites must be considered while defining the message timeout values.
- To create additional new mongo database instances, refer to chapter 'Deploy CPS VMs' in *CPS Installation Guide for VMware*.

- Select **Use origin-host for SPR lookup** to save or retrieve the Sh profile data to and from the appropriate SPR database based on Gx CCR-I origin-host pattern.

Note You need to select **Use Remote SPR Databases** in addition to **Use origin-host for SPR lookup**. For more information, see **Remote Database Configuration** under **USuM Configuration**.

Defining the Additional Profile Data of the Domain

Retrieving a Subscriber Profile from an HSS

For retrieving a connection from a Home Subscriber Server (HSS) it is necessary to define the data sets to enable the retrieval.

See Sh Interface Configuration, on page 192 for configuring the connection to the HSS.

Setting Up Additional Profile Data

Step 1 Complete the preliminary configuration in Sh Interface Configuration, on page 192.

Step 2 Click the **Additional Profile Data** tab of the Sh interface domain.

Step 3 Check the **Additional Profile** check box.

Note If you have installed the LDAP plug-in, this check box is replaced with a drop-down menu. In this scenario, select the **Sh Profile** option.

Step 4 In the **Profile Mappings** table, click **Add** to add one row for each Sh AVP attribute that is retrieved from the HSS.

Table 80: Profile Mapping Parameters

Parameter	Description
External Code	Defines the attribute name to retrieve. This field should match the Code Literal field in the Sh Parsing Rules table. This represents the internal system attribute name which can be used to apply policies.
Mapping Type	Defines the mapping of the data to an internal CPS data type. Select **SubscriberAttribute**. The following data types are supported: • Service: Selecting this type will add a service to the user profile with the code returned on the HSS attribute. • ChargingId: Selecting this type will allow the External Charging Id retriever to retrieve the HSS value. This attribute would only be used if the local balance database is enabled and provisioned with the external charging ID and the charging id is defined in the HSS. • SubscriberAttribute: Selecting this type will add a policy derived AVP with the external code mapped to the code field and the value mapped to the value field. This attribute type is the most common type to set in the profile mappings. • SubscriberIdentifier: Selecting this type will allow the “An external subscriber id exists” condition within a policy to return the subscriber id.
Regex Expression and Regex Group	If parsing of the incoming AVP is required then a regular expression and regular expression group can be defined to support retrieval of the parsed values. In general, Regex Expression can be left blank and each attribute should be assigned to Regex Group number 1.
Missing Avp Value	Defines the default AVP value when subscriber attribute received from the external profile is missing. **Note** • If a subscriber attribute is missing but its missing AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Missing Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.
Empty Avp Value	Defines the default AVP value when subscriber attribute received from external profile has empty or blank value. **Note** • If a subscriber attribute is empty or blank but its empty or blank AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Empty Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.

Parameter	Description
Apply Timer	This check box indicates whether 'Timer Attribute' is applicable to other subscriber attributes or not. You need to select the checkbox if 'Timer Attribute' needs to be applied for that subscriber attribute.
Discard If Empty	When checked, deletes the LDAP attribute from the session (thus preventing any further use) if regex (when configured) does not match the received value. By default, the checkbox is unchecked (false).
Concatenated Attribute	Currently, the column support has been added for Entitlement (External Code). In the Entitlement row, create a string named *concatenated_entitlement* on Concatenated Attribute column. The *concatenated_entitlement* string parameter is of generic name (user-defined name). If the Concatenated Attribute column is empty, then concatenated entitlement is not enabled. It behaves as the default implementation of Entitlement. When the *concatenated_entitlement* is configured, the default Entitlement AVP as well as *concatenated_entitlement* AVP is supported. When the UDA message is received with multiple Entitlement values and the *concatenated_entitlement* flag is configured in Policy Builder, then all the Entitlement AVP values are concatenated as a single string So, all the Profile Mapping Entitlement AVP must be concatenated as *concatenated_entitlement* with comma separator AVP values. In the CRD table, a new mapping named *concatenated_entitlement_bundle_mapping* must be created. It must be mapped with the new concatenated entitlement, which will bind to the Subscriber AVP code *concatenated_entitlement*.

Step 5 In the **Sh Realm** field, enter the HSS Diameter realm name.

Step 6 If **Subscribe to Notifications** is checked, CPS subscribes to HSS notifications by sending SNR. By default, this option is enabled. If not checked, CPS will send UDR.

Step 7 Select the **Enable External Profile Cache Lookup** check box to allow CPS to use subscriber profile cached in the local CPS SPR database (if available) before querying the external SPR/HSS. The fetched profile is provisioned as per the provisioning configuration in the **Provisioning** tab (see External Profile Cache, on page 201). This configuration is used to reduce the number of Sh requests (SNR/UDR) in case there are multiple Gx sessions for a single subscriber. The first Gx session initiates the Sh request and retrieves the profile and all further Gx sessions for the same subscriber lookup the local SPR database for the subscriber's profile.

Step 8 Select the **Broadcast Profile Change** check box to enable triggering a broadcast message for changes in subscriber profile due to a PNR message. A broadcast message is sent only when there are multiple sessions for the same subscriber.

Step 9 Select **Convert All SNA Attributes to Lowercase** and **Convert SubscriberID to Lowercase** to convert and store lowercase values of Sh code in external-profile. This makes implementation generic and CRD table population easier.

Step 10 In **User Identity Avp Formatting** drop down menu, select either **SIPURI** or **TBCD**. This setting configures the User-Identity AVP Format as either MSISDN TBCD encoding or SIP URI (Session Initiation Protocol Uniform Resource Identifier).

If **SIPURI** is selected, use the **Sip Parsing Rules** table to determine how the SIP URI is constructed.

a) In the **Sip Parsing Rules** table, click **Add** to define a parsing rule.

Table 81: Sip Parsing Rules Parameters

Parameter	Description
Static	A literal String value that will be inserted into the SIP URI as is.
Dynamic	Dynamic uses the Retrievers paradigm to get dynamic data from the policy session and insert it into the SIP URI.

For example, the SIP Parsing Rules in Table 81: Sip Parsing Rules Parameters, on page 206 would generate a SIP URI with this format:

```
sip:456123000000001@nai.epc.mnc123.mcc456.3gppnetwork.org
```

The static values are highlighted in bold text. The dynamic portions of the SIP URI are extracted from the following policy session objects, as follows:

- Gx IMSI: 456123000000001
- Gx MNC Trailing Zero IMSI Based: 123
- Gx MCC IMSI Based: 456

Table 82: Sip Parsing Rules Example

Static	Dynamic
sip:	
	Gx IMSI
@nai.epc.mnc	
	Gx MNC Trailing Zero IMSI Based
.mcc	
	Gx MCC IMSI Based
.3gppnetwork.org	

Step 11 In the **Service Indications** table, click **Add** to filter users by a service indication (group) name.

If no Service Indication value is entered, the HSS will deliver data from all available service indication groups.

In the XML sample below, the Service Indication is “Service1”:

```
<ServiceIndication>Service1</ServiceIndication>.
```

Step 12 In the **Sh Parsing Rules** table, click **Add** to define which parameters to parse from the XML provided by the HSS. Each AVP includes a Code and Value pair, and this table allows you to define which literal or dynamic XML values should be parsed from the XML file.

Table 83: Sh Parsing Rules Parameters

Parameter	Description
Code Literal	Use this field to define the literal XML element which represents the Code portion of the user's AVP. Use this when a static value should be set. For example: Entitlement

Code Xpath	Use this field to define a dynamic XML element which represents the Code portion of the user's AVP. Use this when a dynamic value should be parsed.
	For example: /SampleShUser/Custom[@AttributeName='BillingPlan']
	To map default empty and missing value, Sh parsing rule needs to be with Code XPath:
	Sample XML:
	`<Sh-Data>`
	`    <RepositoryData>`
	`    <ServiceIndication>CamiantUserData</ServiceIndication>`
	`    <SequenceNumber>0</SequenceNumber>`
	`    <ServiceData>`
	`   <CamiantShUser xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	` xsi:noNamespaceSchemaLocation="CamiantShUser.xsd">`
	`    <Version>1.0</Version>`
	`    <UserId Type="E164" Scope="Public">19010921003</UserId>`
	`    <UserId Type="NAI"`
	`Scope="Private">311482310921003@nai.epc.mnc482.mcc311.3gppnetwork.org</UserId>`
	`    <UserId Type="IMSI" Scope="Private">311482310921003</UserId>`
	`    <Custom AttributeName="BillingPlanCode">BPC_LO3</Custom>`
	`    <Custom AttributeName="ServiceName">ServiceA</Custom>`
	`    </CamiantShUser>`
	`    </ServiceData>`
	`    </RepositoryData>`
	`  </Sh-Data>`

Value Literal	Use this field to define the literal XML element which represents the Value portion of the user's AVP. Use this when a static value should be set.
Value Xpath	Use this field to define a dynamic XML element which represents the Value portion of the user's AVP. Use this when a dynamic value should be parsed. For example: /SampleShUser/Custom[@AttributeName='4G']

Note The parsed Code value from the XML file must be mapped to one of the attributes in the Profile Mapping table as defined in #unique_150 unique_150_Connect_42_table_E9C733052AE443A8BB19B1BD885BAD8B.

The following example shows how to pair a Code Literal with a Value Xpath to parse the Entitlement information from the following XML:

Code Literal = Entitlement

Value Xpath = /SampleShUser/Entitlement

```
<?xml version="1.0" encoding="UTF-8"?>
 <Sh-Data>
   <RepositoryData>
     <ServiceIndication>Service1</ServiceIndication>
     <SequenceNumber>0</SequenceNumber>
```

```
      <ServiceData>
        <SampleShUser xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:noNamespaceSchemaLocation="SampleShUser.xsd">
          <Version>1.0</Version>
          <UserId Type="E164" Scope="Public">11122333444</UserId>
          <UserId Type="NAI"
           Scope="Private">456123000000001@nai.epc.mnc123.mcc456.3gppnetwork.org</UserId>
          <UserId Type="IMSI" Scope="Private">456123000000001</UserId>
          <Entitlement>Gold</Entitlement>
          <Custom AttributeName="BillingPlan">Level1</Custom>
          <Custom AttributeName="4G">200k200k</Custom>
        </SampleShUser>
      </ServiceData>
    </RepositoryData>
  </Sh-Data>
```

Step 13 Enable **Use Service Indications for Service Data Caching** in Sh Profile. When selected, on receiving Sh messages (SNA/PNR) with Sh-User-Data, CPS verifies if there is any XML blob with ServiceIndication matching the configured Service-Indication in the PB Domain configuration for that Gx Session. If a match is found, corresponding ServiceData attributes are updated for that session.

Step 14 If you want to configure Sh retry, define the parameter values in the **Retry Profile** area. Click the check box to open the **Retry Profile** parameters.

Table 84: Retry Profile Parameters

Parameter	Description
Retry Interval	Determines the number of minutes between retry attempts.
Max Retry Attempts	Determines the maximum number of retries that occur after a failed attempt. The default value is 3 attempts.
Backoff Algorithm	Determines the actual delay between retry attempts. Following are the options: **Constant_Interval:** The configured Retry Interval is used (without any change) for all retry attempts. **Linear_Interval:** Each retry is scheduled after the number of minutes derived from multiplying the Retry Interval by the number of attempts since the last report.

Parameter	Description
Retry Interval Granularity	Determines the retry interval granularity. The default setting is **Minutes**. **Note** • To change the granularity to lower than 1 second (1000 ms), change the following parameter in the `qns.conf` file: `-Dscheduler.executor.granularity=200` (to set the granularity to 200 ms). Setting the value to lower than 200 can cause issues if the retry load is high. • By default, the CPS scheduler does not accept any event that is scheduled to greater than 15 seconds of the current time. To increase this interval, change the following parameter in the `qns.conf` file: `-Dscheduler.interval.max=60000` (to accept events up to 60 seconds). The retry interval should be up to 60 seconds. Setting this value to greater than 60 seconds is not recommended. • The default scheduler queue capacity is 50000. The system discards any event if the queue is full. • If UDR retry from CCR-I and CCR-U come at the same time, there may be an extra UDR generated due to concurrent update of the session.
Retry on CCR-u	When selected, the system will attempt Sh UDR on CCR-u if the UDR is not successful during CCR-i. If the UDR is not successful, the Sh Retry Interval (if active) will be reset. The default setting is false (unchecked).
Retry on Alternate Host	When selected, the system sends the Sh retry messages to a different host in the same realm provided there are multiple hosts in the same realm. The default setting is false (unchecked).
Result Code Based Retries	Determines the result codes for which the Sh UDR/SNR retries should happen. Following are the options: • Result Code: The result codes for which Sh UDR/SNR needs to be retried by QNS. If this list is empty, the Sh UDR/SNR is retried for all 3xxx and 4xxx result codes. • Is Experimental: Indicates that the configured result code is an experimental result code. Hence, retry happens only if the result code is received in Experimental-Result-Code AVP.

Configuring MNC Length

To accommodate networks where both 2-digit and 3-digit MNCs are used, additional identifiers are needed since the same MCC can be used with both MNC lengths. In those cases, an XML file is used to establish a relationship between the MNC length and the MCC (Mobile Country Code). This XML file lists the actual, possible MNC values.

For example:

For MCC 405, the MNC length is 2 for Reliance in most cases, for example, 03.

For the same MCC 405, the MNC length is 3 for TATA DOCOMO in most cases, for example, 030.

For the vast majority of cases, the XML file has sufficient information to determine the MNC length just from the country code. In countries where both 2 and 3 digit MNC values are used, adding the actual MNC into the XML is usually sufficient, but there still are a small number of cases that cannot be differentiated correctly. In the above example, the MCC is 405 in both cases and the problem is that the MNC in both cases starts with 03. CPS checks for both 03 and 030, but because both are found, there is no way to know which is correct. The IMSI is built in the following manner: 3 digit MCC, 2 or 3 digit MNC, and 9 or 10 digit MIN so the total IMSI is 15 digits (an exception to this is some old IMSIs which are 14 digits).

The following known conflicts are included in the XML file.

```
<country name="in" mnc="03" mncLength="2" carrier="Reliance" operator="Bihar" />
<country name="in" mnc="04" mncLength="2" carrier="Reliance" operator="Chennai" />
<country name="in" mnc="030" mncLength="3" carrier="TATADOCOMO" operator="Gujarat"/>
<country name="in" mnc="031" mncLength="3" carrier="TATADOCOMO" operator="Haryana"/>
<country name="in" mnc="032" mncLength="3" carrier="TATADOCOMO" operator="HimachalPradesh"/>
<country name="in" mnc="033" mncLength="3" carrier="TATADOCOMO" operator="JammuAndKashmir"/>
<country name="in" mnc="034" mncLength="3" carrier="TATADOCOMO" operator="Karnataka"/>
<country name="in" mnc="035" mncLength="3" carrier="TATADOCOMO" operator="Kerala"/>
<country name="in" mnc="036" mncLength="3" carrier="TATADOCOMO" operator="Kolkata"/>
<country name="in" mnc="037" mncLength="3" carrier="TATADOCOMO" operator="MaharashtraAndGoa"/>
<country name="in" mnc="038" mncLength="3" carrier="TATADOCOMO" operator="MadhyaPradesh"/>
<country name="in" mnc="039" mncLength="3" carrier="TATADOCOMO" operator="Mumbai"/>
<country name="in" mnc="041" mncLength="3" carrier="TATADOCOMO" operator="Orissa"/>
<country name="in" mnc="042" mncLength="3" carrier="TATADOCOMO" operator="Punjab"/>
<country name="in" mnc="043" mncLength="3" carrier="TATADOCOMO" operator="Rajasthan"/>
<country name="in" mnc="044" mncLength="3" carrier="TATADOCOMO" operator="TamilNaduChennai"/>
<country name="in" mnc="045" mncLength="3" carrier="TATADOCOMO" operator="UttarPradeshE"/>
<country name="in" mnc="046" mncLength="3" carrier="TATADOCOMO"
operator="UttarPradeshWAndUttarkhand"/>
<country name="in" mnc="047" mncLength="3" carrier="TATADOCOMO" operator="WestBengal"/>
```

This XML configuration file is available in the following directory: `/etc/broadhop/pcrf/mcc.xml`.

Modifications to this file requires a server restart (`restartall.sh`).

Caution Executing `restartall.sh` will cause messages to be dropped.

mcc.xml Schema

The mcc.xml file has the following schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="mccList">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="mcc" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="country">
                <xs:complexType>
                  <xs:attribute name="name" type="xs:string"></xs:attribute>
                  <xs:attribute name="mnc" type="xs:int"></xs:attribute>
                  <xs:attribute name="mncLength" type="xs:int"></xs:attribute>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
            <xs:attribute name="id" type="xs:int"></xs:attribute>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

XML Example

The following file shows an example of a simple `mcc.xml` file with several values:

```
<?xml version='1.0' encoding='UTF-8'?>
<mccList>
  <mcc id="202"><country name="gr" mncLength="2" /></mcc><!-- Greece -->
  <mcc id="250">
    <country name="ru" mncLength="2" />
    <country name="ru" mnc="811" mncLength="3" operator="VotekMobile" />
  </mcc><!-- Russian Federation -->
</mccList>
```

XML Nodes Explained

A single mncLength for a country code has a node structure like the following:

```
<mcc id="202"><country name="gr" mncLength="2" /></mcc><!-- Greece -->
```

The code then parses the MCC element into a single id:country:mncLength relationship so that the MNC length returns as 2 in the above case. For a country or carrier that needs to have an MNC length of 3, the following node produces this outcome:

```
<mcc id="310"><country name="us" mncLength="3" /></mcc><!-- United States -->
```

A country that uses both MNC lengths may need multiple child nodes that specify exceptions like the following:

```
<mcc id="405">
  <country name="in" mnc="01" mncLength="2" carrier="Reliance"
operator="AndhraPradeshAndTelangana" />
<!-- more country codes here-->□
</mcc>
```

The features code then parses these exceptions for MNC length retrieval looking for matching conditions within the list of provided specifics to create the relationship between the country code and the MNC length. If a match is not found an empty string is returned as a default. An empty string is returned so that an incorrect SIP URI is not built.

Retrieving Subscriber Profile from an LDAP/Ud Server

For retrieving a connection from an LDAP/Ud server it is necessary to define the following sets of data to enable this retrieval.

LDAP Server Set Definition

Within the **Ldap Server Sets** section on the **Reference Data** tab, create an LDAP Server Set. The Ldap Server Set represents a connection to a logical set of LDAP servers that is reusable across Domain definitions. As a result, most deployments have only one Ldap Server Set defined in this section.

The following parameters can be configured under **Ldap Server Set**:

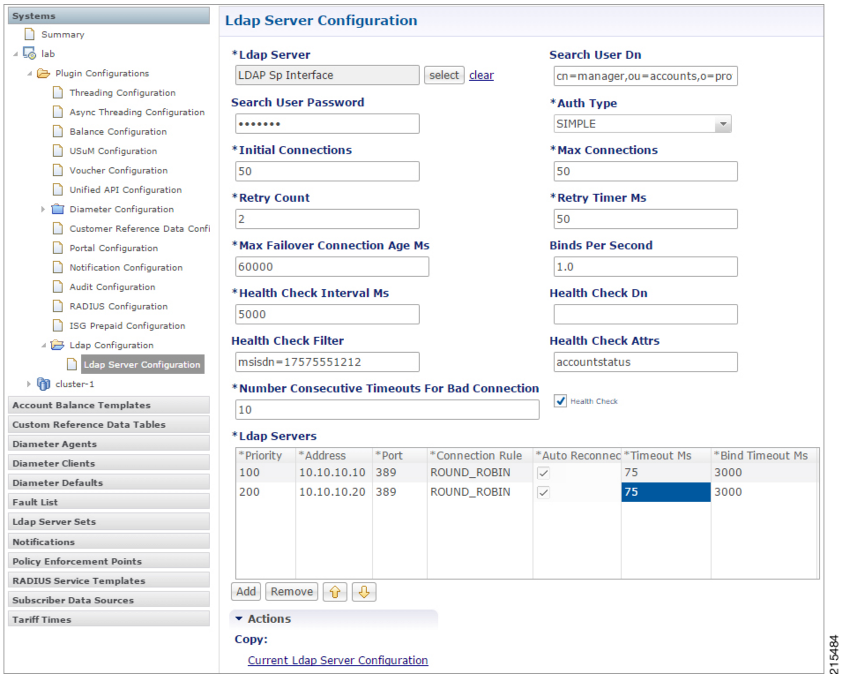
Table 85: Ldap Server Set Parameters

Parameter	Description
Name	A textual description of the LDAP connection. This should be something easily recognizable as the name of the LDAP server containing the subscriber profiles.
Missing Attribute Result Code	Result code expected from LDAP Server in case BaseDN for attribute addition is missing.
Ignore Ldap Error Result Codes	The parameter accepts a list of integer result codes. If an Ldap search response contains one of the configured result codes, then the response is not flagged as error and instead, the `NO_LDAP_ATTRIBUTE_FOUND LDAP` attribute is created locally for use in policy.
Use Asynchronous Operations	This should be is checked (true). Setting to unchecked (false) can result in unpredictable performance and is not supported.
Add Child On Parent Create Failure	If checked, continue creation of attributes even though parent DN creation is success or failure.
Add Request Attributes	This table is used to define the attributes that can be used while sending add Parent DN request in case modifyRequest fails.

LDAP Configuration

Within the **Systems** section on the **Reference Data** tab, create a new plugin configuration for **Ldap Configuration**. Under the Ldap Configuration create a child **Ldap Server Configuration**.

Figure 89: Ldap Server Configuration



Ldap Server Configuration

*Ldap Server: LDAP Sp Interface

Search User Dn: cn=manager,ou=accounts,o=pro

Search User Password: •••••••

*Auth Type: SIMPLE

*Initial Connections: 50

*Max Connections: 50

*Retry Count: 2

*Retry Timer Ms: 50

*Max Failover Connection Age Ms: 60000

Binds Per Second: 1.0

*Health Check Interval Ms: 5000

Health Check Dn:

Health Check Filter: msisdn=17575551212

Health Check Attrs: accountstatus

*Number Consecutive Timeouts For Bad Connection: 10

☑ Health Check

*Ldap Servers

*Priority	*Address	*Port	*Connection Rule	*Auto Reconnec	*Timeout Ms	*Bind Timeout Ms
100	10.10.10.10	389	ROUND_ROBIN	✓	75	3000
200	10.10.10.20	389	ROUND_ROBIN	✓	75	3000

Copy:

Current Ldap Server Configuration

The following parameters can be configured under Ldap Server Configuration:

Table 86: Ldap Server Configuration Parameters

Parameter	Description
Ldap Server	Assign this to the Ldap Server Set created in the previous step.
Search User Dn	Set this to the user DN for connecting to the LDAP server. An example is `cn=managerou=accountso=profile`.
Search User Password	Set this to the password for connecting to the LDAP server. **Note** The same password must apply to all servers defined in this configuration.
Auth Type	Select the LDAP auth type required by the LDAP server. Default value is SIMPLE.
Initial Connections	Set the initial connections to "50". This represents the number of connections from a Policy Director (load balancer) to the LDAP server(s).
Max Connections	Set this value to the same value as the initial connections.
Retry Count	Set this to the total number of "tries" the system should execute for a give LDAP query. For example a value of 2 would indicate one try and then on timeout one more attempt.

Parameter	Description
Retry Timer Ms	Set this to the time period when the policy engine retries to a second Policy Director (load balancer) to send the request. **Note** Setting this value too low results in a large number of additional requests and this value should be set to a value close to the SLA provided by the LDAP server in servicing requests.
Max Failover Connection Age Ms	Set this value to the time period a secondary connection to be utilized before checking to determine if the original primary server is available. An example value is 60000 ms (1minute).
Binds Per Second	Set this to the maximum rate at which to connect to the LDAP server. Setting this to a high value may result in extra load on the peer LDAP server.
Health Check Interval Ms	Set this to the period of time to generate a health check message. An example value is 5000 ms (5 seconds).
Health Check Dn	Set this to the health check DN sent on the health check LDAP query.
Health Check Filter	Set this to the filter sent on the health check LDAP query.
Health Check Attrs	Set this to a comma delimited list of attributes to retrieve in the LDAP health check query.
Health Check	Set this to checked (true) to enable the health check. Default is checked.
Number of Consecutive Timeouts for Bad Connection	Set this to the number of timeouts that triggers a bad connection and force a reconnection.

Add entries to the LDAP Servers to represent the primary and secondary connections from the CPS system to the LDAP servers. The following parameters can be configured:

Table 87: LDAP Servers

Parameter	Description
Priority	The priority of the server when sending requests. Higher number is equal to higher priority.
Address	The IP address of the server to send requests.

Parameter	Description
Connection Rule	Cisco recommends not to use this setting. However, the following options are available: • ROUND_ROBIN: CPS uses a round-robin algorithm to select the server to establish the connection. This is the default setting. • FASTEST: CPS attempts to establish connections to all associated servers in parallel. However, the first successful connection is kept while the other connections are closed. **Note** If the **Priority** setting is the same for multiple LDAP servers with **ROUND_ROBIN** connection rule, CPS makes connections evenly with configured multiple LDAP servers.
Auto Reconnect	This setting is not currently used.
Timeout Ms	Set this to the SLA for queries for the LDAP server.
Bind Timeout Ms	Set this to the SLA for binds to the LDAP server.

Setting Up Additional Profile Data

Within the **Additional Profile Data** tab of the **Domain**, select **Generic Ldap Search** in the upper right corner so that this Domain should retrieve data from an LDAP query.

The following parameters can be configured under Additional Profile Data:

Table 88: Additional Profile Data Parameters

Parameter	Description
Profile Mappings	In the profile mappings table add one row for each attribute that is retrieved from the LDAP server.
External Code	The LDAP attribute name to retrieve.

Parameter	Description
Mapping Type	The mapping of the data to an internal CPS data type. The following data types are supported • Service Selecting this type adds a service to the user profile with the code returned on the LDAP attribute. • ChargingId Selecting this type allows the External Charging Id retriever to retrieve the LDAP value. This attribute would only be used if the local balance database is enabled and provisioned with the external charging ID and the charging id is defined in the LDAP server. • SubscriberIdentifier Selecting this type allows the “An external subscriber id exists” condition within a policy to return the subscriber id. • SubscriberAttribute Selecting this type adds a policy derived AVP with the external code mapped to the code field and the value mapped to the value field. This attribute type is the most common type to set in the profile mappings.
Regex Expression and Regex Group	If parsing of the incoming AVP is required then a regular expression and regular expression group can be defined to support retrieval of the parsed values.
Missing Avp Value	Defines the default AVP value when subscriber attribute received from the external profile is missing. **Note** • If a subscriber attribute is missing but its missing AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Missing Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.
Empty Avp Value	Defines the default AVP value when subscriber attribute received from external profile has empty or blank value. **Note** • If a subscriber attribute is empty or blank but its empty or blank AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Empty Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.
Apply Timer	This check box indicates whether 'Timer Attribute' is applicable to other subscriber attributes or not. You need to select the checkbox if 'Timer Attribute' needs to be applied for that subscriber attribute.
Discard If Empty	When checked, deletes the LDAP attribute from the session (thus preventing any further use) if regex (when configured) does not match the received value. By default, the checkbox is unchecked (false).

Parameter	Description
Ldap Server Set	Associate the LDAP server set defined in the LDAP Server Set Definition.
Base Dn	This should be set to the Base DN sent in the LDAP query. If not defined, then the request does not contain a base DN. **Note** This string supports string replacement using the find / replace of strings with variables from the policy state as defined in the “Replacement Rules” table.
Filter	This should be set to the Filter sent in the LDAP query. If not defined, then the request does not contain a filter. **Note** This string supports string replacement using the find / replace of strings with variables from the policy state as defined in the “Replacement Rules” table.
Dereference Policy	Set this to the dereference policy that the LDAP query requires. Default value is NEVER.
Avp Code to Disable Query	This is an optional field that controls whether to disable the LDAP query. This is often used in conjunction with Custom Reference Data tables and other session attributes to optionally disable an LDAP query. If the calculated CRD AVP has a value (ignoring case) of “false” then the LDAP query is skipped.
Profile Refresh Interval (mins)	Set this value to automatically refresh a profile by querying the profile after a specified delay.
Replacement Rules	In the replacement rules table add one row per replacement string to substitute into the Base DN or Filter string on a request by request basis.
Replacement String	The literal string used in the “From” operation. The best practice is to use a symbol (for example, $) at the front of the string to ensure uniqueness in the find and replacement operation.
Replacement Source	The source of the data for the “To” operation. The most common examples are “Session MSISDN” and “Session IMSI”.
Subscriber Timer Attribute	This parameter indicates which attribute is timer attribute among all the LDAP server attributes. The timer follows the ISO 8601 time standards. Refer to ISO 8601 for more information.
Lower Bound For Timer Attribute In Minutes	This parameter is used to indicate how much time before the start time of Subscriber Timer Attribute CPS has to accept when LDAP server sends timer attribute. Default value is 30 minutes.
Elapsed Time For Timer Attribute In Percentage	This parameter indicates how much time after the start time of Subscriber Timer Attribute CPS has to accept when LDAP server sends timer attribute. Default value is 100. Possible range is from 1 to 100.
Service Attribute Info	For more information, refer to the Table 89: Service Attribute Info, on page 218.

Table 89: Service Attribute Info

Parameter	Description
Attribute Name	This parameter is used to match an External Attribute Code and create a Virtual Service object with that value.
Param Attribute Name	While using Param Attribute Name, the value should have one of its fields match the value of the attribute defined under Attribute Name. This field should have a fixed name "service". The virtual service is created with the value of this field name "service". All the fields in the Param Attribute Name should be provided in-order in the Parameter Fields list (even if some fields are not required/have no value, they need to be included in the list in the expected order). Both Attribute Name and Param Attribute Name can contain the same attribute name.
Delimiter	The delimiter string to be used for splitting the attribute value into fields.
Parameter Fields	The list of field names *in order* as extracted from the parameter attribute value using the delimiter. The field that matches the parameter attribute with the corresponding service attribute value (Attribute Name) is expected to be provided a fixed name called **"service"**. If CPS fails to parse the Parameter Fields, it creates a virtual-service with no AVPs.
Expiration Date Code	This parameter must be one of the field names from the Parameter Fields list that identifies the virtual service expiration date field. If CPS is able to extract the field for expiration-time and also decode a valid date out of it then CPS uses the decoded date value as expiration-date on the virtual-service. If CPS is not able to extract the fields using the delimiter or is not able to decode the date value using the Expiration Date Code and Expiration Date Format values, then that virtual-service never expires and remains active.
Expiration Date Format	The JAVA date format string that is used to decode and extract the exact date-time value for expiration-date. If CPS fails to decode the ExpirationDate using the JAVA date value then the expiration-date does not need to be set on the virtual service.

Retrieving Subscriber Profile from an UDC Server

Within the **Additional Profile Data** tab of the **Domain**, select **UDC Profile** in the upper right corner so that this Domain should retrieve data from an UDC server.

The following parameters can be configured under Additional Profile Data for UDC:

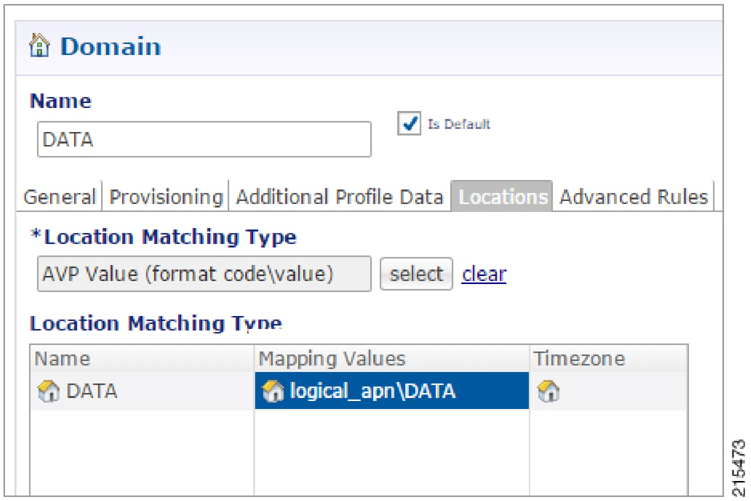
Table 90: Additional Profile Data Parameters - UDC Profile

Parameter	Description
Profile Mappings	In the profile mappings table add one row for each attribute that is retrieved from the UDC server. **Note** Under Profile Mappings table, the External Code can be any LDAP attribute or Sy Counter. The Mapping Type that is supported by UDC currently is SubscriberAttribute (no other Mapping Type is supported).
Subscriber Timer Attribute	This parameter indicates which attribute is timer attribute among all the server attributes. The timer follows the ISO 8601 time standards. Refer to ISO 8601 for more information.
Lower Bound For Timer Attribute In Minutes	This parameter is used to indicate how much time before the start time of Subscriber Timer Attribute CPS has to accept when the server sends timer attribute. Default value is 30 minutes.
Elapsed Time For Timer Attribute In Percentage	This parameter indicates how much time after the start time of Subscriber Timer Attribute CPS has to accept when the server sends timer attribute. Default value is 100. Possible range is from 1 to 100.
Active Traffic Management	CPS uses this field to identify Active Traffic Management attribute when CPS receives profile attributes from UDC. The value of this field should be in same as configured in ADTMAttribute service configuration.

Defining the Location Attributes of the Domain

The content of the **Locations** attributes tab is only required if the “Define one domain per logical APN” strategy is used in defining domains. If this strategy is selected then the following attributes should be set on the location form

Figure 90: Domain Location Attributes



Name: DATA

☑ Is Default

*Location Matching Type: AVP Value (format code\value)

Location Matching Type

Name	Mapping Values	Timezone
DATA	logical_apn\DATA	

The following parameters can be configured under **Locations** tab:

Table 91: Location Tab Parameters

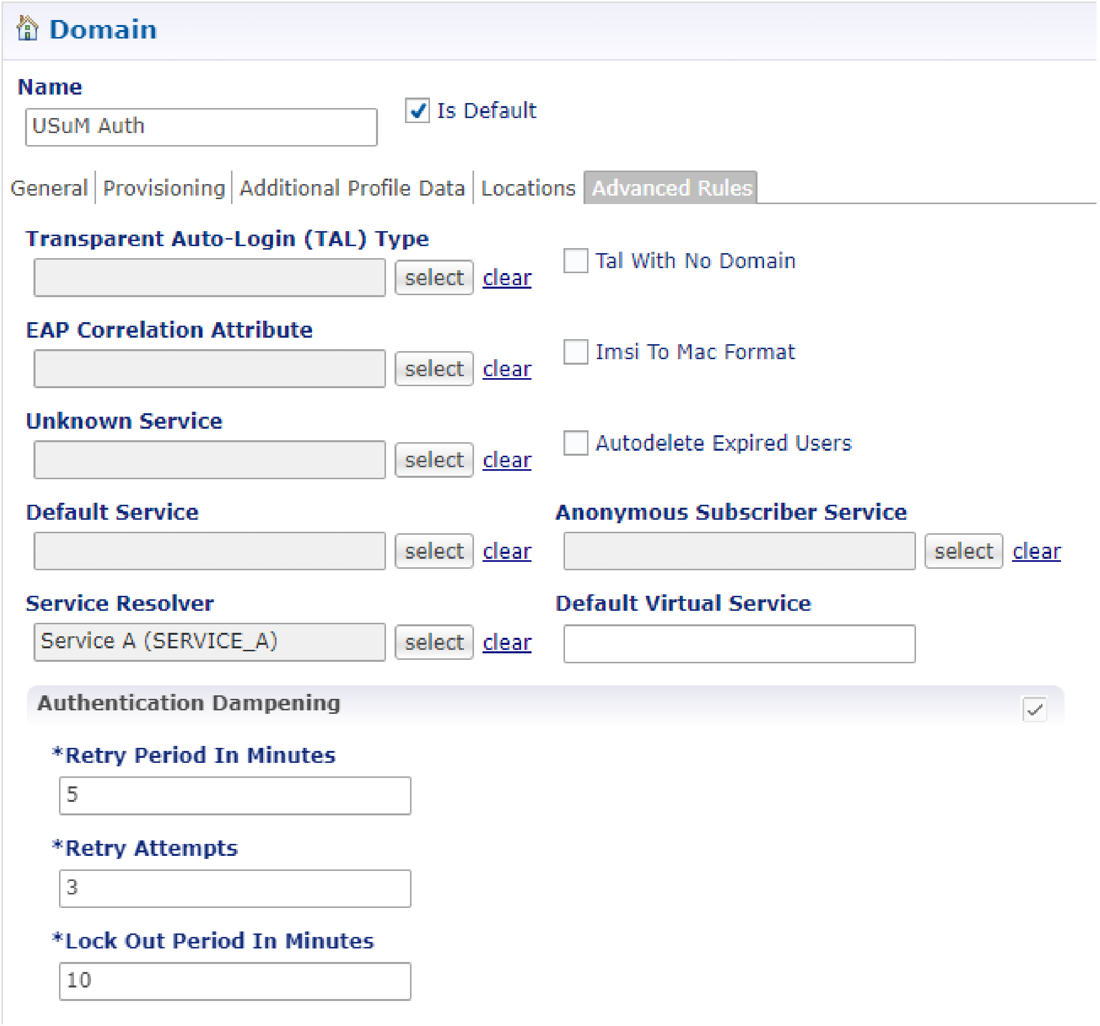
Parameter	Description
Location Matching Type	This attribute should be set to AVP value. The AVP value matching type allows the information from a Custom Reference Data table (CRD) to be used in the domain assignment.
Location Matching Type Table	One entry should be added with a name equal to the logical APN and the mapping value equal to the CRD column code (for example, logical_apn) with a "\" and then the logical APN value. The Timezone attribute is not used in mobility configurations and should be left blank.

Defining the Advanced Rules of the Domain

There are only three fields that should be set on this form when supporting a mobile configuration.

- If the deployed system is using the CPS USuM subscriber database, then there are two options:
  - **Default Service:** The default service applies if the user profile exists in the local SPR and the profile has no associated services.
  - **Unknown Service:** The unknown service applies if the user profile lookup failed against the local SPR.
- Otherwise set the Anonymous Service to apply a service to users that map to this Domain.

Figure 91: Selecting a Service



Domain

Name: USuM Auth

☑ Is Default

Transparent Auto-Login (TAL) Type: select clear

☐ Tal With No Domain

EAP Correlation Attribute: select clear

☐ Imsi To Mac Format

Unknown Service: select clear

☐ Autodelete Expired Users

Default Service: select clear

Anonymous Subscriber Service: select clear

Service Resolver: Service A (SERVICE_A) select clear

Default Virtual Service:

Authentication Dampening ☑

*Retry Period In Minutes: 5

*Retry Attempts: 3

*Lock Out Period In Minutes: 10

- We can also configure the following:
  - **TAL with No Domain:** When enabled the operator allows user to auto login without including the Domain in credential.
  - **Imsi to Mac Format:** When enabled the user IMSI is converted to MAC format before the user can log on to the network.
  - **Autodelete Expired Users:** This check box is used for deletion of credentials which have crossed the expiration date. Removal of expired credentials occurs whenever request for that subscriber is received. After deletion of expired credentials if there are no valid credentials then subscriber is removed from SPR database.
  - **Service Resolver:** The service resolver applies only if the user profile is associated with a virtual service.
  - **Default Virtual Service:** Default Virtual Service is used by CPS to evaluate subscriber policies when no other Virtual Services can be derived. The default Virtual service is empty (does not have any AVPs) and the Virtual Service Code is equal to this configured value.

A virtual service is effectively just a 'code' to label the virtual service and a collection of Service Options which contain the definition of what a virtual service 'is'.

There is no logical difference between a service and a virtual service. Other type of services are Unknown Service, Default Service.

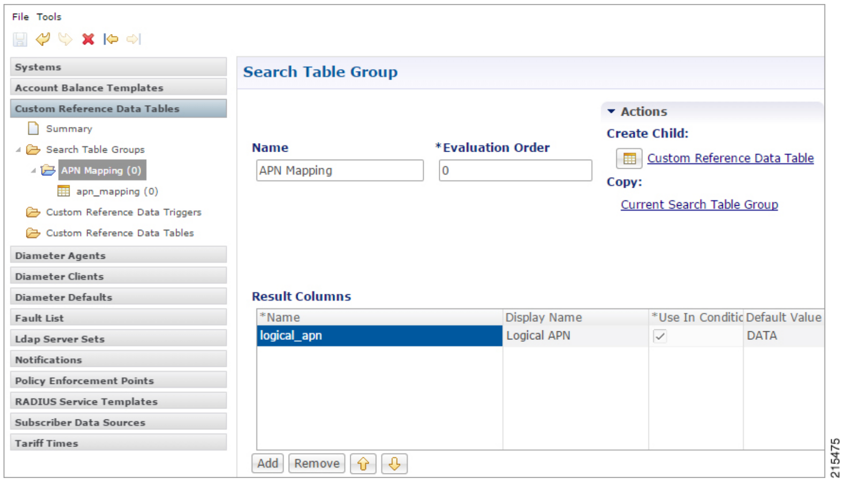
Creating a Custom Reference Data (CRD) table for APN mapping

If the “Define one domain per logical APN” strategy is used for defining domains then creation of a CRD table is required to perform this mapping. Since this is custom to each deployment an individual deployment may define the CRD table with a slightly different structure but the basic definition should be similar to what is described in the following sections.

Define the APN Mapping Search Table Group

In the **Custom Reference Data Tables** section under **Reference Data** tab, add a new **Search Table Group**.

Figure 92: Search Table Group Configuration



Search Table Group

Name: APN Mapping

*Evaluation Order: 0

Result Columns

*Name	Display Name	*Use In Conditic	Default Value
logical_apn	Logical APN	✓	DATA

The following parameters can be configured under **Search Table Group**:

Table 92: Search Table Group Parameters

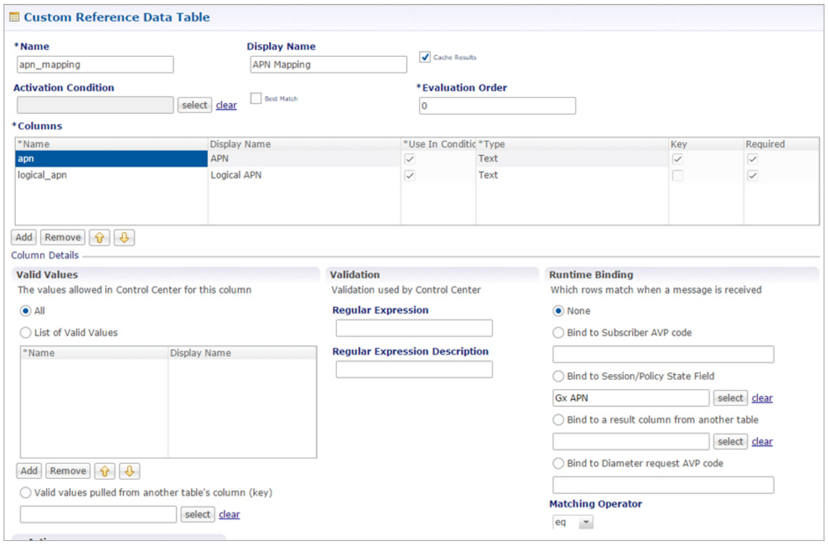
Parameter	Description
Name	Set to recognizable name to indicate that this is the APN mapping search table group. An example is “APN Mapping”.
Evaluation Order	Set to “0” to ensure that this group is processed before other search tables are processed.
Results Column	

Parameter	Description
Name	Set to logical_apn. This is the name of the AVP that will be populated into the policy engine representing the logical APN. The name must not have spaces or special characters. Best practice is to use "_" character for spaces and lowercase letters in place of mixes case or all uppercase letters.
Display Name	Set to "Logical APN" or equivalent display name for use in reference data screens. This field is only used for display purposes and as a result can contain spaces and special characters.
Use In Condition	Set this to "true" which is a checked value.
Default Value	Set this to the default logical APN to if a match is not found in the mapping table. An example of this value is "DATA".

Define the APN Mapping Custom Reference Table

On the "APN Mapping" search table group, create a new Custom Reference Table.

Figure 93: Custom Reference Data Table Configuration



Custom Reference Data Table

*Name: apn_mapping

Display Name: APN Mapping

☑ Cache Results

Activation Condition: select clear

□ Best Match

*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
apn	APN	✓	Text	✓	✓
logical_apn	Logical APN	✓	Text	□	✓

Add Remove ⇧ ⇩

Column Details

Valid Values

The values allowed in Control Center for this column

● All

○ List of Valid Values

*Name	Display Name

Add Remove ⇧ ⇩

○ Valid values pulled from another table's column (key)

select clear

Validation

Validation used by Control Center

Regular Expression

Regular Expression Description

Runtime Binding

Which rows match when a message is received

● None

○ Bind to Subscriber AVP code

○ Bind to Session/Policy State Field

Gx APN select clear

○ Bind to a result column from another table

select clear

○ Bind to Diameter request AVP code

Matching Operator

eq

The following parameters can be configured under **Custom Reference Data Table**:

Table 93: Custom Reference Data Table Parameters

Parameter	Description
Name	Set this to "apn_mapping" or an equivalent table name to contain the mapping data. The name should not have spaces or special characters. A best practice is to use "_" character for spaces and lowercase letters in place of mixes case or all uppercase letters.
Display Name	Set this to "APN Mapping" or equivalent display name for use in reference data screens. This field is only used for display purposes and as a result can contain spaces and special characters.

Parameter	Description
Cache Results	Set this to "true" which is a checked value.
Best Match	This should be set to "false" unless regular expression or defaulting with "*" matches is used in the key fields.
Evaluation Order	Set to "0" to ensure that this group is processed before other search tables are processed.
Columns	For more information, see Table 94: Columns Table, on page 224.

Table 94: Columns Table

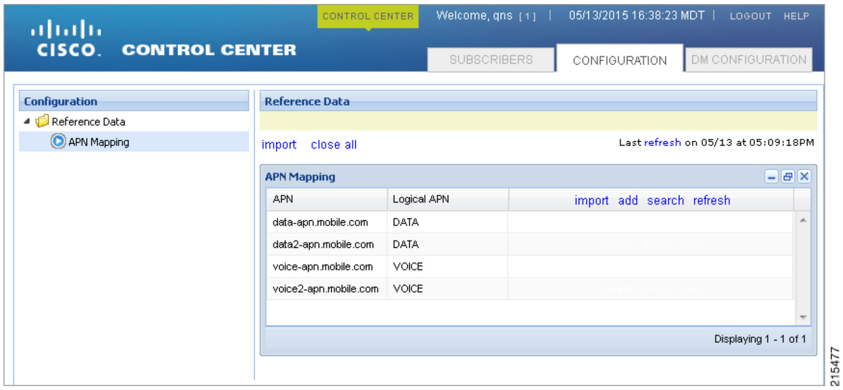
Name	Parameter	Example
apn	Name	apn
	Display Name	APN
	Key	true
	Required	true
	Bind to Session/Policy State Field	Gx APN
Logical_apn	Name	logical_apn
	Display Name	Logical APN
	Required	true

Load Data into the APN Mapping Table

After successfully publishing the configuration to the running system, new APN(s) are defined by entering the data through the Control Center GUI or through API calls (refer to the *CPS Installation Guide for VMware* for this release for instructions on how to access the Control Center).

An example of the definition is shown below:

Figure 94: APN Mapping Table



APN	Logical APN
data-apn.mobile.com	DATA
data2-apn.mobile.com	DATA
voice-apn.mobile.com	VOICE
voice2-apn.mobile.com	VOICE

Validation Steps

The following validation steps are designed to verify whether the “Define one domain per logical APN” approach to APN Profiles is properly configured or not. We will create two domains and map them to a default service based on two different APNs.

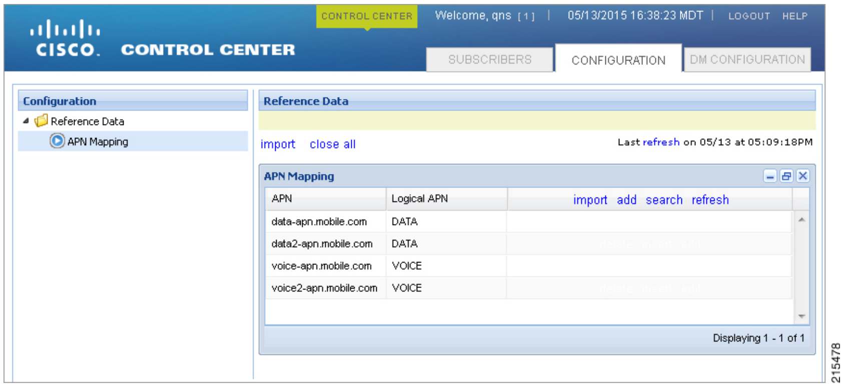
The ability to generate a Gx CCR-i from two different APNs. The actual APN names are not important however they must be different.

Step 1 Configure the CRD table as described in Creating a Custom Reference Data (CRD) table for APN mapping, on page 222.

Step 2 Publish the configuration to the running environment. This is required before data can be loaded into the CRD tables.

Step 3 The actual CRD data to be evaluated is located in the Control Center interface (refer to Load Data into the APN Mapping Table, on page 224). In the control center, make sure there are two different logical APN groups with each group mapping to the Gx APN value that will be passed in the CCR-i. Navigate to the table in Control Center and map each Gx APN to different logical APNs (for example: column apn might have “data.apn.com” and would map to logical APN “DATA” while another “apn” row might map to logical APN “VOICE”).

Figure 95: APN Mapping



APN	Logical APN
data-apn.mobile.com	DATA
data2-apn.mobile.com	DATA
voice-apn.mobile.com	VOICE
voice2-apn.mobile.com	VOICE

Step 4 Configure two different PB domains, one for DATA and one for VOICE.

For more information, see Defining a Domain, on page 198.

Step 5 In each domain, in the **Location** tab, configure the Location Mapping Type of AVP Value to map logical_apn\DATA on the DATA domain and logical_apn\VOICE on the VOICE domain as described in Defining the Location Attributes of the Domain, on page 219.

Step 6 Set the default or anonymous service on the domain's **Advanced** tab to match the service required for the domain.

Step 7 Generate Gx CCR-i from each different APN, validate that the service assigned to the client matches the default/anonymous service for the domain. As per the log below, check that the (location) debug message shows “Location found for avp matching: logical_apn\DATA”:

```
[20XX-XX-XX 12:34:50,025] ===============================================
POLICY RESULT SUCCESS:
        session action = Create
        domainId = location_test
        locationId = apn
        SERVICES: DefaultDataService
        TRIGGER: Message: com.broadhop.diameter2.messages.DiameterRequestMessage
                Application Id: Gx (16777238)
                Command Code: Gx_CCR-I (272)
                Dest host: null
                Dest realm: pcrf.cisco.com
                Device protocol: GX_TGPP
                End to end id: 3024
                Hop by hop id: 6001
                Origin host: pcef-gx
                Origin realm: pcef.cisco.com
                Origin state: 0
                Stack name: null
                Session-Id: .;1096298393;1
                Session-Id: .;1096298393;1
                Auth-Application-Id: 16777238
                Origin-Host: pcef-gx
                Origin-Realm: pcef.cisco.com
                Destination-Realm: pcrf.cisco.com
                CC-Request-Type: 1
                CC-Request-Number: 1
                RAT-Type: 1000
                IP-CAN-Type: 0
                Called-Station-Id: data.apn.com
                Framed-IP-Address: 0x010108f0
                Framed-IPv6-Prefix: 0x004020010b68001400000000000000000000
                3GPP-SGSN-Address: 0x01010101
                3GPP-SGSN-MCC-MNC: 71617
                Supported-Features:
                                Vendor-Id: 10415
                                Feature-List-ID: 1
                                Feature-List: 1
                Subscription-Id:
                                Subscription-Id-Type: 1
                                Subscription-Id-Data: 1234567890
                Subscription-Id:
                                Subscription-Id-Type: 0
                                Subscription-Id-Data: AAAA.BBBB.CCCC
                QPS-Internal-Route-Record-Host: pcef-gx
                QPS-Internal-Route-Record-Realm: pcef.cisco.com
        DEBUG MSGS:
                INFO : (core) Tagging message with ID: GX_TGPP
                INFO : (core) Lock obtained on key: diameterSessionKey:.%3B1096298393%3B1
                INFO : (core) Start session triggered
                INFO : (gx) Rel8 feature supported on session .;1096298393;1
                INFO : (gx) Creating new diameter session .;1096298393;1
                INFO : (custrefdata) Adding AVP [GetLogicalApn/logical_apn], value: DATA
                INFO : (location) Location found for avp matching: logical_apn\DATA
                INFO : (auth) Success ALLOW_ALL authorization
                INFO : (core) No service is associated, added default service code:
DefaultDataService for session
```

Configuring Domain to Parse Sh Attributes in Date and Time Format

Step 1 Log in to Policy Builder.

Step 2 Navigate to **Services** tab.

Step 3 Select **Domain** and configure a new domain.

Step 4 Go to **Additional Profile Data** tab and select **Sh Profile**.

Step 5 Under **Profile Mappings**, add the following:

Table 95: Profile Mappings

External Code	Mapping Type
vdsThrtlPlcyExpireTs	Subscriber Attribute
vdsThrtlExpireTs_Reval	Subscriber Attribute

Step 6 Under **Sh Parsing**, add the following:

Table 96: Sh Parsing

Code Literal	Value Xpath
vdsThrtlPlcyExpireTs	[Name=‘vdsThrtlPlcyExpireTs’

Configuring a Virtual Service

Step 1 Log in to Policy Builder.

Step 2 Navigate to **Services** tab.

Step 3 Select **Domain** and configure a new domain.

Step 4 Go to **Additional Profile Data** and select Sh Profile.

Step 5 Under **Profile Mappings**, add the following:

Table 97: Profile Mappings

External Code	Mapping Type
svcplan	SubscriberAttribute

Step 6 Go to **Advanced Rules**.

Step 7 Set **Service Resolver** to the configured virtual service.

Step 8 Select **Services** tab and configure a virtual service.

CHAPTER 7

Services

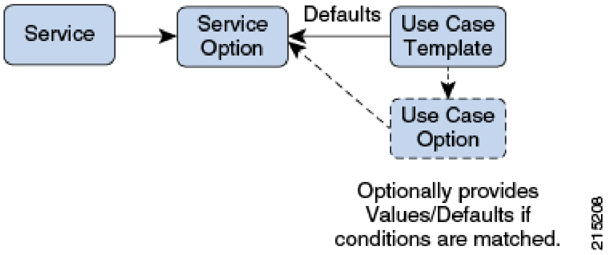
Overview

In CPS, a 'Service' it what is assigned to a subscriber (in USuM) to define how that subscriber is treated. Some basic examples of services would be a 'GOLD' user might get a high upload/download speed whereas a 'BRONZE' user would get a low one. Other examples would include having one type of user be redirected to a portal when their Quota is exhausted whereas another type would only have their speed downgraded.

As the Service maps as closely as possible to how a Service Provider wants to classify their customers, the Service in CPS is flexibly defined to allow configuration at different levels.

Below is an overview of the different objects referenced in the Services tab in PB. The detailed description of each object is provided in below sections.

Figure 96: Services



Service

- A service is effectively just a 'code' to label the service and a collection of Service Options which contain the definition of what a service 'is'.
- What a Customer Service Representative assigns to a subscriber to describe the user's plan.
- Multiple services can be assigned to a single subscriber

- If multiple services are assigned to a subscriber, the service options are combined between all assigned services.

  Therefore, there is no logical difference between a subscriber with:

  - A single service with 10 service options
  - 10 services with 1 option each

Service Option

- Provides the concrete values which can be re-used for multiple services.

  For example, one subscriber might have one service option which describes the values for 10 MB Upload/Download speed and another subscriber which describes 1 MB Upload/Download speed. Continuing the example from above, 10 MB could be assigned to a GOLD service and 1 MB could be assigned to BRONZE.

- What values are configurable in a Service Option are setup by the Use Case Template object. The Use Case Template can provide defaults to the Service Option or hide values in Service Configuration objects not necessary for certain use cases.

- If a Service Configuration's value is not defined in a Service Option, the value from the Use Case Template is used.

Service Configuration

- The low-level configuration objects used by the CPS code to drive functionality. These objects are used to drive functionality in the system. The whole point of the Service > Service Option > Use Case Template chain of functionality is to flexibly configure these Service Configuration objects which the code uses to drive system logic.

- These objects are defined by the CPS code.

Types of service configurations:

- PriorityConfiguration: Only one allowed to be active at a time. If multiples priority configurations are added, highest priority is used.

  These are used in cases where only a single value makes sense. For example, when sending an 'Accept' message, we can only have one template and multiples do not make sense.

  Objects of this type always have a priority field. If multiple priority configurations are added, the highest priority object is used.

  Example: AccessAcceptConfiguration, RegisterMacAddress

- GroupConfiguration (most common): Only 1 per 'Group Name' are allowed to be active. If multiple configurations are added highest priority per 'Group Name' is used.

  These are used in cases where a configuration only makes sense for a single 'group' (key). For example, if it makes sense to control the upload/download speed based on the network type (cell, Wi-Fi, and so on) a service configuration to control network speed with a group set for cell/Wi-Fi would allow multiple service configurations to be added.

Note RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.

These objects always have a group field as well as a priority field. For each unique group value, the highest priority is used.

Example: IsgServiceConfiguration, All Diameter Configurations, OneTimeUsageCharge

- ServiceConfiguration: Multiples allowed. If multiple configurations are added, all are used. 'Modify' functionality in PB for Use Case Options/Service Options can override values conditionally.

  Example: AutoChargeUpAccounts, AutoProvisionQuota, BalanceRateConfiguration

Use Case Templates

Use case templates are the building blocks of the Cisco Policy Builder Service Model architecture.

- Defines the Service Configuration objects to be set by a Service Option.
- Provide default values and/or hide values which do not need to be set by a use case
- Optionally, contains 'Initiators' (Conditions) which define when the template is active.
- Created by an advanced user (usually Engineering/AS).
- Makes Service Option and Service creation easier.

For example, a Use Case Template set up to create different upload or download speeds includes a 'DefaultBearer' QoS Service Configuration object. The user creating a Use Case Template can default and/or hide the values for 'ARP' and other values not directly related to upload or download speed. This allows the creation of the Service Option to be much simpler.

A copy of the Use Case Options is created while copying a Use Case Template.

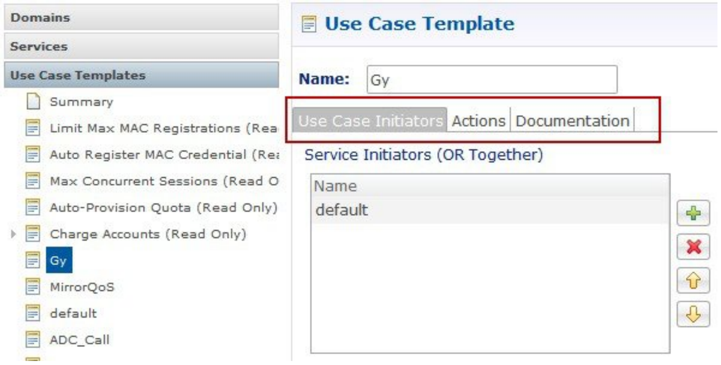
Use Case Template tab Order

A new parameter *`-DshowUseCaseInitiatorTabFirst`* can be added in `pb.conf` (`/etc/broadhop/pb/`) file on pcrfclient01/02 to re-order the **Use Case Template** and **Use Case Option** tabs. This parameter also renames **Use Case Template** and **Use Case Option** tabs to **Actions** tab.

By default, *`-DshowUseCaseInitiatorTabFirst`* is set to *true* (does not required to be added in `pb.conf` file by default).

- If set to *true*, the tabs will be displayed in the following order:

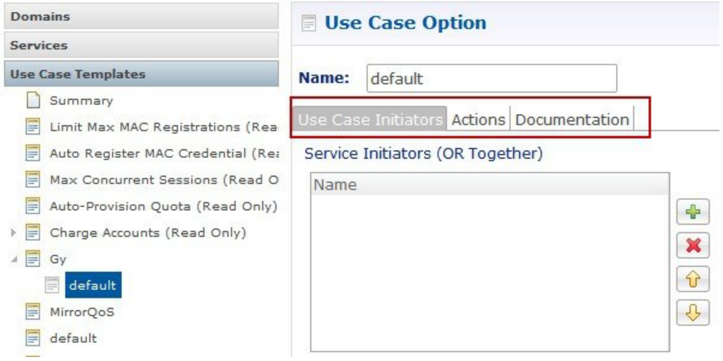
Figure 97: Use Case Initiators > Actions > Documentation


Domains
Services
Use Case Templates
Summary
Limit Max MAC Registrations (Rea
Auto Register MAC Credential (Rea
Max Concurrent Sessions (Read O
Auto-Provision Quota (Read Only)
Charge Accounts (Read Only)
Gy
MirrorQoS
default
ADC_Call
Use Case Template
Use Case Initiators
Actions
Documentation
Service Initiators (OR Together)
Name

Name: Gy

default

Figure 98: Use Case Initiators > Actions > Documentation


Domains
Services
Use Case Templates
Summary
Limit Max MAC Registrations (Rea
Auto Register MAC Credential (Rea
Max Concurrent Sessions (Read O
Auto-Provision Quota (Read Only)
Charge Accounts (Read Only)
Gy
default
MirrorQoS
default
Use Case Option
Use Case Initiators
Actions
Documentation
Service Initiators (OR Together)
Name

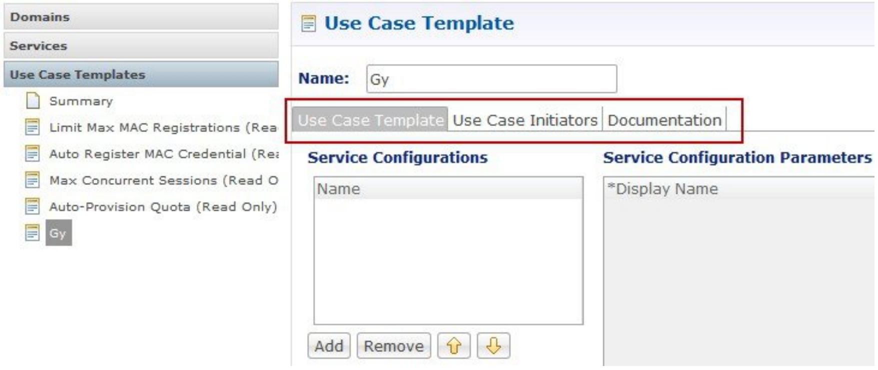
Name: default

- For backward compatibility, the configuration parameter `-DshowUseCaseInitiatorTabFirst` in `pb.conf` (`/etc/broadhop/pb/`) file on pcrfclient01/02 can be set to *false*.

  This parameter also renames **Actions** tab back to **Use Case Template** and **Use Case Option** tabs.

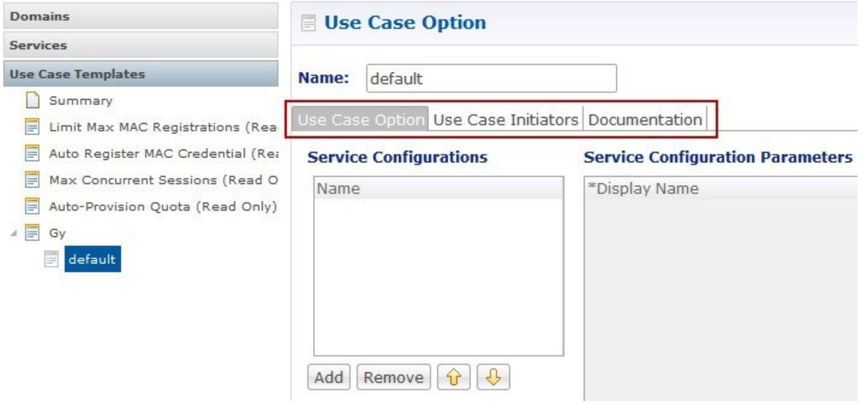
  Use Case Template and **Use Case Option** tabs will be displayed in the following order:

Figure 99: Use Case Template > Use Case Initiators > Documentation


Domains
Services
Use Case Templates
Summary
Limit Max MAC Registrations (Rea
Auto Register MAC Credential (Rea
Max Concurrent Sessions (Read O
Auto-Provision Quota (Read Only)
Gy
Use Case Template
Use Case Template
Use Case Initiators
Documentation
Service Configurations
Service Configuration Parameters
Name
*Display Name
Add
Remove

Name: Gy

Figure 100: Use Case Option > Use Case Initiators > Documentation


Domains
Services
Use Case Templates
Summary
Limit Max MAC Registrations (Rea
Auto Register MAC Credential (Re:
Max Concurrent Sessions (Read O
Auto-Provision Quota (Read Only)
Gy
default
Use Case Option
Use Case Option
Use Case Initiators
Documentation
Service Configurations
Service Configuration Parameters
Name
*Display Name
Add
Remove

Name: default

Use Case Option

- A child of Use Case Template used to add or modify Service Configurations objects when certain conditions occur.
- Provides a way to separate Service Configurations within a use case based on conditions.
- Contains the same functionality of a Use Case Template.
- Adds or modifies new service options from parent Use Case Template.

While copying a Use Case Option, all the corresponding children Use Case Options get copied as well.

For example, if a user's upload or download speed should be decreased when they are out of quota, a **Use Case Option** is added with a condition indicating the user is out of quota. The service configurations in the use case options can have a higher priority than those in the use case template to override the normal values. The service option then allows setting both the normal upload or download speed and the upload or download speed when the user is out of quota.

Service Example

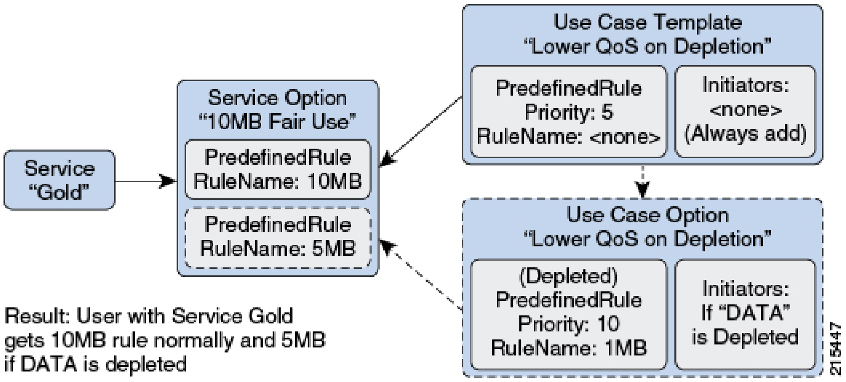
The following diagram illustrates how a 'Service Configuration' object called PredefinedRule can be flexibly configured as part of a service. For those unfamiliar, a predefined rule is just an identifier sent to PCEF which controls a users upload or download speed (QoS) among other things.

In this case, the service gold is assigned a Service Option called 10MB Fair Use. This service option results in a rule being passed to PCEF called 10MB by default and switching the rule to 5 MB when the users quota is depleted.

Notice that it would be easy to add another service option for 20MB Fair use, and so on.

The Use case template defines the low-level information that a 'PredefinedRule' be created of priority five. This rule is default and always present. Additionally, a Use Case Option defaults that another PredefinedRule of priority ten be added. The higher priority results in the new rule name being switched when quota is depleted.

Figure 101: Service Using Use Case Option

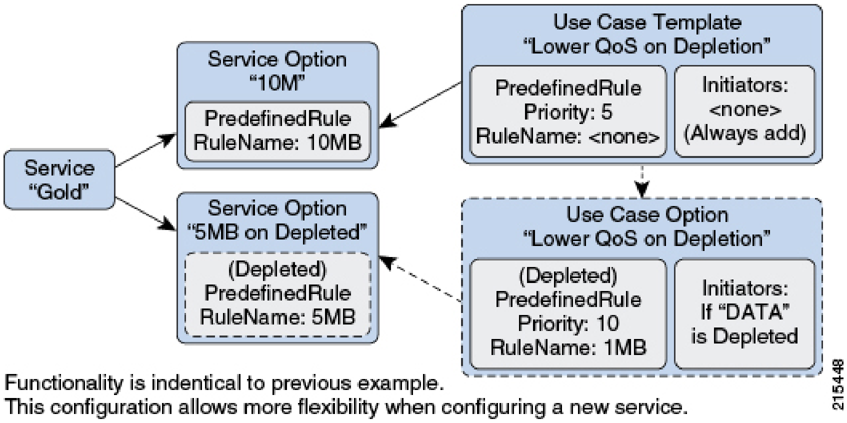


Instead of using a Use Case Option to define what happens when a user is depleted, they set up another Use Case Template.

This could have an advantage if a customer wanted services for a large combination of values (10 MB default with any combination of 1 MB - 9 MB depleted speed). Also, to support a use case where the end user could be independently assigned a default speed and a depleted or downgrade speed. A service for 10 MB default and 5 MB depleted would also be functionally equivalent.

This flexibility in the service model allows mapping CPS closely to the Service Providers concept of a service.

Figure 102: Service Using Use Case Template



Service Screens

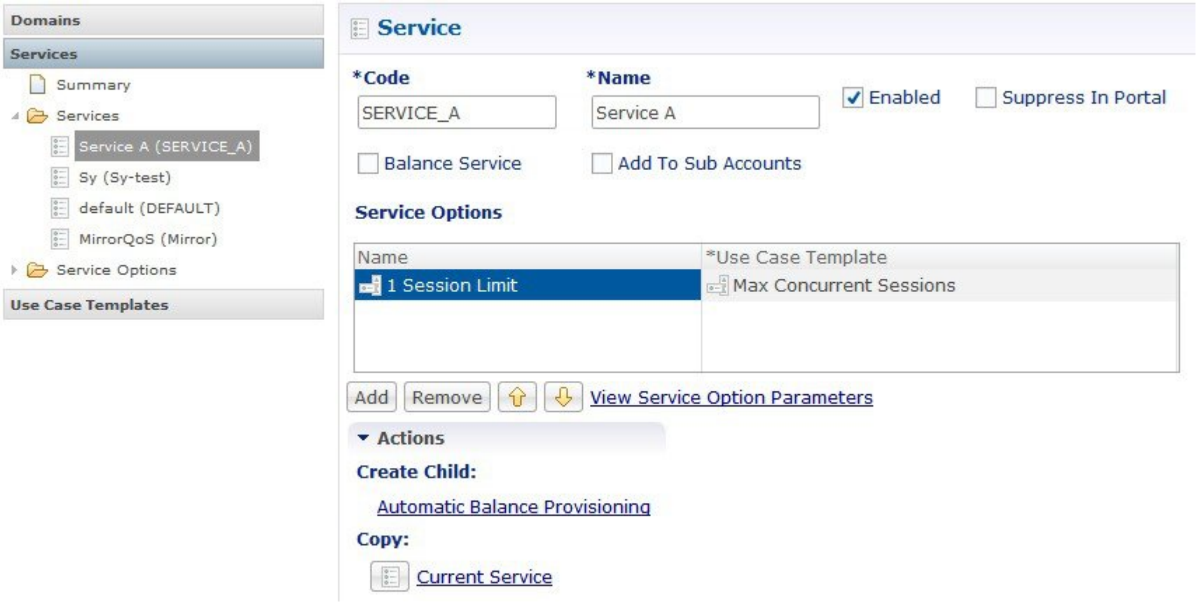
The following screens set up the example seen in the previous section. Service 'Gold' with two separate service options. The 'Predefined Rule' that is part of the setup is just an example, so not all fields on the Predefined Rule are described.

For example, a 'Rule Name' is a label and can be assigned to a subscriber on a PCEF. PCEF is responsible for defining what the rule 'means'. In this example, we make the assumption that PCEF has rules set up for '10_MB' and '5_MB' which control the users QoS (Quality of Service - effectively upload or download speed) to 10 MB upload or download and 5 MB upload or download respectively.

Note The subtle difference between 10 MB and '10_MB' is to ensure that it is clear which name is used for internal reference and which is sent to PCEF.

Services

Figure 103: Service Page



*Code: SERVICE_A

*Name: Service A

☑ Enabled □ Suppress In Portal

□ Balance Service □ Add To Sub Accounts

Service Options

Name	*Use Case Template
1 Session Limit	Max Concurrent Sessions

The following parameters can be configured under Service:

Table 98: Service Parameters

Parameter	Description
Code	This is what is saved on the subscriber. It defaults to 'default'. This value is the link between the Services assigned a subscriber in Control Center and the Service in Policy Builder. This value is not updated if existing users have it assigned, as the 'link' is be broken. Instead, the name is updated.
Name	This is the name displayed in Control Center.
Enabled	If this value is unchecked, the service is not evaluated by the Policy Engine and is not displayed in Control Center. Default value is checked (true).

Parameter	Description
Suppress in Portal	If this value is checked, this Service is not displayed in the Portal. This is specific for SP Wi-Fi call flows. Default value is unchecked (false). **Note** RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.
Balance Service	If this value is checked, the Service runs through balance processing. This results in one database read or write against the balance database. Performance improves (due to fewer database read or writes). For the services which don't rely on Balance or Quota, this value is unchecked. Default value is checked (true).
Add to Sub Accounts	If this value is checked, this service is considered to be also assigned to any 'subaccounts' associated to the main subscriber. This is useful if you had a family plan where the QoS is controlled at the main subscriber level and 'trickles down' to the family sub accounts rather than being set at each individual level. Default value is unchecked (false).

Service Options Table

This table displays a read-only version of the service options associated to the Service. Service Options can be added or removed to the service.

Table 99: Service Options Table Parameters

Parameter	Description
Name	The name of the associated Service Option.
Use Case Template	The name of the associated use case template.
Add	Allows adding another Service Option to this service. The Add dialog shows the Use Case Template > Service Option hierarchy on the left and a preview of the parameters set by the Service Option or Use Case Template on the right.
Remove	Removes a Service Option from the Service.
Up or Down Arrow	Allows moving a Service Option up or down. This only affects the ordering of service options in the list and does not functionally affect the resolution of services.

View Service Option Parameters

This hyperlink shows a consolidated list of the Service Configuration Parameters from the Use Case Template and Service Options. This view is useful for simple service options or use case templates. However, since it does not show the distinction between different Service Configuration objects. Hence, it can be difficult to read for more complicated configurations.

Service Options

The service option dialog allows setting the concrete values for service configuration parameters used in the Use Case Template. The groups under service options are Use Case Templates. Adding a new Use Case Template adds a new group under Service Options so you can provide concrete values for the Use Case Templates.

The following parameters can be configured under Service Option:

Table 100: Service Option Parameters

Parameter	Description
Name	This is the name of the service option which is referenced by the Service.
Use Case Template	This is a link that allows quickly seeing the associated Use Case Template and going straight to this Use Case Template. **Note** You can use the 'left' arrow in the Policy Builder toolbar to go 'back' to the service option after clicking into the Use Case Template.
Service Configurations	This is a list of the 'Service Configuration' objects that are to be set as part of the Service Option. This list can usually be used 'as is' upon creation. The Service Configuration objects from the Use case template is used as a default and any values set here 'overrides' the use case template. • Add: This allows adding a new Service Configuration that has been added to the Use Case Template. This is only really useful when a new Service Configuration object was added to a Use Case Template after this service option was created and you now what to override some values on this new object. • Remove: This is only really useful if you don't want to use your configured values at all and just use the values from the Use Case Template. In that case you can just remove the Service Configuration Objects and the values from the Use Case Template is used.
PreDefinedRule Parameters	These are the parameters being overridden from the use case template.
Add	This allows adding a parameter from the Use Case Template even if it is not marked as 'Allow Override'. It also allows customizing a parameter that didn't exist previously in the Use Case Template or was removed from the Service Option.
Remove	This allows removing a parameter from the Service Option. This means that the value specified for the Use Case Template's version of this parameter is used.
Display Name	This column shows the 'Display Name' of the parameter. This name can be updated by either the Service Option or the Use Case Template to make it clearer for users to understand what this value does. The 'true' name of the field can be seen by hovering over the cell.
Value	This is the value of the parameter which should be set. If there is a value set in the 'Pull Value From…' column, this value is used as the default and overridden with the 'Pull Value From…' information.

Parameter	Description
Pull Value From...	This allows setting this value dynamically through AVP's, Custom Reference Data or the 'Policy State'. For more information, refer to Table 101: Pull Value From..., on page 238.

Table 101: Pull Value From...

Parameter	Description
Subscriber AVP Code	This allows pulling values from AVPs on the subscriber. This field now also supports AVP's on the subscriber's session and 'Policy Derived AVP's added in policies.
Custom Reference Data Column	This allows pulling the value from the Custom Reference Data table's column specified. **Note** Custom Reference Data takes care of which 'row' in the column is matched, so this ends up specifying a single value.
Bind to Session/Policy State	This allows pulling the value from the state of the system. This uses any of the preconfigured 'Policy State Data Retrievers' that are plug-in code that know how to get a certain value from the system.
Dynamic Reference Data Key	This allows pulling the value from other reference data configuration (Policy Builder or CRD, for example, Account Balance Templates) as value for the use case attribute. Currently, only Account Balance Template type attributes are supported. The intended Account Balance Template code can be configured in the text field. Both Policy Builder and CRD Balance templates can be pulled using this field. Policy Builder templates are checked first, if not found then CRD templates are searched.

Use Case Templates

Use case templates form the basis of a service and are in general more complicated than creating a service or service option. For more information on creating Use Case Templates, contact your Cisco Technical Representative.

The following parameters can be configured under **Actions** (Use Case Template) tab:

Table 102: Actions (Use Case Template) Parameters

Parameter	Description
Name	This is the name used to identify the Use Case Template. It can be changed.

Parameter	Description
Service Configurations	This is where you add the Service Configuration objects needed to configure your use case. • Add: The Add button brings up the full list of Service Configuration objects. Which to choose should be based on the use case documentation you are implementing. The right column of the screen displays the parameters that are in a specific service configuration. If you 'uncheck' a parameter, the default as seen on this screen (from the code) will be utilized. Unchecking is functionally equivalent to 'removing' a field from the table after adding it. • Add New: Implies that you are adding a new Service Configuration to be configured. This is almost always what you want. • Modify: Implies that you are modifying an existing Service Configuration. This is used in a 'Use Case Option' and in general not recommended as it's preferred to use the 'priority' fields to update the service configuration objects.
Create Child: Use Case Option	This allows creating a child use case option of this use case template.
PreDefinedRule Parameters	
Add	This allows adding a parameter to the Use Case Template even if it wasn't added initially (unchecked or a code update added a new parameter).
Remove	This allows removing a parameter from the Use Case Template. This means that the value specified in the code (as seen on the Add Service Configuration screen) will be utilized.
Display Name	This column shows the 'Display Name' of the parameter. This name can be updated by either in the Use Case Template to make it clearer for users to understand what this value does. The 'true' name of the field can be seen by hovering over the cell.
Value	This is the value of the parameter which should be set. If there is also a value set in the 'Pull Value From…' column, this value will be used as the default and overridden with the 'Pull Value From…' information.
Pull Value From…	This allows setting this value dynamically through AVP's, Custom Reference Data or the 'Policy State'.
Allow Override	This value indicates whether this option will show up for configuration in the Service Option by default. In general, it is best to only check this box for values you expect to be configured in the Service Option. This will make it easier to configure and maintain the service options.

Use Case Initiators

Use Case Initiators are groups of conditions that indicate whether or not the Service Configuration objects within this use case template are used. If no use case initiators are specified, the Service Configuration objects will always be added.

The following parameters can be configured under the **Use Case Initiators** tab.

Table 103: Use Case Initiators Parameters

Parameter	Description
Service Initiators (OR Together)	Service Initiators are a grouping of conditions. If ANY of the service initiators on a Use Case Template are true then that Use Case template is active and the Service Configurations are used. When you add multiple Service Initiators, the Use Case Template is activated and Service Configurations are used when ANY one of these initiators are true, as indicated by the caption “(OR Together)”. • Plus/X: Lets the user add or remove a service initiator. • Up/Down arrow: The user can move the initiators up and down. This affects the order in which the service initiators are evaluated.
Initiator Name	This is a logical name for this grouping of conditions.
Conditions (AND Together)	These are the conditions associated with the service initiator. Conditions usually pertain to this messages session, subscriber information, balance information, or the message itself. The current values of the condition are set up by the code/messaging. When you add multiple conditions, ALL of the listed conditions must be true, as indicated by the caption “(AND Together)”. • Add/Remove: Lets the user add or remove a condition. • Up/Down arrow: Lets the user move a condition up or down in the list. This is usually only needed when referencing a previous condition in this condition. For example, the user can check a 'session exists' in the first condition and then use the 'session user name' in the second condition. The user can only reference previous conditions. • Input Variables (AND Together): These input variables are specific to each condition. If the current value of the condition matches the input variable, this condition is true. When you define multiple input variables for a condition, ALL of the variables are evaluated and must be true for the condition to be true, as indicated by the caption "(AND Together)". • Input Variable: This is the name of the variable. • Type: This is either 'Literal' matching where we match against a hard-coded 'value' or 'Output' where the value is pulled from a previous (or current) condition. If output is chosen, a popup will appear where the values from the current or previous conditions can be selected and the 'value' box is replaced with the selection. • Operator: This allows editing how 'true' is determined given the current value of the condition and the value specified. The default and by far most common option is '=' equals.

Parameter	Description
Operator	= (Equals): The condition is true if the values are equal. This uses the Java equals() function. Multiple value with comma separated is not allowed with = operator for string datatype.
	<> (Not Equals): The condition is true if the values are not equal.
	isNull: The condition is true if the value is null (empty).
	!isNull: The condition is true if the value is not null (empty).
	Matches: The condition is true and the value is a regex that successfully matches the current value. Java regex is utilized. Example: .* matches anything.
	[0-9]+: Matches 1 or more numbers.
	^[0-9]*$: Matches a string which is only numbers or empty.
	!matches: The logical opposite of matches (if matches would be true, !matches is false).
	In: This is true if the current value is equal to one of the values listed (comma separated).
	!In: This is the logical opposite of In (if In would be true; !In is false).
	Contains (Only for lists): True if the list contains the value or values.
	!Contains (Only for list): The logical opposite of contains.
	Value: This is the hard-coded value which should be compared against the current value in the system.
	Remove (link): This allows removing this input variable.

The following sections describe the input variables that can be configured for the following conditions:

A Customer Reference Data AVP Exists

This condition indicates that a custom reference data table exists in the Policy Builder configuration with one or more Column Names mapped to a unique Attribute Value pair. Any column marked as Use in conditions can be used.

In order to protect a customer reference column's integrity, once it has been created and published, it cannot be changed.

Note Under Use Case initiator tab for **A customer reference data AVP exists** condition, if you configure a regex expression that is a combination of multiple conditions, then specify each condition as a separate entry with AND together.

For example, instead of using the complex regex like “(?=MCC.*)(?!MCC1904)”, use two “A customer reference data AVP exists” condition (AND together). Configure one reference data with MCC.* and other reference data should not be equal to (<> as operator) MCC1904.

The following condition input variables can be exposed in the Policy Builder GUI:

Table 104: Available Input Variables used for A Customer Reference Data AVP Exists

Condition Input Variable	AVP Used/Description
tableName	The custom Reference Table Name.
code	The custom AVP column Name.
value	The custom AVP column’s value.

A Customer Reference Data AVP Does Not Exist

This condition indicates that a custom reference data table exists in the Policy Builder configuration with one or more Column Names not mapped to a unique Attribute Value pair. Any column, which is not marked as Use in conditions cannot be used.

In order to protect a customer reference column's integrity, once it has been created and published, it cannot be changed.

The input variables that can be exposed for this condition in the Policy Builder GUI are the same as described in A Customer Reference Data AVP Exists, on page 241.

A Diameter Gx TGPP Session Exists

This condition indicates that a valid Diameter Gx 3GPP session exists in the Policy Builder configuration for a given subscriber. The following condition input variables can be exposed in the Policy Builder GUI:

Table 105: Available Input Variables for Diameter Gx TGPP Session Exists

Condition Input Variable	AVP Used/Description
msisdn	The subscriber identity in the Subscription-Id AVP being msisdn.
imsi	The subscriber identity in the Subscription-Id AVP being imsi.
framedIpv6	The Ipv6 prefix allocated for the user.
framedIp	The Ipv4 address allocated for the user.
sessionId	The unique Id of the session generated by PCEF
commandCode	The unique Command Code to identify the Gx Request/Response Type – CCR/CCA or RAR/RAA.

Condition Input Variable	AVP Used/Description
requestType	The type of the request (initial, update, termination).
destRealm	The destination realm derived from the Origin-Realm of CCR-I and used in PCRF RAR request.
destHost	The destination host derived from the Origin-Host of CCR-I and used in PCRF RAR request.
ratType	Identifies the radio access technology that is serving the UE. PCRF supports devices using narrow band Internet of Things (NB-IoT) RAT that is a 3GPP radio interface to support IoT devices. PCRF can create a session with UE having RAT-type as NB-IOT and provides all functionalities (such as policy control and charging rule functionality) to an NB-IOT devices.
appId	The Unique Application Identifier to identify the Gx Session.
mccmnc	Concatenated value of Mobile Country Code (mcc) and Mobile Network Code.
calledStationId	The address the user is connected to. For GPRS the APN.
lac	Extracted from either the **3GPP-User-Location-Info** AVP, which provides details of where the UE is currently located, or the **RAI** AVP, which contains the Routing Area Identity of the SGSN where the UE is registered.
rac	Extracted from either the **3GPP-User-Location-Info** AVP, which provides details of where the UE is currently located, or the **RAI** AVP, which contains the Routing Area Identity of the SGSN where the UE is registered.
sac	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
ci	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
tgppRatType	**3GPP-RAT-Type** AVP. Indicates the Radio Access Technology that is currently serving the UE.
eventTriggers	NA
outofCredit	An OUT_OF_CREDIT trigger reported by **Event-Trigger** AVP.
cgi	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
Ecgi	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
Tai	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.

Condition Input Variable	AVP Used/Description
Sai	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
Tac	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
Eci	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
Imeisv	International Mobile Equipment Identifier along with Software Version. Extracted from **User-Equipment-Info-Value** AVP.
networkRequestSupport	**Network-Request-Support** AVP. Indicates whether or not the UE and access network supports the network requested bearer control mode.
Nai	The Network Access Identifier.
bearerControlMode	**Bearer-Control-Mode** AVP. Indicates the PCRF selected bearer control mode.
sgsnIpAddress	**3GGP-SGSN-Address** AVP. Indicates the Ipv4 address of the SGSN.
ipcanType	**IP-CAN-Type** AVP. Indicates the type of Connectivity Access Network in which the user is connected.
Mnc	Extracted from either the **3GPP-User-Location-Info** AVP, which provides details of where the UE is currently located or the **RAI** AVP, which Contains the Routing Area Identity of the SGSN where the UE is registered.
Mcc	Extracted from either the **3GPP-User-Location-Info** AVP, which provides details of where the UE is currently located, or the **RAI** AVP, which contains the Routing Area Identity of the SGSN where the UE is registered.
Rai	Extracted from either the **3GPP-User-Location-Info** AVP, which provides details of where the UE is currently located, or the **RAI** AVP, which contains the Routing Area Identity of the SGSN where the UE is registered.
qosUpgrade	**Qos-Upgrade** AVP. Indicates whether the SGSN Supports the QOS Upgrade or not.
sgsnIpv6Address	**3GPP-SGSN-IPv6-Address** AVP. Indicates the Ipv6 address of the SGSN.
targetApn	**Called-Station-Id** AVP. The same as called Station Id condition.
globalCiCode	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
globalAreaCode	Extracted from **3GPP-User-Location-Info** AVP. Provides details of where the UE is currently located.
imeiTac	Same as Imeisv extracted from **User-Equipment-Info-Value** AVP.
Mac	Extracted from **User-Equipment-Info-Value** AVP. The identification and capabilities of the terminal.

Condition Input Variable	AVP Used/Description
Eui64	Extracted from **User-Equipment-Info-Value** AVP. The identification and capabilities of the terminal.
modifiedEui64	Extracted from **User-Equipment-Info-Value** AVP. The identification and capabilities of the terminal.
qosNegotiation	**Qos-Negotiation** AVP. Indicates if the PCRF is allowed to negotiate the QoS.
Offline	**Offline** AVP. Defines whether the offline-charging interface from the TDF shall be enabled.
Online	**Online** AVP. Defines whether the offline charging interface from the TDF shall be enabled.
Ipv4AnGWAddress	IPv4 Gateway Address.
Ipv6AnGWAddress	IPv6 Gateway Address.
mpsEpsPriority	Value of the mspEpsPriority set.
tgppMsTimeZone	**3GPP-MS-TimeZone** AVP. Indicates the offset between universal time and local time in steps of 15 minutes of where the MS currently resides.
accessNetworkChargingAddress	**Access-Network-Charging-Address** AVP. Indicates the IP Address of the network entity within the access networks performing charging (e.g. the GGSN IP address).
usageReportET	NA
Meid	Extracted from **User-Equipment-Info-Value** AVP. The identification and capabilities of the terminal.
Bsid	Base Station Identifier.
chargingCharacteristics	**3GPP-Charging-Characteristics** AVP. The Charging Characteristics applied to the IP-CAN session.
chargingCharacteristicsBits	Extracted from **3GPP-Charging-Characteristics** AVP. The Charging Characteristics applied to the IP-CAN session
appName	Application Name.

A Diameter Gy v8 TGPP Session Exists

This condition indicates that a valid Diameter Gy v8 3GPP session exists in the Policy Builder configuration for a given subscriber. The following condition input variables can be exposed in the Policy Builder GUI:

Table 106: Available Input Variables for Diameter Gy v8 TGPP Session Exists

Condition Input Variables	AVP Used/Description
Msisdn	**Subscription-Id-Data** AVP. The identification of the subscription (IMSI, MSISDN, etc.).

Condition Input Variables	AVP Used/Description
sessionId	The unique Id of the session generated by PCEF.
requestType	**CC-Request-Type** AVP. The type of the request (initial, update, termination).
requestNumber	**CC-Request-Number** AVP. The number of the request for mapping requests and answers.
destRealm	**Destination-Realm** AVP. The destination realm derived from the Origin-Realm of CCR-I and used in PCRF RAR request.
destHost	**Destination-Host** AVP. The destination host derived from the Origin-Host of CCR-I and used in PCRF RAR request.
ratType	**3GPP-RAT-Type** AVP. Indicates the Radio Access Technology is currently serving the UE.
appId	**Auth-Application-Id** AVP. Used to advertise support of the Authentication and Authorization portion of an application.
ggsnIpAddress	**GGSN-Address** AVP. PGW Address Used.
Apn	**Called-Station-Id** AVP. Access Point Name Network Identifier.
sgsnMccmnc	**3GPP-SGSN-MCC-MNC** AVP. Serving node PLMN Identifier.
userLocationInfo	**3GPP-User-Location-Info** AVP. User Location Information.
sgsnIpAddress	**SGSN-Address** AVP. S-GW Address used.
sharedBucketReservationStatus	A boolean that indicate whether or not the sharedBucketReservation Status is set.
selectionMode	**3GPP-Selection-Mode** AVP. APN Selection Mode.
chargingCharacteristics	**3GPP-Charging-Characteristics** AVP. The Charging Characteristics applied to the IP-CAN session.
charingRuleBaseName	**Charging-Rule-Base-Name** AVP. Charging Rule Base Name.
eventTimeStamp	**Event-Timestamp** AVP. Corresponds to the exact time the accounting is requested.
chargingCharecteristicsBits	Extracted from **3GPP-Charging-Characteristics** AVP. The Charging Characteristics applied to the IP-CAN session.
appName	Application Name.
chargingID	**3GPP-Charging-Id** AVP. Charging ID.
userName	**User-Name** AVP. Contains the identification of the user.

A Diameter Sh v11 Session exists

The following condition input variables can be exposed in the Policy Builder GUI:

Table 107: Available Input Variables for Diameter Sh v11 Session Exists

Condition Input Variable	AVP Used/Description
Connected	A Boolean, which indicates whether a successful Sh Connection between PCRF and HSS is established, and a success Response (Diameter Result Code 20001) was received for the Sh requests (UDR/SNR).

A Diameter Sy v11 Session exists

This condition indicates that a valid Diameter Sy v11 session exists in the Policy Builder configuration for a given subscriber.

The following condition input variables can be exposed in the Policy Builder GUI:

Table 108: Available Input Variables for Diameter Sy v11 Session Exists

Condition Input Variable	AVP Used/Description
destRealm	Destination realm for Sy.
destHost	Destination host for Sy.
failureReason	The reason for failure in case Sy session is not established due to error (Last error code only).
destQueue	Destination queue (Internal field to know which policy director instance pick the request for processing).
retryTime	Retry timer in case connection fails.
lastSLReqType	Last spending limit request type.
lastSyResultCode	Last Sy result code.
syCountersIdentifierAndStatus	Sy counter identifier and status.
subscriberAccState	Subscriber account status.
slaReceived	A Boolean, set to true when a successful SLA-Initial is received.
sessionId	The unique id of the session.
connected	A Boolean, which indicates whether a successful Sy peer connection is established or not.

A Policy Derived AVP Exists

This condition indicates that a custom policy AVP that has been derived out of PolicyState exists in the system. The following condition input variables can be exposed in the Policy Builder GUI:

Table 109: Available Input Variables used for A Policy Derived AVP Exists

Condition Input Variable	AVP Used/Description
code	A derived AVP Name from the PolicyState.
value	A derived AVP value from the PolicyState.

The following AVPs are treated as Policy-Derived AVPs:

- Gx

  3GPP-MS-TimeZone and SN-Transparent-Data

  The following policy-derived AVP codes from the above AVPs can be used in the Use case Initiators:

  - UE HOUR OFFSET
  - UE MINUTE OFFSET
  - UE DST
  - UE DST
  - BganMonthlyFapVolume

- Rx

  Dynamic-PCC-Parameter AVP

  - Dynamic-PCC-APN-Aggregate-Max-Bitrate-DL
  - Dynamic-PCC-APN-Aggregate-Max-Bitrate-UL
  - DynamicPCC-Congestion-Level

- Profile Related Mapping

  The following profile related derived AVP codes can be used in the Use Case Initiators:

  - Sh Profile
  - LDAP Profile
  - SPR Profile
  - Additional ones

    Charging – congestionNextHourLevel

A Policy Derived AVP Does Not Exist

This condition indicates that a custom policy AVP that has been derived out of PolicyState does not exist in the system.

The input variables that can be exposed for this condition in the Policy Builder GUI are the same as those described in A Policy Derived AVP Exists, on page 247.

An APN Bearer Details exists

This condition indicates APN bearer details as received in Active Traffic Management attribute exists in PCRF. The following condition input variables can be exposed in the Policy Builder GUI:

Table 110: Available Input Variables for Diameter Gx TGPP Session Exists

Condition Input Variable	AVP Used/Description
stage	Stage string as received in Active Traffic Management Attribute notification from UDC FE. Valid value is string.
ackMode	Acknowledge mode QCI as received in Active Traffic Management Attribute notification from UDC FE. Valid value is an Integer.
unackMode	Unacknowledge mode QCI as received in Active Traffic Management Attribute notification from UDC FE. Valid value is an Integer.
logicalAPN	Logical APN string as received in Active Traffic Management Attribute notification from UDC FE. Valid value is string.
frontEndId	Front End ID string as received in Active Traffic Management Attribute notification from UDC FE. Valid value is string.
priority	Priority value as received in Active Traffic Management Attribute notification from UDC FE. Valid value is an Integer.

An APN Bearer Details does not exists

This condition indicates no APN bearer details exist in Active Traffic Management attribute in PCRF. The input variables that can be exposed for this condition in the Policy Builder GUI are the same as described in An APN Bearer Details exists , on page 249.

There Exists a Network Session

This condition indicates that a valid network session exists in the Policy Builder configuration for a given subscriber. The network session exists irrespective of the interface type – Gx/Gy/Sh/Sy.

The following condition input variables can be exposed in the Policy Builder GUI:

Table 111: Available Input Variables for There Exists a Network Session

Condition Input Variable	AVP Used/Description
Mac Address	The mac address present in the session.

Condition Input Variable	AVP Used/Description
User Id	User Identifier – Can be msisdn or extracted from Network Access Identifier.
Framed IP	**Framed-IP-Address** AVP. The Ipv4 address allocated for the user.
Start Time	When the session starts.
Access Type	How the subscriber is accessing network.
Imsi	The subscriber identity in the Subscription-Id AVP being imsi.
Msisdn	The subscriber identity in the Subscription-Id AVP being msisdn.
Cell Site Id	The ID of the cell tower.
End Time	If the session is set to end, this gets set.
Framed IPV6 Prefix	**Framed-IPv6-Prefix** AVP. The Ipv6 prefix allocated for the user.
Msbm Initialized	NA
Credential Id	The Subscriber Profile Repository credential.
Spr Version	Version loaded from SPR in case an update is needed.
Current Session Duration	How long the session has been going.
Next Evaluation Date	The time when CPS will wake itself up and re-evaluate the session if another message is not received.
Expiration Date	Used on soft delete to note when the session should be cleaned up

There does not exist a network session

This condition indicates that a valid network session does not exist in the Policy Builder configuration for a given subscriber. The network session does not exist irrespective of the interface type – Gx/Gy/Sh/Sy.

The input variables that can be exposed for this condition in the Policy Builder GUI are the same as described in There Exists a Network Session, on page 249.

ADTM Attribute Bearer Details Exists

This condition provides option to check for total of ACK mode, UNACK mode and combined for the subscriber across all the existing APNs.

The following condition input variables can be exposed in the Policy Builder GUI:

Table 112: Available Input Variables used for ADTM Attribute Bearer Details Exists

Condition Input Variable	AVP Used/Description
totalAckMode	Total ACK mode bearers (count) across all existing APNs for a subscriber. Valid value is an Integer.

Condition Input Variable	AVP Used/Description
totalUnAckMode	Total UNACK mode bearers (count) across all existing APNs for a subscriber. Valid value is an Integer.
totalCount	Total number of bearers (count) across all existing APNs for a subscriber. Valid value is an Integer.

A MSBMRolloverQuota exists

This condition is used to handle rollover use cases.

Note When rollover occurs for different rollover quotas (for same subscriber) at the same time, CPS sends a single notification with *Quota ID* as comma separated and consolidated roll-over amount. In such scenarios, it's highly recommended to configure rollover condition only with *rollOverOccur*.

The following condition input variables can be exposed in the Policy Builder GUI:

Table 113: Available Input Variables for MSBMRolloverQuota exists

Condition Input Variables	AVP Used/Description
rollOverOccur	Identifies rollover occurs or not. Value is **true** when rollover occurs.
accountBalance Code	Value will be account balance codes of rollover quota to which rollover occurs. If more than one rollover quota gets created at the same time, then value is a comma separated account balance codes.
quotaCode	Value will be quota codes of rollover quota to which rollover occurs. If more than one rollover quota gets created at the same time, then value is a comma separated quota codes.

Documentation

The documentation tab allows writing notes about the implementation which can be referred to later.

Custom Reference Data Tables

Overview

Custom Reference Data tables allow defining custom derived data for your installation and making decision based upon that data.

For example, a customer may not want to directly assign each subscriber a service so they get the appropriate QoS, instead, they want to derive the QoS based on data we get from the subscribers session. Custom Reference Data tables are the way to do that. Then (as per the previous section) we can wire the derived data directly into the service with the “Bind Field…” or “Pull Value From…” options.

Example

The following screens have a simple example setup. The example is that we want to derive the PCEF Rule Name based on the users APN (Access Point Name) and RAT (Radio Access Technology) name.

The logic is as follows:

Table 114: Example Table

APN	RAT	Rule Name	Rule Name Depleted
Cisco	3G	10_MB	5_MB
Cisco	Wi-Fi	20_MB	5_MB
Cisco	*	5_MB	1_MB
CiscoTest	3G	1_MB	5_KB
CiscoTest	Wi-Fi	2_MB	50_KB
*	*	1_MB	500_KB

The * (asterisk) can be read as a wildcard, but the table should match the 'most specific' entry. So, if my APN and RAT are Cisco and 3G, match the first row, not the 3rd row (Cisco, *) or the last row (*,*).

Note These values are for example purposes only. Things like the RAT type value have been simplified to make the example easier to understand.

Note RADIUS-based policy control is no longer supported in CPS 14.0.0 and later releases as 3GPP Gx Diameter interface has become the industry-standard policy control interface.

Screens

Search Table Groups

Search table groups allow grouping multiple Custom Reference Data Tables together logically, only executing the searching when needed. It also allows ordering the execution of tables so that tables can reference output of one table group in another to provide consistent and expected results. Additionally, Search Table Groups allows multiple different tables to populate the same AVPs in different ways.

Note Search table groups and their respective CRD tables are listed based on the evaluation order value. If the evaluation order value is same for two or more tables then they are listed alphabetically.

The following parameters are configured under Search Table Group:

Table 115: Search Table Group Parameters

Parameter	Description
Name	The name of the Search Table Group.
Evaluation Order	The order in which groups get evaluated, starting with 0 and going higher.
Results Columns	These are the AVPs that will be added into processing. These need to be mapped to be the same as values from underlying tables. This allows populating the same AVPs from different tables. • Name: The name of the AVP. It should start with alphanumeric characters, should be lowercase, and should not start with numbers, no special characters are allowed, use "_" to separate words. For example, logical_apn = GOOD, logicalAPN = BAD, no_spaces • Display Name: The more human readable name of the AVP. • Use In Condition: This represents whether this row will be available for conditions in Policies or Use Case Templates. There is a performance cost to having these checked, so we recommend not checking them unless they are required. Default value is checked (true). • Default Value: The default value if no results are found from a Custom Reference Data Table. • Add/Remove: Adds or removes a row from the table. • Up/Down: Allows ordering the list, but has no impact on processing.
Table Search Initiators (OR Together)	This section controls whether or not the Search Table Group and all tables below will be executed. When you add multiple Initiators to the Search Table Group, the search is activated when ANY one of these initiators are true, as indicated by the caption "(OR Together)". For more information, refer to table in section Use Case Initiators, on page 239.

Custom Reference Data Table

Policy Builder can be thought of as defining the 'schema' for the Custom Reference Data and the Control Center is responsible for filling out the schema.

Note Cisco recommends creating Custom Reference Data Tables under Search Table Groups. This allows you to specify the order in which the tables are searched and provide the default values if nothing is found. It is possible to re-parent a Custom Reference Data Table to another Search Table Group.

The following parameters can be configured under Custom Reference Data Table:

Table 116: Custom Reference Data Table Parameters

Parameter	Description
Name	This is the name of the table that is stored in the database. It must: • Start with alphanumeric characters • Have lowercase OR uppercase but no mixed case • Not start with numbers • Not have special characters • Use "_" to separate words For example, logical_apn = GOOD, logicalAPN = BAD, no_spaces.
Display Name	This is the name of the table that is displayed in Control Center.
Cache Results	This indicates whether the tables are cached in memory. This must be checked for production.
Activation Condition	This is the Custom Reference Data Trigger, which must be true before evaluating this table. This can be used to have multiple tables create the same data depending on conditions or to improve performance if tables are not required to be evaluated based on an initial condition.
Svn Crd Data	When enabled, indicates that the CRD table is an SVN CRD table and CRD data for the table is fetched from CRD CSV file present in SVN data source. When disabled, indicates that the CRD table data needs to be fetched from Mongo database.
Best Match	If checked, look-ups occur within a CRD table in the following order: • Exact string match • Higher priority regex match (if multiple regex patterns match) • Regular expression match (default behavior) • Wildcard character (*) For more information, refer to Best Match, on page 256.
Evaluation Order	This indicates the order the tables within the search table group should be evaluated. Starting with 0 and increasing.

Parameter	Description
Columns	Columns correspond to the schema for each column you are creating for this custom reference data table. • Name: The name of the column in the database. • Display Name: A more readable display name. • Use In Conditions: This represents whether this row is available for conditions in Policies or Use Case Templates. There is a performance cost to having these checked, so we recommend leaving them unchecked unless they are required. Default value is checked (true). • Type: the type determines what values are allowed when creating them in Control Center. • Text: The value is allowed to be any characters. For example, example123!. • Number: The value is allowed to be any whole number. For example, 1234. • Decimal: The value is allowed to be any number (including decimals). For example, 1.234. • True or False: The value must be true or false. For example, true. • Date: The value is a date without a time component (May 17th, 2020). • DateTime: The value is a date + time (May 17th, 2020 5:00pm). • Key: This indicates that this column is all or part of the key for the table that makes this row unique. By default, a key is required. Keys are also allowed to set the Runtime Binding fields to populate the data from the current message and session. Typically, keys are bound to data from the current session (APN, RAT Type) and other values are derived from them. Keys can also be set to a value derived from another custom reference data table. • Required: This indicates whether this field is marked required in Control Center. A key is always required.
Valid Values	These are the valid values which are allowed in Control Center (creates a list box). • List of Valid Values: A list of name and display name pairs which are used to create the list. Valid values can also contain a name which is the actual value of the column and a display value which allows Control Center to display an easier to use name. • Valid Values pulled from another Table: This allows initializing the list based on another custom reference data table. The name value is pulled from another table. There is no way to customize a display name in this manner.

Parameter	Description
Validation	The validation set here is checked by the Control Center before allowing a row to be added. • Regular Expression: This is the Java regular expression that is run on the proposed new cell value to validate it as described here. • Regular Expression Description: This is a message to the user indicating what the regular expression is trying to check.
Runtime Binding	Runtime binding is how key column data gets filled out (bound) from data in the current session. There are multiple ways to bind this data and it is also possible to set an operator to define what must match (equals, less than, and so on). • Bind to Subscriber AVP Code: This pulls the value from an AVP on the subscriber. It also pulls values from a session AVP or a Policy Derived AVP. • Bind to Session and Policy State Field: This pulls the value from a Policy State Data Retriever which knows how to retrieve a single value for a session The following Policy State Data Retrievers cannot be used for binding in CRD Tables: • Gx Predefined Charging Rules Retriever • Gx Charging Rulebase Names Retriever • Sd TDF Application Id List Retriever • Bind to a Result Column from another Table: This allows the key to be filled out from a columns value from another table. This allows normalizing the table structure and not having a large table with many duplicated values. • Bind to Diameter Request AVP code: This allows the key be filled out from an AVP on the Diameter request. • Matching Operator: This allows the row to be matched in other ways than having the value be equals. Default value is equals. • eq: Equal • ne: Not Equal • gt: Greater than • gte: Greater than or equal • lt: Less than • lte: Less than or equal

Best Match

CRD best match uses a hierarchical structure to perform match. The hierarchical structure is based on the input columns that is, key columns. The order of the input column is important in this hierarchy.

The data in the CRD table is cached in memory according to the hierarchy described in the following section:

Values in the first column are the root of the hierarchy. Number of unique values in the first column creates those many hierarchies. Then under the root, the values of the second key column similarly create those many children, and so on, and so forth, for other columns in the order.

While performing the best match, the value for the first column is used to select the root of the hierarchy. Once the root is selected, then the next match is performed only under the selected hierarchy so on, and so forth, for the children. At any level, first exact match is performed, if that fails then the pattern match is performed. Once the root or the child is selected, next search for the remaining column is restricted only to that hierarchy.

Example 1

If there are four columns in a best match table that is, {A,B,C,D} out of which key columns are {A,B,C} and output column is D and the table has the following values:

A	B	C	D
1	2	3	4
1	*	3	5
1	*	*	6
*	2	3	7

This results in the hierarchy as follows:

```
{1=
      {2=
            {3=4}
      {*=
            {3=5}
            {*=6}
{*=
      {2=
            {3=7}
```

In the hierarchy, following input {4,6,3} results in no output. 4 matches "*" hierarchy thereby restricting the next input key to have only value 2 and the other key to have only value 3.

Regex Example:

Regex can be assigned priority by using numbers such as, "match1=" instead of "match=". The higher the number, higher is the priority.

Table 117: First Column is the Output Column

Test1	"a"	"b"	"*"
Test2	"a"	"b"	"c"
Test3	"*"	"b"	"d"
Test4	"*"	"*"	"*"
Test5	"a"	"c"	"*"

Test6	"*"	"*"	"7"
Test7	"a"	"match=[a-zA-Z]"	"*"
Test8	"a"	"7"	"match=[a-zA-Z]"
Test9	"a"	"match=[a-zA-Z]"	"1"
Test10	"a"	"match=[a-zA-Z]"	"2"
Test11	"Internet"	" match=P03.*"	"2001"
Test12	"Internet"	"match3=P03-Sy.*"	"2001"
Test13	"Internet"	"match2=P03-S.*"	"2001"
Test14	"Internet"	"match2=P03-[abc].*"	"2001"
Test15	"Internet"	"match1=P03-.*"	"2001"
Test16	"Internet"	"match3=P03-Gy.*"	"2001"

Table 118: Output with following Input

("a", "b", "4")	("Test1")
("a", "b", "c")	("Test2")
("7", "b", "d")	("Test3")
("7", "b", "e")	("Test4")
("a", "c", "4")	("Test5")
("a", "c", "7")	("Test5")
("a", "3", "7")	("Test6")
("a", "dd", "7")	("Test6")
("a", "7", "7")	("Test6")
("a", "W", "79")	("Test7")
("a", "7", "a")	("Test8")
("a", "W", "1")	("Test9")
("a", "W", "2")	("Test10")
("Internet", "P03", "2001")	("Test11")
("Internet", "P03-Sy", "2001")	("Test12")
("Internet", "P03-S", "2001")	("Test13")

("Internet", "P03-a", "2001")	("Test14")
("Internet", "P03-", "2001")	("Test15")
("Internet", "P03-Gy", "2001")	("Test16")

Example 2

Based on first key column (if all first key columns are same, then based on second key column and so on):

1. CPS selects root node of the search and gives preference to that row to continue the search in that row.
2. While traversing from top to bottom, this root node selection happens by giving preference to exact match.
3. If there is a priority configured, CPS gives preference to that row irrespective of the position of the row (except exact match scenario).

   In case column values are same and one row has priority and other does not, then CPS ignores the row with the priority.

If there are four columns in a best match table that is, {A,B,C,D} out of which input columns are {A,B,C} and output column is D:

For example, if M, A_B, 12.2 are the first three inputs in the following rows, other are outputs:

- **Case 1:**

A	B	C	D
match=R|P|M	match=^(A?_)?B$| ^(A?_)?B_C.	*	Test1
match=M|S	match=^A_B.*	12.2	Test2

  In this case, while traversing from top to bottom, CPS took the Row1 and continued the search and was able to satisfy the input.

- **Case 2:** Here Row2, first column has exact match for input, so preference is given to Row2.

A	B	C	D
match=R|P|M	match=^(A?_)?B$| ^(A?_)?B_C	*	Test1
MYPHONE	match=^A_B.*	12.2	Test2

  In this case, based on first key, column Row2 is chosen (as it is exact match for the input) and search is continued in Row2. If Row2 search fails, then preference is given to Row1.

- **Case 3:** In case of priority configuration, root node is selected based on the priority (if exact match is present, then CPS goes for exact match row).

A	B	C	D
match=M	match=^A_B.*	12.2	Test2

A	B	C	D
match1=R| P|M	match=^(A?_)?B$ | ^(A?_)?B_ C.*	^B_C.*	Test1

In this case Row2 has the priority. CPS selects Row2 as the root node and takes Row2 as output, or else it goes for Row1.

- **Case 3a:** When first column has priority but has same values, then priority is ignored.

A	B	C	D
match=R| P|M	match=^A_B.*	12.2	Test2
match1=R| P|M	match=^(A?_)?B$ | ^(A?_)?B_ C.*	^B_C.*	Test1

In this case, Row1 is the output.

Custom Reference Data Trigger

A custom reference Data Trigger is group of conditions that can be used to decide whether to evaluate a table or not. This can be used to derive the same data in different ways depending on conditions.

Refer to Use Case Initiators, on page 239 as it is identical in function of setting up conditions and only different in what it is used for.

OOC and ROC Policy CRD Event Trigger Configuration

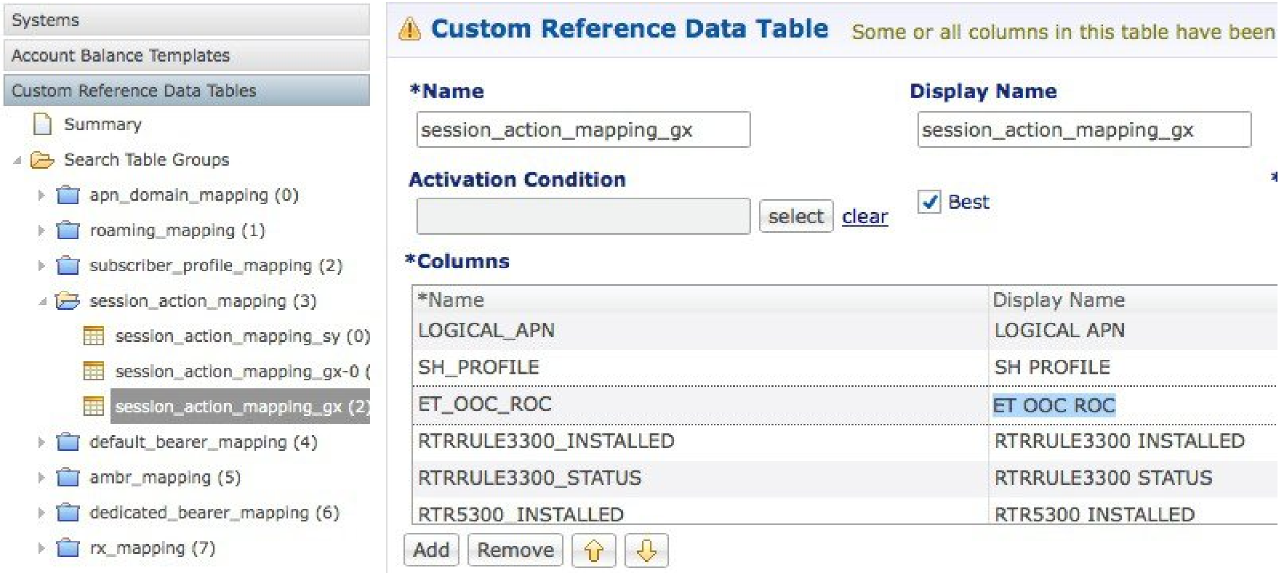
To enable a trigger for Out of Credit (OOC) and Retrieval of Credit (ROC) events, you must configure the Gx Out of Credit Retriever event in the session_action_mapping_gx CRD table. The configuration is used in conjunction with the other columns in the Session_Actions_Gx table in Control Center to derive the actions in the Session_Action output column.

Step 1 In Policy Builder, select the **Reference Data** tab.

Step 2 In the left pane, select **Custom Reference Data Tables** > **Search Table Groups** > **session_action_mapping** > **session_action_mapping_gx**.

Step 3 In the **Custom Reference Data Table** pane under **Columns**, select **ET_OOC_ROC** in the **Display Name** column.

Figure 104: ET OOC ROC Column Display Name



Systems
Account Balance Templates
Custom Reference Data Tables
Summary
Search Table Groups
apn_domain_mapping (0)
roaming_mapping (1)
subscriber_profile_mapping (2)
session_action_mapping (3)
session_action_mapping_sy (0)
session_action_mapping_gx-0 (
session_action_mapping_gx (2)
default_bearer_mapping (4)
ambr_mapping (5)
dedicated_bearer_mapping (6)
rx_mapping (7)
Custom Reference Data Table
Some or all columns in this table have been
select
clear
Add
Remove

*Name: session_action_mapping_gx

Display Name: session_action_mapping_gx

Activation Condition:

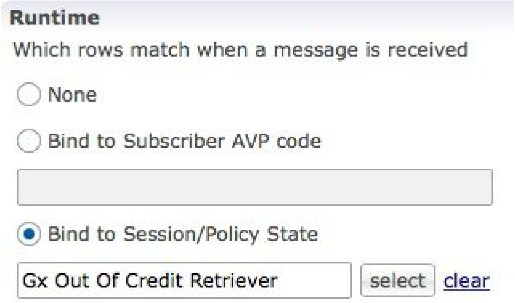
☑ Best

*Columns

*Name	Display Name
LOGICAL_APN	LOGICAL APN
SH_PROFILE	SH PROFILE
ET_OOC_ROC	ET OOC ROC
RTRRULE3300_INSTALLED	RTRRULE3300 INSTALLED
RTRRULE3300_STATUS	RTRRULE3300 STATUS
RTR5300_INSTALLED	RTR5300 INSTALLED

Step 4 In the **Runtime** area, select the **Bind to Session/Policy State** option, and click **Select**.

Figure 105: Bind to Session/Policy State Option



Runtime

Which rows match when a message is received

○ None

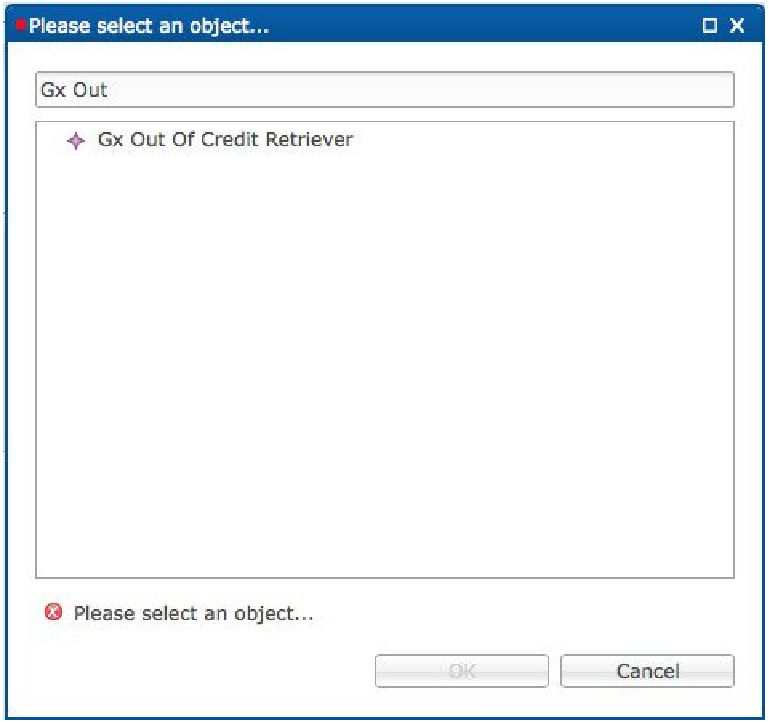
○ Bind to Subscriber AVP code

● Bind to Session/Policy State

Gx Out Of Credit Retriever

Step 5 In the **Please select an object** dialog box, locate and select **Gx Out Of Credit Retriever**, and click **OK**.

Figure 106: Gx Out Of Credit Retriever Object


Please select an object...
Gx Out
Gx Out Of Credit Retriever
Please select an object...
OK
Cancel

In the CCR-U message, the PCEF/PGW sends the following AVPs:

```
<messageid="CCR_U_01"appInterface="GX_TGPP">
<avp name="Charging-Rule-Report">
     <avp name="Charging-Rule-Name" value="SessionAction-Table_output-Column"></avp>
</avp>
```

The following AVP is sent for an Out of Credit event:

```
<avpname="Event-Trigger" value="15"></avp>
```

The following AVP is sent for a Reallocation of Credit event:

```
<avp name="Event-Trigger" value="16"></avp>
```

Expose Rules Installed to Policy CRD

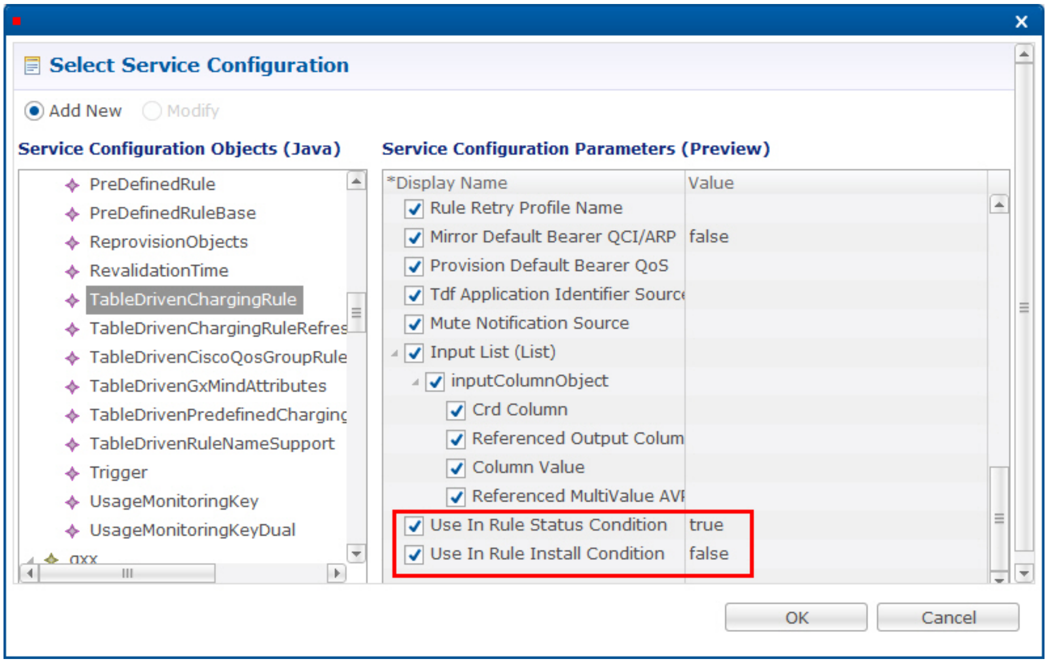
Two parameters have been provided in the Gx PreConfiguredRule, TableDrivenChargingRule, and TableDrivenPredefinedChargingRule service configuration objects to expose installed PCC rules to the policy engine to be used for policy decisions in the CRD. These parameters are described below:

- Use In Rule Status Condition – Controls whether or not the PCC rule reported status AVPs are created. By default, this parameter is set to **true** for PreConfiguredRule and TableDrivenChargingRule, and to **false** for TableDrivenPredefinedChargingRule.
- Use in Rule Install Condition – Controls whether or not the PCC rule installed AVPs are created. By default, this parameter is set to false.

Note To expose installed PCC rules to the policy CRD, you must set this parameter to true.

These parameters are shown in the following two figure as they appear in the TableDrivenChargingRule and PreConfiguredRule service configuration objects.

Figure 107: TableDrivenChargingRule



Select Service Configuration

● Add New ○ Modify

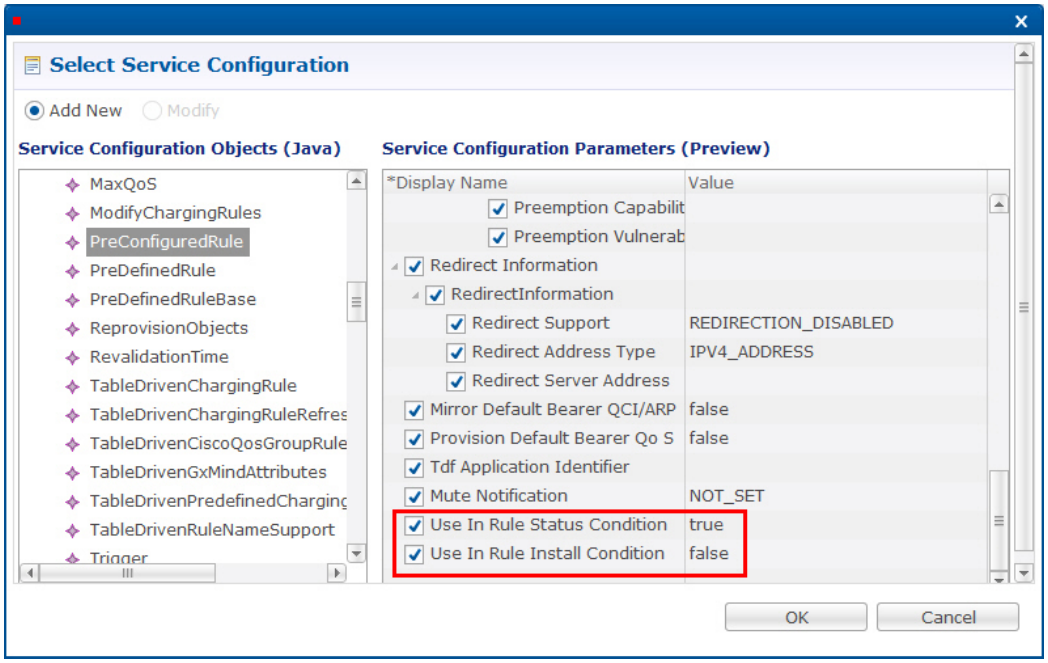
Service Configuration Objects (Java)

- PreDefinedRule
- PreDefinedRuleBase
- ReprovisionObjects
- RevalidationTime
- TableDrivenChargingRule
- TableDrivenChargingRuleRefres
- TableDrivenCiscoQosGroupRule
- TableDrivenGxMindAttributes
- TableDrivenPredefinedChargin
- TableDrivenRuleNameSupport
- Trigger
- UsageMonitoringKey
- UsageMonitoringKeyDual
- gxx

Service Configuration Parameters (Preview)

*Display Name	Value
☑ Rule Retry Profile Name	
☑ Mirror Default Bearer QCI/ARP	false
☑ Provision Default Bearer QoS	
☑ Tdf Application Identifier Sourc	
☑ Mute Notification Source	
☑ Input List (List)	
☑ inputColumnObject	
☑ Crd Column	
☑ Referenced Output Colum	
☑ Column Value	
☑ Referenced MultiValue AVI	
☑ Use In Rule Status Condition	true
☑ Use In Rule Install Condition	false

Figure 108: PreConfiguredRule



Select Service Configuration

● Add New ○ Modify

Service Configuration Objects (Java)

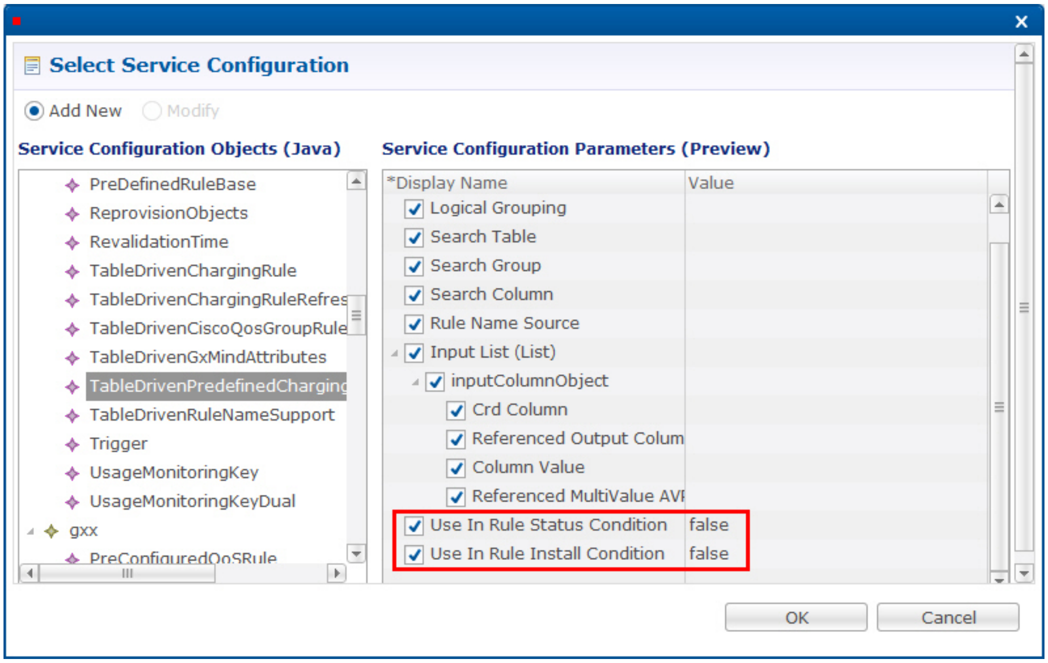
- MaxQoS
- ModifyChargingRules
- PreConfiguredRule
- PreDefinedRule
- PreDefinedRuleBase
- ReprovisionObjects
- RevalidationTime
- TableDrivenChargingRule
- TableDrivenChargingRuleRefres
- TableDrivenCiscoQosGroupRule
- TableDrivenGxMindAttributes
- TableDrivenPredefinedCharging
- TableDrivenRuleNameSupport
- Trigger

Service Configuration Parameters (Preview)

*Display Name	Value
☑ Preemption Capabilit	
☑ Preemption Vulnerab	
☑ Redirect Information	
☑ RedirectInformation	
☑ Redirect Support	REDIRECTION_DISABLED
☑ Redirect Address Type	IPV4_ADDRESS
☑ Redirect Server Address	
☑ Mirror Default Bearer QCI/ARP	false
☑ Provision Default Bearer Qo S	false
☑ Tdf Application Identifier	
☑ Mute Notification	NOT_SET
☑ Use In Rule Status Condition	true
☑ Use In Rule Install Condition	false

The following figure shows the two parameters as they appear in the TableDrivenPredefinedChargingRule service configuration object.

Figure 109: TableDrivenPredefinedChargingRule



Select Service Configuration

● Add New ○ Modify

Service Configuration Objects (Java)

- PreDefinedRuleBase
- ReprovisionObjects
- RevalidationTime
- TableDrivenChargingRule
- TableDrivenChargingRuleRefres
- TableDrivenCiscoQosGroupRule
- TableDrivenGxMindAttributes
- TableDrivenPredefinedCharging
- TableDrivenRuleNameSupport
- Trigger
- UsageMonitoringKey
- UsageMonitoringKeyDual
- gxx
- PreConfiguredQoSRule

Service Configuration Parameters (Preview)

*Display Name	Value
☑ Logical Grouping	
☑ Search Table	
☑ Search Group	
☑ Search Column	
☑ Rule Name Source	
☑ Input List (List)	
☑ inputColumnObject	
☑ Crd Column	
☑ Referenced Output Colum	
☑ Column Value	
☑ Referenced MultiValue AVI	
☑ Use In Rule Status Condition	false
☑ Use In Rule Install Condition	false

In the CCR-U request, the PCEF/PGW sends the following AVPs:

```
<avp name="Charging-Rule-Report">
      <avp name="Charging-Rule-Name" value="DTL3300"> </avp>
```

```
        <avp name="PCC-Rule-Status" value="0"> </avp>
</avp>
```

You must also configure your CRD table by binding the **<*RuleName*>_installed** column with RI-<*RuleName*> and by binding the **<*RuleName*>_Status** column with RS-<*RuleName*>.

Step 1 In Policy Builder, select the **Services** tab.

Step 2 In the left pane, click **Services**.

Step 3 Navigate to any service options that use the PreConfiguredRule, TableDrivenChargingRule, and TableDrivenPredefinedChargingRule service configuration objects, and change their **Use In Rule Install Condition** parameters to **true**.

Step 4 In Policy Builder, select the **Reference Data** tab.

Step 5 In the left pane, select **Custom Reference Data Tables** > **Search Table Groups**.

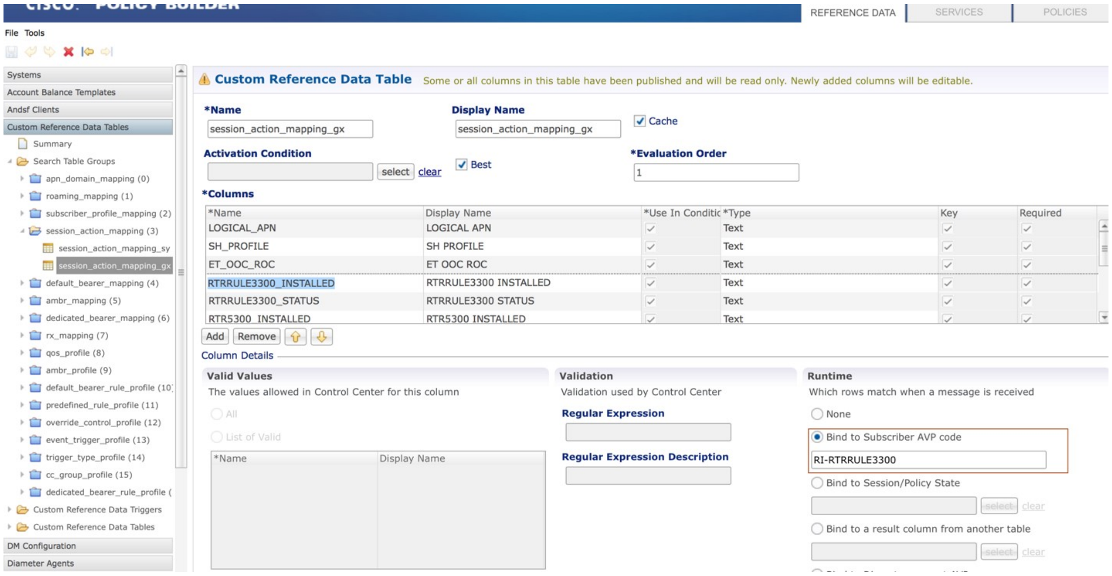
Step 6 Go to your CRD table; for example, under **session_action_mapping** > **session_action_mapping_gx**.

Step 7 In the **Custom Reference Data Table** pane under **Columns**, select **<*Rulename*>_Installed**.

Step 8 In the **Runtime** area, select the **Bind to Subscriber AVP code** option, and type **`RI-<RuleName>`**.

An example is shown in the following figure.

Figure 110: Binding to RI-RTRULE3300 Subscriber AVP code


CISCO. POLICY BUILDER
REFERENCE DATA
SERVICES
POLICIES
File
Tools
Systems
Account Balance Templates
Andsf Clients
Custom Reference Data Tables
Summary
Search Table Groups
apn_domain_mapping (0)
roaming_mapping (1)
subscriber_profile_mapping (2)
session_action_mapping (3)
session_action_mapping_sy
session_action_mapping_gx
default_bearer_mapping (4)
ambr_mapping (5)
dedicated_bearer_mapping (6)
rx_mapping (7)
qos_profile (8)
ambr_profile (9)
default_bearer_rule_profile (10
predefined_rule_profile (11)
override_control_profile (12)
event_trigger_profile (13)
trigger_type_profile (14)
cc_group_profile (15)
dedicated_bearer_rule_profile (
Custom Reference Data Triggers
Custom Reference Data Tables
DM Configuration
Diameter Agents
Add
Remove
select
clear

Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

*Name: session_action_mapping_gx
Display Name: session_action_mapping_gx
☑ Cache
Activation Condition:
☑ Best
*Evaluation Order: 1

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
LOGICAL_APN	LOGICAL APN	✓	Text	✓	✓
SH_PROFILE	SH PROFILE	✓	Text	✓	✓
ET_OOC_ROC	ET OOC ROC	✓	Text	✓	✓
RTRRULE3300_INSTALLED	RTRRULE3300 INSTALLED	✓	Text	✓	✓
RTRRULE3300_STATUS	RTRRULE3300 STATUS	✓	Text	✓	✓
RTR5300_INSTALLED	RTR5300 INSTALLED	✓	Text	✓	✓

Column Details

Valid Values
The values allowed in Control Center for this column
○ All
○ List of Valid

*Name	Display Name

Validation
Validation used by Control Center
Regular Expression:
Regular Expression Description:

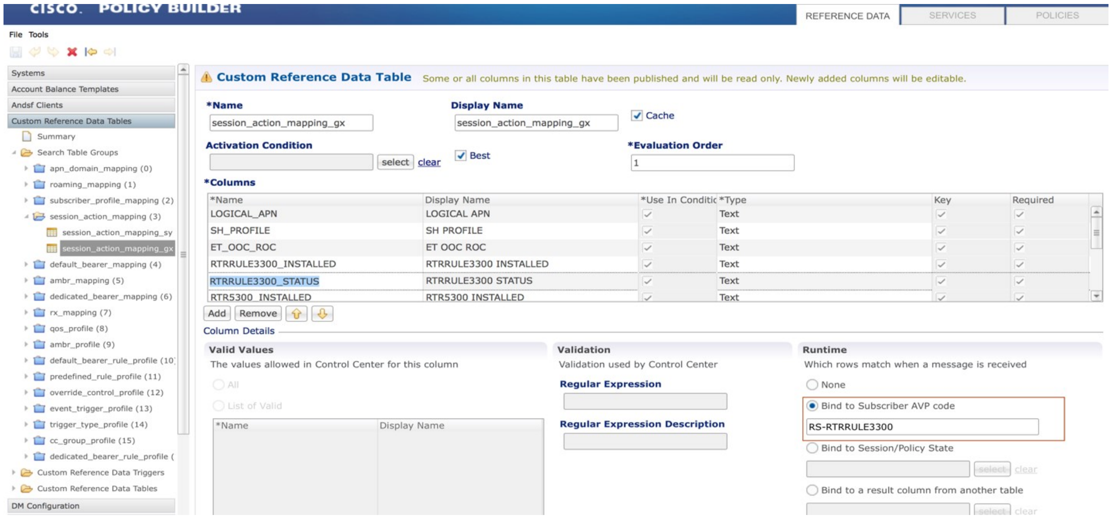
Runtime
Which rows match when a message is received
○ None
● Bind to Subscriber AVP code: RI-RTRRULE3300
○ Bind to Session/Policy State
○ Bind to a result column from another table

Step 9 Select <***RuleName***>**_STATUS** under **Columns**.

Step 10 In the **Runtime** area, select the **Bind to Subscriber AVP code** option, and type **`RS-<RuleName>`**.

An example is shown in the following figure.

Figure 111: Binding to RS-RTRULE3300 Subscriber AVP code


CISCO. POLICY BUILDER
REFERENCE DATA
SERVICES
POLICIES
File
Tools
Systems
Account Balance Templates
Andsf Clients
Custom Reference Data Tables
Summary
Search Table Groups
apn_domain_mapping (0)
roaming_mapping (1)
subscriber_profile_mapping (2)
session_action_mapping (3)
session_action_mapping_sy
session_action_mapping_gx
default_bearer_mapping (4)
ambr_mapping (5)
dedicated_bearer_mapping (6)
rx_mapping (7)
qos_profile (8)
ambr_profile (9)
default_bearer_rule_profile (10
predefined_rule_profile (11)
override_control_profile (12)
event_trigger_profile (13)
trigger_type_profile (14)
cc_group_profile (15)
dedicated_bearer_rule_profile (
Custom Reference Data Triggers
Custom Reference Data Tables
DM Configuration
Add
Remove
select
clear

Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

***Name** session_action_mapping_gx

Display Name session_action_mapping_gx

☑ Cache

Activation Condition

☑ Best

***Evaluation Order** 1

***Columns**

*Name	Display Name	*Use In Conditic	*Type	Key	Required
LOGICAL_APN	LOGICAL APN	✓	Text	✓	✓
SH_PROFILE	SH PROFILE	✓	Text	✓	✓
ET_OOC_ROC	ET OOC ROC	✓	Text	✓	✓
RTRRULE3300_INSTALLED	RTRRULE3300 INSTALLED	✓	Text	✓	✓
RTRRULE3300_STATUS	RTRRULE3300 STATUS	✓	Text	✓	✓
RTR5300_INSTALLED	RTR5300 INSTALLED	✓	Text	✓	✓

Column Details

Valid Values

The values allowed in Control Center for this column

○ All

○ List of Valid

*Name	Display Name

Validation

Validation used by Control Center

Regular Expression

Regular Expression Description

Runtime

Which rows match when a message is received

○ None

● Bind to Subscriber AVP code

RS-RTRRULE3300

○ Bind to Session/Policy State

○ Bind to a result column from another table

CHAPTER 8

Gx/Sd Services

Gx Services

This section covers the following topics:

QoS Profile

Overview

When UE attaches to the network for the first time, it will be assigned default bearer which remains as long as UE is attached. Default bearer is best effort service. Each default bearer comes with an IP address.

This section provides details of Gx default bearer QoS parameters and also explains how CPS derives QoS in different configurations.

Policy Builder Configuration

Case 1- QoS under Gx Profile

Step 1 Log into Policy Builder.

Step 2 Select the **Reference Data** tab, and click **Diameter Defaults** > **Gx Profile**.

Step 3 On the right side, click **Create Child** to the open the **Gx Profile** pane.

Case 2 - Default Bearer QoS in Service

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

Step 4 Enter the name for use case template.

Step 5 Select **Actions** tab.

Step 6 Click **Add** under **Service Configurations** to open the **Select Service Configuration** dialog box.

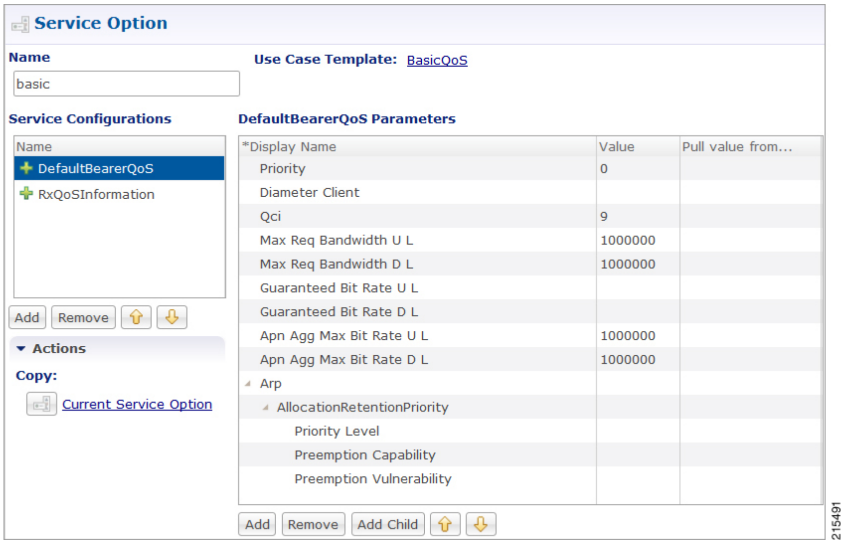
Step 7 Select **DefaultBearerQoS** under **gx** and select the required service configuration parameters.

Step 8 Click **OK** to add the service in the **Service Configuration** pane.

Step 9 On the **Services** tab, click **Services** > **Service Options** to create a service option, and add the use case template that the user just configured.

An example is shown.

Figure 112: Creating a Service Option



Service Option

Name: basic

Use Case Template: BasicQoS

Service Configurations

Name
DefaultBearerQoS
RxQoSInformation

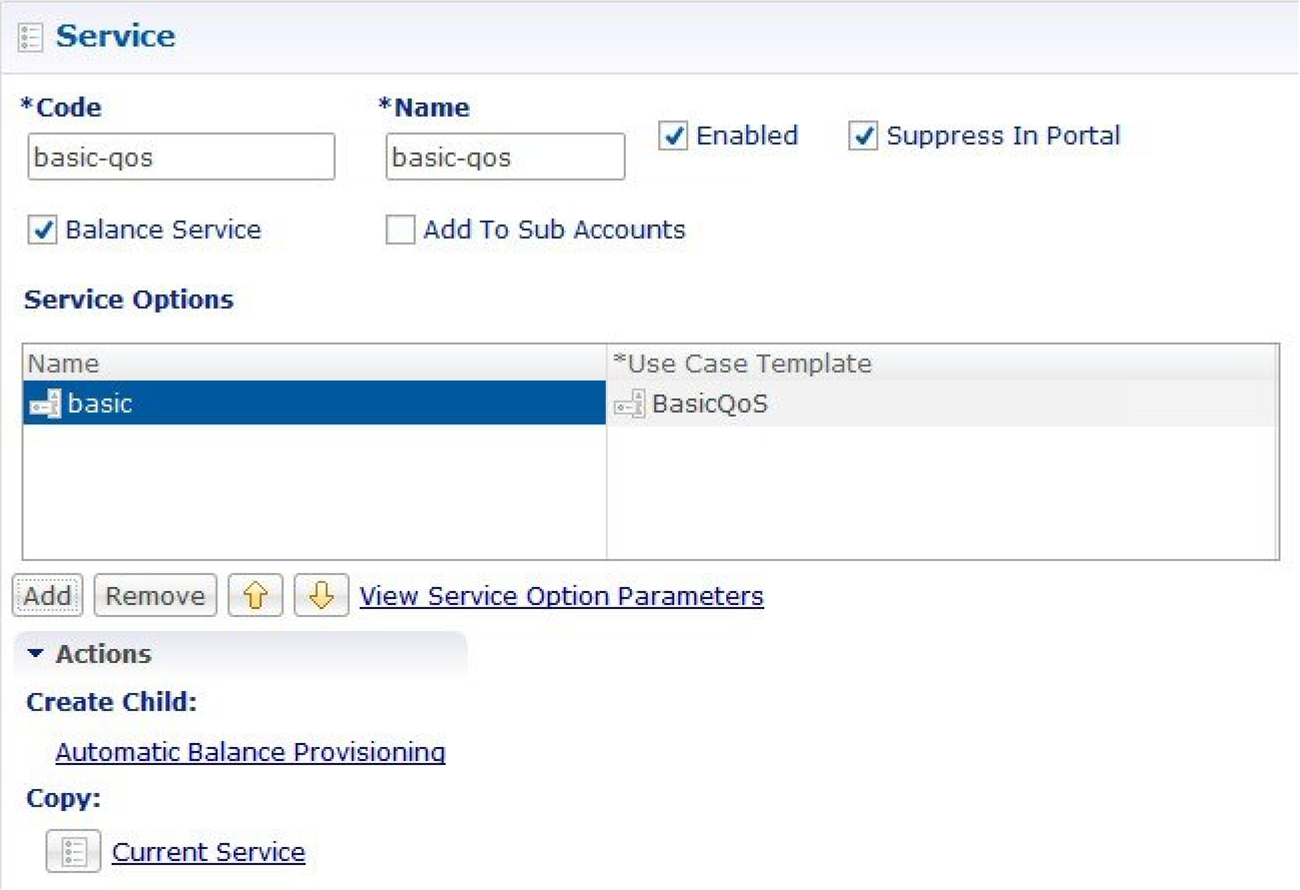
DefaultBearerQoS Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Qci	9	
Max Req Bandwidth U L	1000000	
Max Req Bandwidth D L	1000000	
Guaranteed Bit Rate U L		
Guaranteed Bit Rate D L		
Apn Agg Max Bit Rate U L	1000000	
Apn Agg Max Bit Rate D L	1000000	
Arp		
AllocationRetentionPriority		
Priority Level		
Preemption Capability		
Preemption Vulnerability		

Step 10 On the **Services** tab, click **Services** > **Services** to create a service, and add the same use case template.

An example is shown.

Figure 113: Creating a Service



Service

*Code: basic-qos

*Name: basic-qos

☑ Enabled ☑ Suppress In Portal

☑ Balance Service ☐ Add To Sub Accounts

Service Options

Name	*Use Case Template
basic	BasicQoS

Add
Remove
View Service Option Parameters
Actions
Create Child:
Automatic Balance Provisioning
Copy:
Current Service

Default Bearer QoS Enhancements - Gx

CPS supports the management of Default Bearer QoS attribute values for IP-CAN sessions by applying QoS-Bounding, QoS-Mirroring and QoS-Enforced on Default Bearer QoS and these actions for individual QoS attributes can be derived based on SPR or Gx session attributes.

- QoS-Bounding is the ability for the PCRF to calculate the minimum QoS between the Requested QoS (from the P-GW) and the Authorized QoS (based on internal computation of the Logic in the PCRF) and assign that in the response message back to the P-GW.
- QoS-Mirroring is the ability for the PCRF to mirror the same QoS values back that were being requested by the P-GW in the Request Message.
- QoS-Enforcement is the ability for the PCRF to enforce the Authorized QoS computed based on its internal logic back to the P-GW in the request/response message.

To support QoS Enhancements, the user can configure object DefaultBearerQoSAction with action attribute for each possible QoS attribute and bind to the QoS action columns of the Default Bearer CRD. Also CPS binds the DefaultBearerQoS service configuration object attributes to QoS columns of the Default Bearer CRD.

CPS when sends or receives a Gx request message then it needs to do a lookup from CRD tables for a match of input attributes and perform calculation of DefaultBearer QoS using values from the output attributes and the default configured in service. The QoS Actions are also applicable to PreConfigured Rules defined in CPS service configurations and are used to calculate the QoS-Information grouped AVPs of such charging rules.

CPS after calculation of default bearer QoS applies the QoS actions bounding, mirroring and enforcement to each attribute of current calculated QoS. A new class QoSInformationActions is used to override the QoS calculated from the QoSInformation and assigning the values as defined by CRD table and corresponding action from DefaultBearerQoSAction.

The DefaultBearerQoS calculations explained above are applied if the service configuration contains the service object DefaultBearerQoSAction.

CPS also supports the Gx TGPP session to store the last received QoS parameters from PCEF/PGW which helps in evaluating the QoS during CCR-U or RAR trigger.

CPS also supports QoS calculations for MPS and it takes precedence over QoS Actions while calculating default bearer QoS.

The **QoS-Information AVP** (AVP code 1016) is of type Grouped, and it defines the QoS information for resources requested by the UE, an IP-CAN bearer, PCC rule, QCI or APN. When this AVP is sent from the PCEF to the PCRF, it indicates the requested QoS information associated with resources requested by the UE, an IP CAN bearer or the subscribed QoS information at APN level.

When the QoS-Information AVP is provided within the CCR command along with the RESOURCE_MODIFICATION_REQUEST event trigger, the QoS-information AVP includes only the QoS-Class-Identifier AVP and Guaranteed-Bitrate-UL and/or Guaranteed-Bitrate-DL AVPs.

The Allocation-Retention-Priority AVP is an indicator of the priority of allocation and retention for the Service Data Flow.

- **QCI**: The QoS-Class-Identifier AVP (AVP code 1028) is of type Enumerated, and it identifies a set of IP-CAN specific QoS parameters that defines the authorized QoS, excluding the applicable bitrates and ARP for the IP-CAN bearer or service flow. Possible values: 1 - 9.
    - 1: Conversational Traffic class
    - 2: Conversational Traffic class
    - 3: Streaming
    - 4: Streaming
    - 5 to 8: Interactive
    - 9: Background
- **ARP**: The Allocation-Retention-Priority AVP (AVP code 1034) is of type Grouped, and it is used to indicate the priority of allocation and retention, the pre-emption capability and pre-emption vulnerability for the SDF if provided within the QoS-Information-AVP or for the EPS default bearer if provided within the Default-EPS-Bearer-QoS AVP.

Note The Priority-Level AVP of the default bearer will be set to a sufficiently high level of priority to minimize the risk for unexpected PDN disconnection or UE detach from the network according to operator specific policies.

AVP Format:

```
Allocation-Retention-Priority ::= < AVP Header: 1034 >
                     { Priority-Level }
                     [ Pre-emption-Capability ]
                     [ Pre-emption-Vulnerability ]
```

MIRRORING ACTION

Table 119: Mirroring Action

CCR (INPUT)	Calculated QoS Value	QoS Action	CCA (OUTPUT)
MBR[3]	MBR	MIRROR	MBR
GBR[4]	GBR	MIRROR	GBR
QCI [5]	QCI	MIRROR	QCI
ARP[6]	ARP	MIRROR	ARP

[3] Maximum -Bit-Rate

[4] Guaranteed-Bit-Rate

[5] QoS-Class-Identifier AVP

[6] Allocation-Retention-Priority

ENFORCING ACTION

Table 120: Enforcing Action

CCR (INPUT)	Calculated QoS Value	QoS Action	CCA (OUTPUT)
MBR	MBR	ENFORCE	MBR
GBR	GBR	ENFORCE	GBR
QCI	QCI	ENFORCE	QCI
ARP	ARP	ENFORCE	ARP

BOUNDING ACTION

Italics text: In the Table 121: Bounding Action, on page 272, the *MBR*, *GBR*, *QCI*, and *PL* represents values received in CCR request (CCR (INPUT)).

Bold text: In the Table 121: Bounding Action, on page 272, **MBR**, **GBR**, **QCI**, and **PL** represents values calculated internally in CPS (Calculated QosS Value).

Table 121: Bounding Action

CCR (INPUT)	Calculated QoS Value	QoS Action	CCA (OUTPUT)
MBR	MBR	BOUND	min(*MBR*, **MBR**) CCA value for the MBR AVP is minimum of *MBR* and **MBR**.
GBR	GBR	BOUND	min(*GBR*, **GBR**) CCA value for the GBR AVP is minimum of *GBR* and **GBR**.
QCI	QCI	BOUND	max(*QCI*, **QCI**) CCA value for the QCI AVP is maximum of *QCI* and **QCI**.
ARP-PL[7]	ARP-PL	BOUND	max(*PL*, **PL**) and PV, PC based on chosen ARP
ARP-PV	ARP-PV	BOUND	Set based on PL. IF PL comes from CCR set CCR Value, or retain Granted QoS Values
ARP-PC	ARP-PC	BOUND	Set based on PL. IF PL comes from CCR set CCR Value, or retain Calculated/Granted Values

[7] The Priority-Level AVP (AVP code 1046) is of type Unsigned 32. The AVP is used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest priority level. Values 1 to 8 should only be assigned for services that are authorised to receive prioritised treatment within an operator domain. Values 9 to 15 may be assigned to resources that are authorised by the home network and thus applicable when a UE is roaming.

Note If the received and calculated PL values are equal, then the configured/calculated (not received) ARP is considered for PCI and PVI.

Creating the CRD Table

The user must take special care while defining the CRD table to avoid an unconditional loop in case CRD uses cross referencing data from one table to another table.

Step 1 Log into Policy Builder.

Step 2 Select the **Reference Data** tab.

Step 3 Click **Custom Reference Data Tables** and create a CRD table.

Step 4 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 5 Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

Step 6 Enter the name for use case template.

Step 7 Select **Actions** tab.

Step 8 Click **Add** in the **Service Configuration** pane to open the **Select Service Configuration** dialog box.

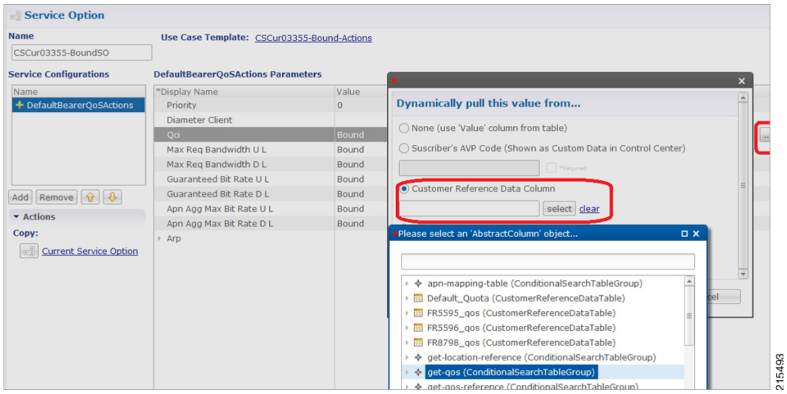
Step 9 Select **DefaultBearerQoSActions** and click **OK** to add it in the **Service Configurations** pane.

Step 10 Click **DefaultBearerQoSActions** to open the parameters pane on the right side.

Note By default, **Enforce** is selected.

Use the following table if the user wants to bind QoS with the CRD table.

Figure 114: Custom Reference Data Column



Service Option

Name: CSCur03355-BoundSO

Use Case Template: CSCur03355-Bound-Actions

Service Configurations

Name: DefaultBearerQoSActions

DefaultBearerQoSActions Parameters

*Display Name	Value
Priority	0
Diameter Client	
Qci	Bound
Max Req Bandwidth U L	Bound
Max Req Bandwidth D L	Bound
Guaranteed Bit Rate U L	Bound
Guaranteed Bit Rate D L	Bound
Apn Agg Max Bit Rate U L	Bound
Apn Agg Max Bit Rate D L	Bound
Arp	

Dynamically pull this value from...

○ None (use 'Value' column from table)

○ Suscriber's AVP Code (Shown as Custom Data in Control Center)

● Customer Reference Data Column

Please select an 'AbstractColumn' object...

- apn-mapping-table (ConditionalSearchTableGroup)
- Default_Quota (CustomerReferenceDataTable)
- FR5595_qos (CustomerReferenceDataTable)
- FR5596_qos (CustomerReferenceDataTable)
- FR8798_qos (CustomerReferenceDataTable)
- get-location-reference (ConditionalSearchTableGroup)
- get-qos (ConditionalSearchTableGroup)
- get-qos-reference (ConditionalSearchTableGroup)

When the use case template is used in a Service Options, the user can bind each DefaultBearerQoSAction service object action attribute to the QoS action columns of the CRD. Similar binding of DefaultBearerQoS service configuration object attributes to QoS columns of the Default Bearer CRD can be done.

Step 11 Log into the Control Center to define the values for the parameters defined in Custom Reference Data tables.

Step 12 Select the **Configuration** tab.

Step 13 Under **Reference Data**, click the **Custom Reference Data Table** name to open a dialog box. Select a row and edit the values according to the user requirements.

Parameter Descriptions

The following table contains a list of common parameters:

Table 122: QoS Profile - Common Parameters

Parameter	Description
Grant Requested QoS	It controls whether the requested QoS should be granted or not as the default bearer QoS. Default value is unchecked.
Gx Client QoS Exclusion List	Gx client names that are allowed not to have a default bearer QoS installed.

Parameter	Description
Grant Requested QoS Over Global QoS	If this option is selected then the requested QoS should be granted even if the global QoS is provisioned. There are three types of QoS: • From service • From default QoS • From requested If this flag is checked then requested QoS takes priority over default QoS. Default value is unchecked.

Note For description/usage of other parameters, see Common Steps, on page 285.

Default Bearer QoS Algorithm

Table 123: Default Bearer QoS Algorithm

Service Configuration	Requested QoS	Granted QoS	
Yes	Yes	Follow the rules mentioned in QoS Authorization Algorithm, on page 274for Granted QoS calculation.	
Yes	No	Granted configured.	
No	Yes	Reference data parameter value is “Yes”.	Grant requested QoS. CPS can throttle the user based on the use case.
		Reference data parameter value is “No”.	Grant QoS using defaults values. If default values are not available, reject the request. CPS must define Gx QoS defaults like QCI, bit rates.
No	No	Grant QoS using defaults values. If default values are not available, reject the request. CPS must define Gx QoS defaults like QCI, bit rates.	

QoS Authorization Algorithm

CPS uses the following rules to calculate granted QoS. For default bearer, configured QoS refers to Default-Bearer-QoS and for dedicated bearers configured QoS refers to Max-QoS.

Table 124: QoS Authorization Algorithm

IP-CAN-Type/RAT-Type	Evaluation Criteria	Granted QoS		
IP-CAN:GPRS RAT Type: Any	Evaluate QoS-Upgrade, QoS-Negotiation	QoS-Negotiation	QoS-Upgrade	Result
		Yes	Yes	If Requested QoS > configured QoS: Grant Configured If Requested QoS < configured QoS: Upgrade to configured
		Yes	No	Requested QoS > configured QoS: Grant configured QoS Requested QoS < configured QoS: Grant Requested QoS
		No	Yes	Requested QoS > configured QoS: Reject with BEARER_NOT_AUTHORIZED Requested QoS < configured QoS: Grant Requested QoS
		No	No	Requested QoS > configured QoS: Reject with BEARER_NOT_AUTHORIZED Requested QoS < configured QoS: Grant Requested QoS
=3GPP-EPS, RAT-Type = GERAN/UTRAN/EUTRAN	Evaluated based on IP-CAN-Type	Provision both QoS-Information and Default-EPS-Bearer-QoS. If Requested QoS > configured QoS: Grant Configured QoS If Requested QoS < configured QoS: Upgrade to configured QoS		
	If RAT-Type is GERAN	Follow the rules as in IP-CAN-Type GPRS.		
IP-CAN-Type=Non-3GPP-EPS	Evaluate based on IP-CAN-Type	Provision both QoS-Information and Default-EPS-Bearer-QoS.		
IP-CAN-Type=DOCSIS (1), xDSL (2), WiMAX (3), 3GPP2 (4)	Evaluate based on IP-CAN-Type	Reject CCR request with DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143) result code.		

PCC Rules

Overview

The purpose of the PCC rule is:

- To detect a packet belonging to an SDF to map that packet to proper IP-CAN bearer in downlink and uplink direction
- To identify the service
- To provide appropriate applicable charging
- To provide policy control

There are two different types of PCC rules:

- Dynamic PCC rules: These PCC rules are dynamically provisioned by PCRF to PCEF over Gx interface.
  - Pre-configured dynamic rules: These rules can be configured using Policy Builder
  - Dynamic generated rules: These rules can be generated by CPS e.g., as result of Rx interaction.
- Pre-defined PCC rules: These PCC rules are pre-configured in the PCEF. The PCRF can advise the PCEF to activate a set of PCC rules over Gx interface.

CPS can be configured to re-attempt to install PCC rules that fail to install or activate. See Rule Retry Profiles, on page 173 for more information.

Policy Builder Configuration

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *PreConfiguredRule*.

Step 4 Enter the name for use case template. For example, name the new template as **PreConfiguredRule**.

Step 5 Select **Actions** tab.

Step 6 Click **Add** to open the **Select Service Configuration** dialog box.

Step 7 Select **PreConfiguredRule**, **PreDefinedRule**, and **PreDefinedRuleBase** one after another, and select the required service configuration parameters.

Step 8 Click **OK** to add the service in the **Service Configuration** pane.

A PCC rules consists of following parameters:

Table 125: PCC Rules Parameters

Parameter	Description
Service Identifier	The service identifier is used to identify a service or service component the SDF relates to.
charging key and charging parameters	online or offline charging
Flow status	Defines whether the service data flow is enabled (2) or disabled (3).
Rating Group	The charging key for the PCC rule used for rating purposes.

Parameter	Description
Service Identifier	The service identifier is used to identify the service or the service component the service data flow relates to.
Reporting Level	The Reporting-Level AVP is of type Enumerated, and it defines on what level the PCEF reports the usage for the related PCC rule.There are three types of reporting levels: • SERVICE_IDENTIFIER_LEVEL (0): This value shall be used to indicate that the usage shall be reported on service id and rating group combination level, and is applicable when the Service-Identifier and Rating-Group have been provisioned within the Charging-Rule-Definition AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. • RATING_GROUP_LEVEL (1): This value shall be used to indicate that the usage shall be reported on rating group level, and is applicable when the Rating-Group has been provisioned within the Charging-Rule-Definition AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. • SPONSORED_CONNECTIVITY_LEVEL (2): This value shall be used to indicate that the usage shall be reported on sponsor identity and rating group combination level, and is applicable when the Sponsor-IdentityAVP, Application-Service-Provider-Identity AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging.
Metering Method	The Metering-Method AVP (AVP code 1007) is of type Enumerated, and it defines what parameters shall be metered for offline charging. The PCEF may use the AVP for online charging in case of decentralized unit determination and having three values: • DURATION (0): This value shall be used to indicate that the duration of the service data flow shall be metered. • VOLUME (1): This value shall be used to indicate that volume of the service data flow traffic shall be metered. • DURATION_VOLUME (2): This value shall be used to indicate that the duration and the volume of the service data flow traffic shall be metered.
Precedence	Indicates the precedence of QoS rules or packet filters.
Retry Profile	Indicates the Rule Retry Profile to be used. Upon receipt of a Charging-Rule-Report indicating the failure to install or activate one or more rules, CPS will evaluate the failed rules and take further action. See Rule Retry Profiles, on page 173 for more information.

Step 9 On the **Services** tab, click **Services** > **Service Options** to create a service option and add the configured use case template.

Note To activate a predefined charging rule at PCEF, charging rule name must be used as a reference to the predefined charging rule. To activate a group of predefined charging rules within PCEF (For example, Gold users or gaming services) charging rule base name must be used as a reference to the group of predefined charging rules.

Step 10 On the **Services** tab, click **Services** > **Services** to create a service and add the configured use case template.

Table (CRD) Driven Rules

Overview

ASR5K supports handling of Service Group QoS and defines new Gx AVPs which are exchanged between PCEF and PCRF. Additionally, CPS (PCRF) already supports various use cases related to PCC Rules provisioning and usage monitoring control as defined in 3GPP specification 29.212. Also, the new AVPs related to CISCO Service Group QoS are already supported in CPS.

This feature uses capabilities of Custom Reference Data tables and Search Table Group functionality of CPS.

CPS supports defining a Custom Reference Data table where in all sub-elements of Cisco QoS Group rules are possible to be configured with different values for each element. Also, it is possible to group these rules under a logical group. The application at run time supports queries based on this configured logical group, and Search Table Group, and is able to retrieve all applicable CISCO Service QoS Group rules and its sub-elements.

This feature can be configured by using three service options namely, TableDrivenCiscoQosGroupRule (For Cisco QoS Group rules), TableDrivenChargingRule (For dynamic PCC rules), and TableDrivenPredefinedChargingRule (For predefined PCC charging rules) . Description of their common parameters is listed in the following table.

Note Currently, Table Driven Rules does not support wildcards.

Table 126: Common Parameters between TableDrivenCiscoQosGroupRule, TableDrivenChargingRule, and TableDrivenPredefinedChargingRule

Parameter	Description
Search Group	Search Group is a constant value which CPS uses to search within the Search Table Group indicated by “Search Table” element.
Search Column	Search Column must be bound to the Key column of the STG (which must be given a data type of Text).
Rule Name Source	Rule Name Source must be a key column as well. This filed must be bound to the rule name column within the STG which should be Text.

Table 127: Common Parameters between TableDrivenCiscoQosGroupRule and TableDrivenChargingRule

Parameter	Description
Flow Status Source	Flow Status Source must be bound to the Flow status column within the STG which should be Text.
Monitoring key Source	Monitoring key Source must be bound to the Monitoring Key column within the STG which should be Text.
Encoding format Source	Encoding format Source must be bound to the Encoding format column within the STG which should be either Boolean or Text. If this is defined as Text Data Type then Valid Values must be provided as (True/False).
Redirect Enabled Source	Redirect Enabled Source must be bound to the Redirect Enabled column within the STG which should be either Boolean or Text. If this is defined as Text Data Type then Valid Values must be provided as (True/False).
Redirect Address Type Source	Redirect Address Type Source must be bound to the Redirect Address Type column within the STG which should be Text.
Redirect Address Source	Redirect Address Source must be bound to the Redirect Address column within the STG which should be Text.
Use Override Server Address	Use Override Server Address must be bound to the Use Override Server Address column within the STG which should be either Boolean or Text. If this is defined as Text Data Type then Valid Values must be provided as (True/False). If this flag is true then it will take the address from the service option and if it is false then it would not override the redirect server address.

Table 128: Common Parameters between TableDrivenChargingRule and TableDrivenPredefinedChargingRule

Parameter	Description
Input List (List)	
Crd Column	The Crd column is bound to the appropriate key column within the STG for those AVPs which are inputs to this table.
Referenced Output Column	Reserved for future use.
Column Value	The value of the AVP that is bound to the Crd Column and has a single value.
Referenced MultiValue AVP Name	The name of the attribute that is bound to the Crd Column and has multiple values.

Policy Builder Configuration

Table Driven Cisco QoS Group Rule

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *TableDrivenCiscoQosGroupRule*.

a) Enter the name for use case template. For example, name the new template as **TableDrivenCiscoQoSGroupRule**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.

Select Service Configuration dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select **TableDrivenCiscoQoSGroupRule**.

Step 4 Select **Services** > **Summary**.

Step 5 Click the **Service Option** link from the right side under **Actions** to create a service option using the *TableDrivenCiscoQosGroupRule* use case template.

For usage of common parameters, see Common Parameter Descriptions, on page 508.

Step 6 To bind the **Value**, select the name from the **Display Name** column and in **Value** column click **....** to open **Please select a 'CustomerReferenceDataTable' object**.

See Common Steps, on page 285 to continue with the configuration.

Table Driven Charging Rule

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then select **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for Table Driven Charging Rule.

a) Enter the name for use case template. For example, name the new template as **TableDrivenChargingRule**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.

Select Service Configuration dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select **TableDrivenChargingRule**.

Step 4 Select **Services** > **Summary**.

Step 5 Click the **Service Option** link from the right side under **Actions** to create a service option using the *TableDrivenChargingRule* use case template.

For usage of common parameters, see Common Parameter Descriptions, on page 508. Other parameters can be configured as follows:

Table 129: TableDrivenChargingRule Parameters

Parameter	Description
Online Source	Online Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.

Parameter	Description
Offline Source	Offline Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.
Rating Group Source	Rating Group Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.
Service Id Source	Service Id Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.
Reporting Level Source	Reporting Level Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.
Precedence Source	Precedence Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.
Metering Method Source	Metering Method Source must be bound to the appropriate column within the STG, and Type should be Number. The possible values are mentioned in 3GPP specification 29.212.
Flow Information Source	Flow Information Source must be bound to the appropriate column within the STG, and Type should be Text. **Note** A particular format should be used when adding Flow Information Source parameter so that CPS can perform proper Flow Information grouped AVP mapping. A wrongly formatted Flow Information Source can result in missing AVPs under Gx Flow Information AVP. Here is the format: **`<Flow-Description>;<Flow-Direction>;<Decimal value of first octet of ToS-Class-AVP>;<Decimal value of second octet of ToS-Class-AVP>`**
Use Override Server Address	Use Override Server Address must be bound to the appropriate column within the STG, and Type should be either True/False or Text. If this is defined as Text Type then valid values must be provided as True/False.
Override Server Address	Override Server Address is a constant value and if the Use Override Server Address flag is set to False, the parameter value is ignored.
Qci Source	Qci Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Max Req Bandwidth U L Source	Max Req Bandwidth U L Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Max Req Bandwidth D L Source	Max Req Bandwidth D L Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.

Parameter	Description
Guaranteed Bit Rate U L Source	Guaranteed Bit Rate U L Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Guaranteed Bit Rate D L Source	Guaranteed Bit Rate D L Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Arp Priority Level Source	Arp Priority Level Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Arp Preemption Capability Source	Arp Preemption Capability Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Arp Preemption Vulnerability Source	Arp Preemption Vulnerability Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Apn Agg Max Bit Rate U L Source	Apn Agg Max Bit Rate U L Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Apn Agg Max Bit Rate D L Source	Apn Agg Max Bit Rate D L Source must be bound to the appropriate column within the STG, and Type should be Number. For more information, refer to Common Parameters Used, on page 317.
Rule Retry Profile Name	Rule Retry Profile Name must be bound to the appropriate column within the STG, and Type should be Text. For more information, refer to Common Parameters Used, on page 317.
Provision Default Bearer Qo S	Provision Default Bearer Qo S must be bound to the appropriate column within the STG, and Type should be either True/False or Text. If Type is defined as Text, then valid values must be provided as True/False. If the value is True, the Default Bearer QoS information from the session is applied to the rule while QoS information derived from the above parameters in this STG are ignored.
Tdf Application Identifier Source	Tdf Application Identifier Source references the application detection filter (for example, its value may represent an application such as a list of URLs, etc.), which the PCC rule for application detection and control in the PCEF applies. Tdf Application Identifier Source must be bound to the appropriate column within the STG, and Type should be Text.
Mute Notification Source	An indication whether application start/stop notification is to be muted for ADC Rule by the TDF. Mute Notification Source must be bound to the appropriate column within the STG, and it should be either Number or Decimal.

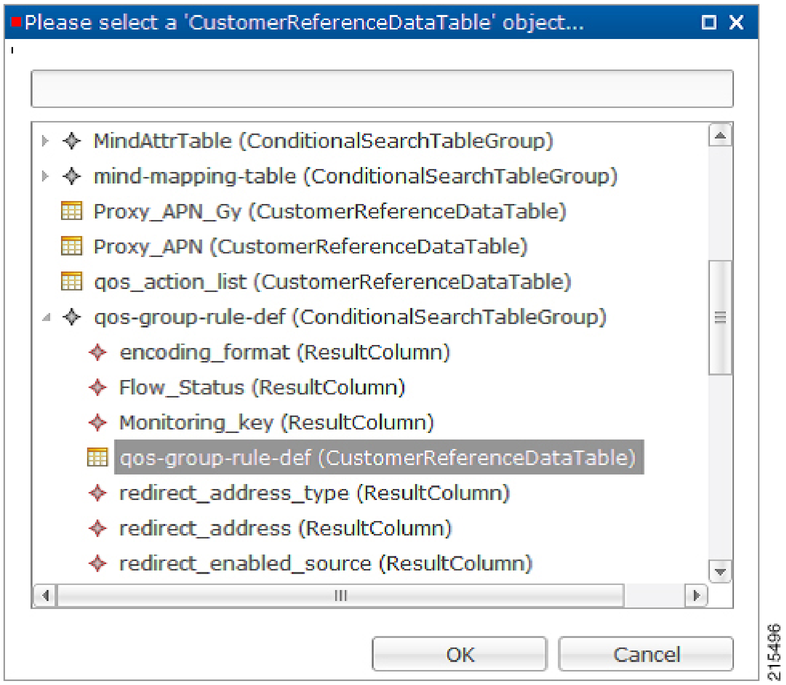
Parameter	Description
Input List (List)	
Crd Column	The Crd column is bound to the appropriate key column within the STG for those AVPs which are inputs to this table.
Referenced Output Column	Reserved for future use.
Column Value	The value of the AVP that is bound to the Crd Column and has a single value.
Referenced MultiValue AVP Name	The name of the attribute that is bound to the Crd Column and has multiple values.

Step 6 To bind the value, click the **Value** field, and then click **...** to select a value.

Step 7 Select the required object to bind and click **OK**.

A sample selection is shown as follows:

Figure 115: Binding a Value


Please select a 'CustomerReferenceDataTable' object...
MindAttrTable (ConditionalSearchTableGroup)
mind-mapping-table (ConditionalSearchTableGroup)
Proxy_APN_Gy (CustomerReferenceDataTable)
Proxy_APN (CustomerReferenceDataTable)
qos_action_list (CustomerReferenceDataTable)
qos-group-rule-def (ConditionalSearchTableGroup)
encoding_format (ResultColumn)
Flow_Status (ResultColumn)
Monitoring_key (ResultColumn)
qos-group-rule-def (CustomerReferenceDataTable)
redirect_address_type (ResultColumn)
redirect_address (ResultColumn)
redirect_enabled_source (ResultColumn)
OK
Cancel
215496

See Common Steps, on page 285 to continue with the configuration.

Table Driven Predefined Charging Rule

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then select **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for Table Driven Predefined Charging Rule.

a) Enter the name for use case template. For example, name the new template as **TableDrivenPredefinedChargingRule**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.

   Select Service Configuration dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select **TableDrivenPredefinedChargingRule**.

e) Save the use case template.

Step 4 Select **Services** > **Summary**.

Step 5 Click the **Service Option** link from the right side under **Actions** to create a service option using the *TableDrivenPredefinedChargingRule* use case template.

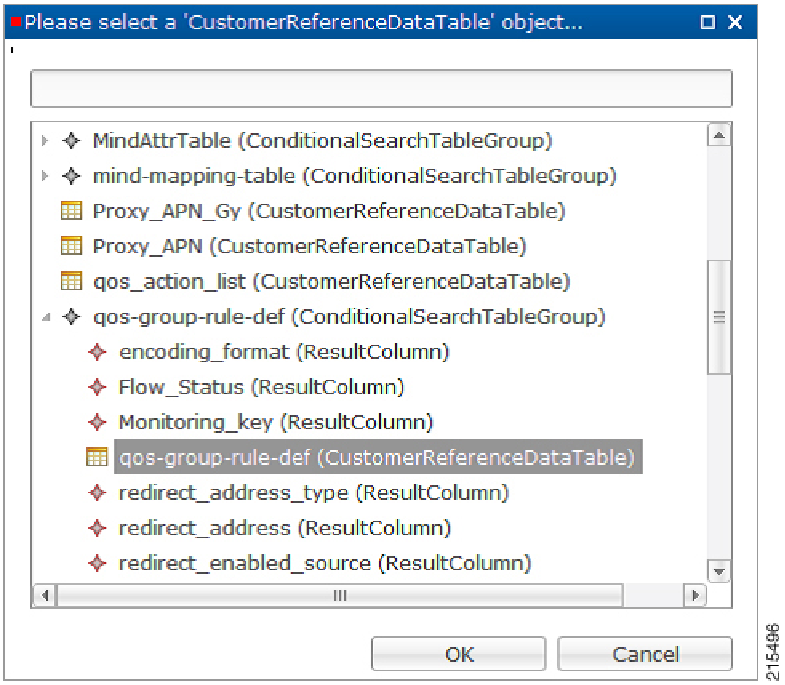
For description/usage of common parameters, see Overview, on page 278 and Common Parameter Descriptions, on page 508.

Step 6 To bind the value, click the **Value** field and enter a value or click **...** to select a value.

Step 7 Select the required object to bind and click **OK**.

A sample selection is shown as follows:

Figure 116: Binding a Value


Please select a 'CustomerReferenceDataTable' object...
MindAttrTable (ConditionalSearchTableGroup)
mind-mapping-table (ConditionalSearchTableGroup)
Proxy_APN_Gy (CustomerReferenceDataTable)
Proxy_APN (CustomerReferenceDataTable)
qos_action_list (CustomerReferenceDataTable)
qos-group-rule-def (ConditionalSearchTableGroup)
encoding_format (ResultColumn)
Flow_Status (ResultColumn)
Monitoring_key (ResultColumn)
qos-group-rule-def (CustomerReferenceDataTable)
redirect_address_type (ResultColumn)
redirect_address (ResultColumn)
redirect_enabled_source (ResultColumn)
OK
Cancel
215496

See Common Steps, on page 285 to continue with the configuration.

Common Steps

Step 1 Since this approach leverages Custom Reference and Search Table Group capabilities of CPS, we need to configure a Search Table Group to be able to use the above Service Configuration to configure a Search-Group-Table with the output column specified.

- The “Rule_Group” in the STG is the key column indicating that searches need to be based on it.
- The “Search Group” and “Search Column” are expected to be configured or bound to the “Rule_Group” column of the STG.

Step 2 It is possible to retrieve the redirect Address related elements of CISCO Service Group QoS from another table.

Note In other cases if Redirect URL STG is not required, and if redirect URL is being derived from other components of CPS, the use of override address is essential. The override server address can be derived from retrievers when the redirect address is not populated from CRD.

Control Center Configuration

Step 1 Log into Control Center.

Step 2 Select the **Configuration** tab, and then select **Configuration** > **Reference Data**.

Step 3 Select the STG created in Policy Builder and add data by creating new rows.

CRD Supported Features

Table Driven Rule Name Support

This feature allows CPS to filter the table generated rules (TableDrivenCiscoQosGroupRule, TableDrivenChargingRule, and TableDrivenPredefinedChargingRule) based on what the PCEF supports (via another rule list from CRD). Only rules common to both tables are included in actual policy.

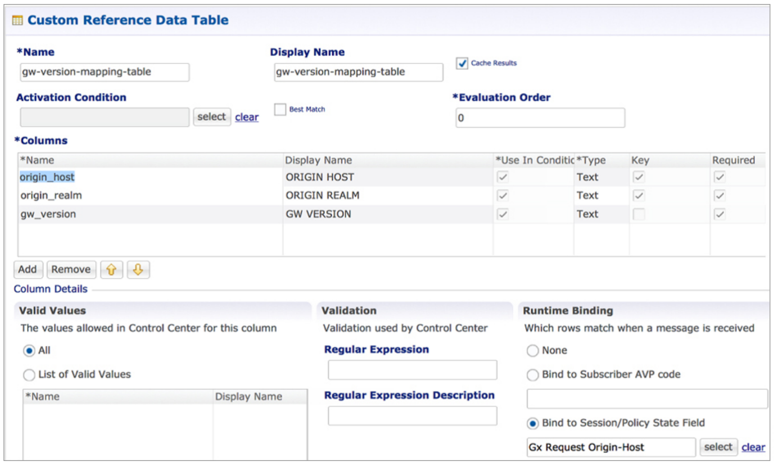
Step 1 Create a new STG/CRD called 'gw-version-mapping-table'.

- Based on the incoming Gx origin Host and Gx Origin Realm, determine the GW Version.
- Make this table as 'Best Match': Enable the check box for best match utility.

Table 130: gw-version-mapping-table Parameters

Origin Host (Input)	Original Realm (Input)	GW Version (Output)
gx_origin_host	gx_origin_realm	gw_version
Bind to 'Gx Request Origin-Host'	Bind to 'Gx Request Origin-Realm'	NA

Figure 117: Origin Host



Custom Reference Data Table

*Name: gw-version-mapping-table

Display Name: gw-version-mapping-table

☑ Cache Results

Activation Condition: select clear

□ Best Match

*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
origin_host	ORIGIN HOST	✓	Text	✓	✓
origin_realm	ORIGIN REALM	✓	Text	✓	✓
gw_version	GW VERSION	✓	Text	□	✓

Add Remove

Column Details

Valid Values

The values allowed in Control Center for this column

● All

○ List of Valid Values

*Name	Display Name

Validation

Validation used by Control Center

Regular Expression

Regular Expression Description

Runtime Binding

Which rows match when a message is received

○ None

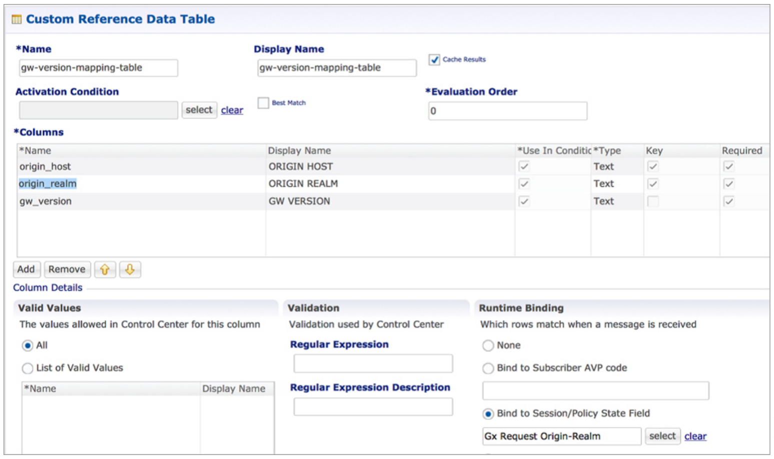
○ Bind to Subscriber AVP code

● Bind to Session/Policy State Field

Gx Request Origin-Host select clear

215497

Figure 118: Origin Realm



Custom Reference Data Table

*Name: gw-version-mapping-table

Display Name: gw-version-mapping-table

☑ Cache Results

Activation Condition: select clear

□ Best Match

*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
origin_host	ORIGIN HOST	✓	Text	✓	✓
origin_realm	ORIGIN REALM	✓	Text	✓	✓
gw_version	GW VERSION	✓	Text	□	✓

Add Remove

Column Details

Valid Values

The values allowed in Control Center for this column

● All

○ List of Valid Values

*Name	Display Name

Validation

Validation used by Control Center

Regular Expression

Regular Expression Description

Runtime Binding

Which rows match when a message is received

○ None

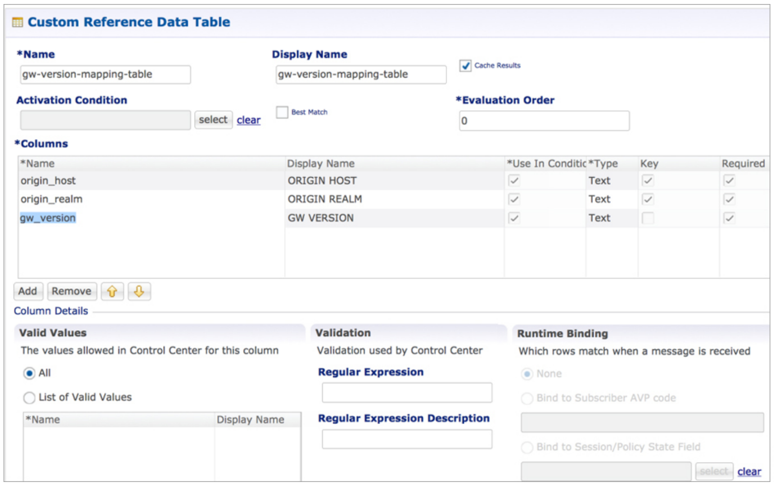
○ Bind to Subscriber AVP code

● Bind to Session/Policy State Field

Gx Request Origin-Realm select clear

215498

Figure 119: GW Version



Custom Reference Data Table

*Name: gw-version-mapping-table

Display Name: gw-version-mapping-table

☑ Cache Results

Activation Condition: select clear

□ Best Match

*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
origin_host	ORIGIN HOST	✓	Text	✓	✓
origin_realm	ORIGIN REALM	✓	Text	✓	✓
gw_version	GW VERSION	✓	Text	□	✓

Add Remove

Column Details

Valid Values

The values allowed in Control Center for this column

● All

○ List of Valid Values

*Name	Display Name

Validation

Validation used by Control Center

Regular Expression

Regular Expression Description

Runtime Binding

Which rows match when a message is received

● None

○ Bind to Subscriber AVP code

○ Bind to Session/Policy State Field

select clear

215499

Step 2 Create another STG/CRD called 'gw-rule-mapping-table'.

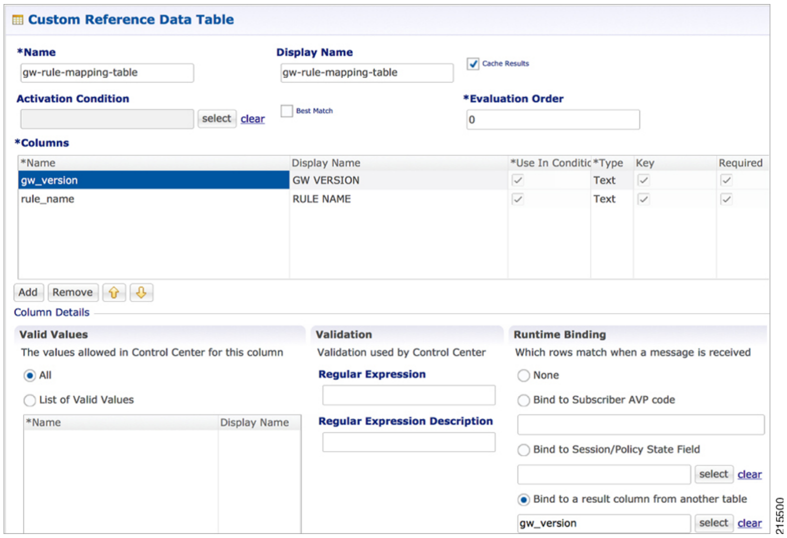
- Link the input column 'gw_version' in this table to the output from the earlier table.
- Both columns are input columns in this case.

Table 131: gw-rule-mapping-table Parameters

GW Version (Input)	Rule Name (Input)
Gw_version	Rule_name
Bind to result column from 'gw_version_mapping-table'	NA

Note For same GW version, we can define multiple rules, so we need to have each rule name as an input column.

Figure 120: GW Version



Custom Reference Data Table

*Name: gw-rule-mapping-table
Display Name: gw-rule-mapping-table
☑ Cache Results
Activation Condition: select clear
□ Best Match
*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
gw_version	GW VERSION	✓	Text	✓	✓
rule_name	RULE NAME	✓	Text	✓	✓

Add Remove

Column Details

Valid Values
The values allowed in Control Center for this column
● All
○ List of Valid Values

*Name	Display Name

Validation
Validation used by Control Center
Regular Expression
Regular Expression Description

Runtime Binding
Which rows match when a message is received
○ None
○ Bind to Subscriber AVP code
○ Bind to Session/Policy State Field
select clear
● Bind to a result column from another table
gw_version select clear

Step 3 In the existing 'QoS-Group-Rules' template (where we already have the Table Driven objects) add the new object 'TableDrivenRuleNameSupport'.

Step 4 In the same Service Configuration Object 'QoS-Group-Rules', then click add. The new service configuration object (added in the template) is available here.

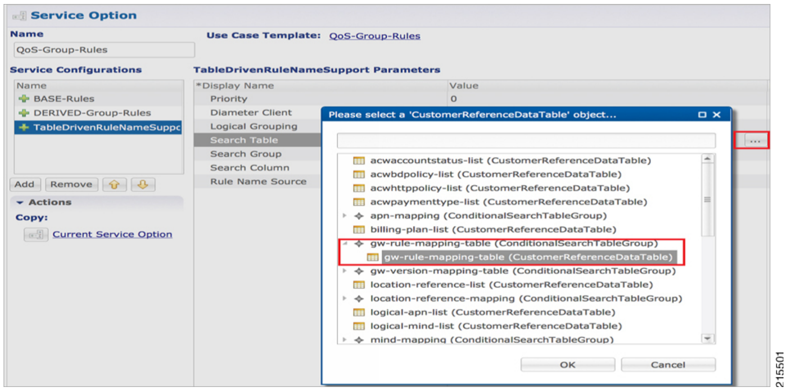
Update the following fields in the new service configuration object:

- Search Table: Click the icon in the **Value** section and select **gw-rule-mapping-table** from the drop-down list.
- Search Group: Click the icon in the **Pull Value from** section and select the Group level output **gw_version** from **gw-version-mapping-table**.
- Search Column: Click the icon the **Value** section and select **gw_version** input column from **gw-rule-mapping-table**.
- Rule Name Source: Click the icon the **Value** section and select **rule_name** input column from the same **gw-rule-mapping-table** as above.

With this configuration, CPS would do a UNION operation with the QoS groups obtained from the new 'TableDrivenRuleNames' Object (based on the GW version) and the ones retrieved from 'TableDrivenCiscoQoSGroupRules' (based on Rule-Mapping table & Rule-Group-Mapping table).

Mapping for Search Table of TableDrivenRuleNameSupport:

Figure 121: Search Table Mapping



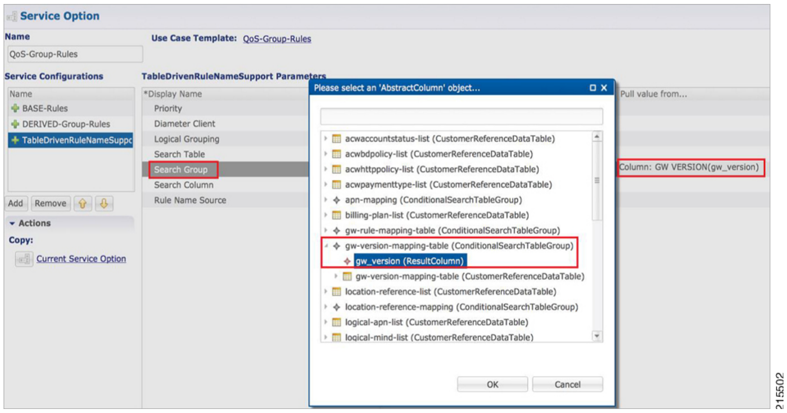
Name: QoS-Group-Rules
Use Case Template: QoS-Group-Rules
Priority: 0

Please select a 'CustomerReferenceDataTable' object...

- acwaccountstatus-list (CustomerReferenceDataTable)
- acwbdpolicy-list (CustomerReferenceDataTable)
- acwhttppolicy-list (CustomerReferenceDataTable)
- acwpaymenttype-list (CustomerReferenceDataTable)
- apn-mapping (ConditionalSearchTableGroup)
- billing-plan-list (CustomerReferenceDataTable)
- gw-rule-mapping-table (ConditionalSearchTableGroup)
  - gw-rule-mapping-table (CustomerReferenceDataTable)
- gw-version-mapping-table (ConditionalSearchTableGroup)
- location-reference-list (CustomerReferenceDataTable)
- location-reference-mapping (ConditionalSearchTableGroup)
- logical-apn-list (CustomerReferenceDataTable)
- logical-mind-list (CustomerReferenceDataTable)
- mind-mapping (ConditionalSearchTableGroup)

Mapping for Search Group of TableDrivenRuleNameSupport:

Figure 122: Search Group Mapping



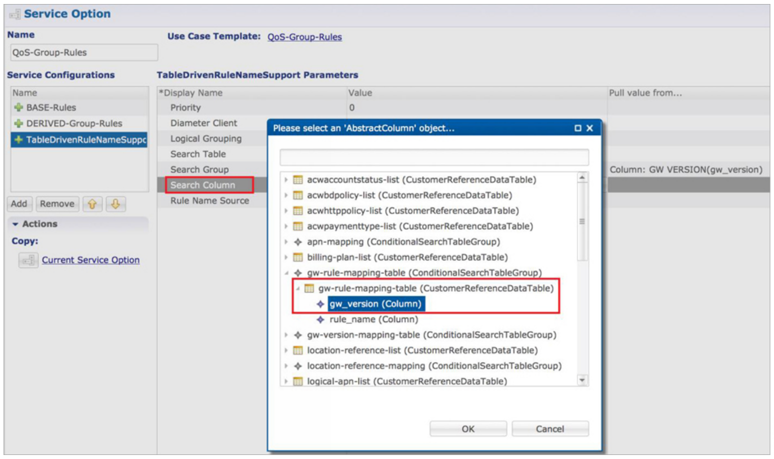
Name: QoS-Group-Rules
Use Case Template: QoS-Group-Rules
Search Group: Column: GW VERSION(gw_version)

Please select an 'AbstractColumn' object...

- acwaccountstatus-list (CustomerReferenceDataTable)
- acwbdpolicy-list (CustomerReferenceDataTable)
- acwhttppolicy-list (CustomerReferenceDataTable)
- acwpaymenttype-list (CustomerReferenceDataTable)
- apn-mapping (ConditionalSearchTableGroup)
- billing-plan-list (CustomerReferenceDataTable)
- gw-rule-mapping-table (ConditionalSearchTableGroup)
- gw-version-mapping-table (ConditionalSearchTableGroup)
  - gw_version (ResultColumn)
  - gw-version-mapping-table (CustomerReferenceDataTable)
- location-reference-list (CustomerReferenceDataTable)
- location-reference-mapping (ConditionalSearchTableGroup)
- logical-apn-list (CustomerReferenceDataTable)
- logical-mind-list (CustomerReferenceDataTable)

Mapping for Search Column of TableDrivenRuleNameSupport:

Figure 123: Search Column Mapping



Service Option

Name: QoS-Group-Rules

Use Case Template: QoS-Group-Rules

Service Configurations

Name
BASE-Rules
DERIVED-Group-Rules
TableDrivenRuleNameSuppc

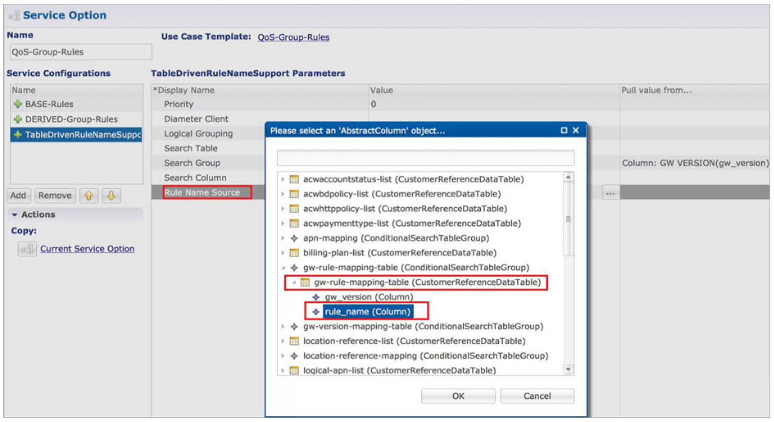
TableDrivenRuleNameSupport Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Logical Grouping		
Search Table		
Search Group		Column: GW VERSION(gw_version)
Search Column		
Rule Name Source		

Please select an 'AbstractColumn' object...

- acwaccountstatus-list (CustomerReferenceDataTable)
- acwbdpolicy-list (CustomerReferenceDataTable)
- acwhttppolicy-list (CustomerReferenceDataTable)
- acwpaymenttype-list (CustomerReferenceDataTable)
- apn-mapping (ConditionalSearchTableGroup)
- billing-plan-list (CustomerReferenceDataTable)
- gw-rule-mapping-table (ConditionalSearchTableGroup)
  - gw-rule-mapping-table (CustomerReferenceDataTable)
    - gw_version (Column)
    - rule_name (Column)
- gw-version-mapping-table (ConditionalSearchTableGroup)
- location-reference-list (CustomerReferenceDataTable)
- location-reference-mapping (ConditionalSearchTableGroup)
- logical-apn-list (CustomerReferenceDataTable)

Figure 124: Rule Name Source



Service Option

Name: QoS-Group-Rules

Use Case Template: QoS-Group-Rules

Service Configurations

Name
BASE-Rules
DERIVED-Group-Rules
TableDrivenRuleNameSuppc

TableDrivenRuleNameSupport Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Logical Grouping		
Search Table		
Search Group		Column: GW VERSION(gw_version)
Search Column		
Rule Name Source		

Please select an 'AbstractColumn' object...

- acwaccountstatus-list (CustomerReferenceDataTable)
- acwbdpolicy-list (CustomerReferenceDataTable)
- acwhttppolicy-list (CustomerReferenceDataTable)
- acwpaymenttype-list (CustomerReferenceDataTable)
- apn-mapping (ConditionalSearchTableGroup)
- billing-plan-list (CustomerReferenceDataTable)
- gw-rule-mapping-table (ConditionalSearchTableGroup)
  - gw-rule-mapping-table (CustomerReferenceDataTable)
    - gw_version (Column)
    - rule_name (Column)
- gw-version-mapping-table (ConditionalSearchTableGroup)
- location-reference-list (CustomerReferenceDataTable)
- location-reference-mapping (ConditionalSearchTableGroup)
- logical-apn-list (CustomerReferenceDataTable)

Best Match Table Logic

CPS supports each table look-up in CRD, which needs to be one of the match types shown in the following list, along with Best Match table. This approach is fast, efficient, and very easy to troubleshoot, and scales when there are dozens, scores, or hundreds of combinations of values.

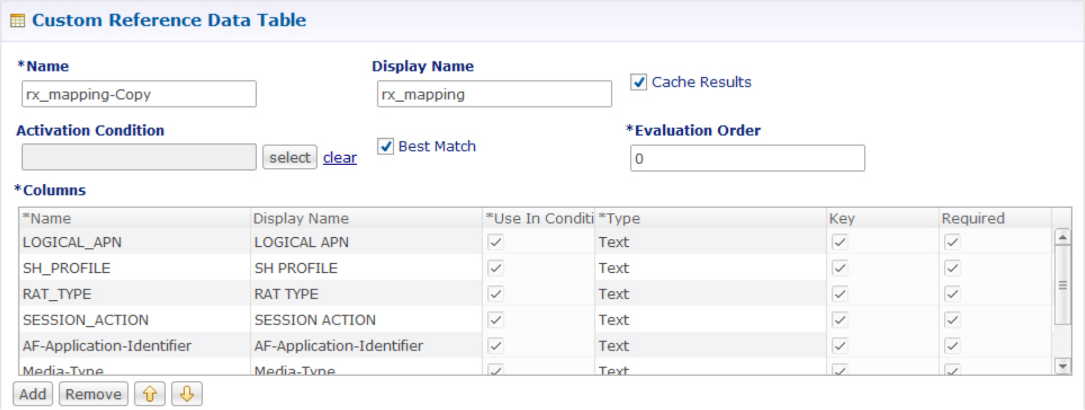
When the **Best Match** option is selected in the Custom Reference Data Table configuration, look-ups occur within a CRD table in the following order:

- Exact string match
- Higher priority regex match (if multiple regex patterns match)
- Regular expression match (default behavior)
- Wild card character (*)

The following figures contain examples of a CRD table configuration and its corresponding output table in Control Center.

- STG Table as Input for Best Match:

Figure 125: Best Match Option



Custom Reference Data Table

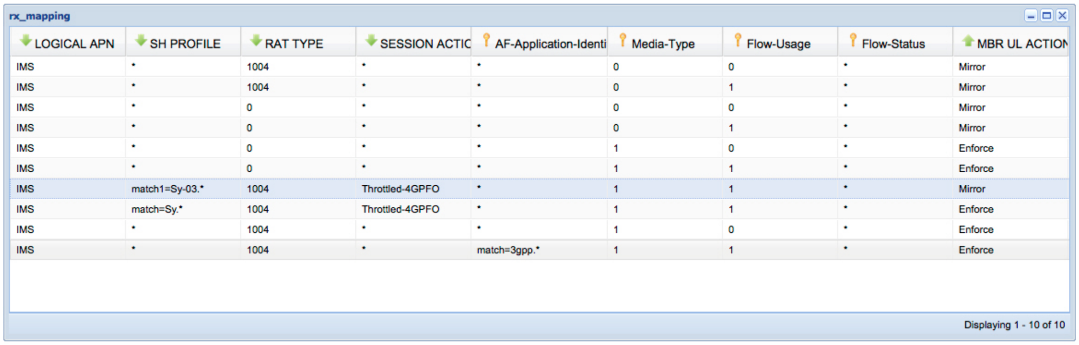
*Name: rx_mapping-Copy
Display Name: rx_mapping
☑ Cache Results
Activation Condition: select clear
☑ Best Match
*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditi	*Type	Key	Required
LOGICAL_APN	LOGICAL APN	✓	Text	✓	✓
SH_PROFILE	SH PROFILE	✓	Text	✓	✓
RAT_TYPE	RAT TYPE	✓	Text	✓	✓
SESSION_ACTION	SESSION ACTION	✓	Text	✓	✓
AF-Application-Identifier	AF-Application-Identifier	✓	Text	✓	✓
Media-Type	Media-Type	✓	Text	✓	✓

- Output Table, which can take an exact string match, a higher priority regex match, a regular expression match, and a wildcard entry like *.

Figure 126: Matching Examples



rx_mapping

LOGICAL APN	SH PROFILE	RAT TYPE	SESSION ACTIC	AF-Application-Identi	Media-Type	Flow-Usage	Flow-Status	MBR UL ACTION
IMS	*	1004	*	*	0	0	*	Mirror
IMS	*	1004	*	*	0	1	*	Mirror
IMS	*	0	*	*	0	0	*	Mirror
IMS	*	0	*	*	0	1	*	Mirror
IMS	*	0	*	*	1	0	*	Enforce
IMS	*	0	*	*	1	1	*	Enforce
IMS	match1=Sy-03.*	1004	Throttled-4GPFO	*	1	1	*	Mirror
IMS	match=Sy.*	1004	Throttled-4GPFO	*	1	1	*	Enforce
IMS	*	1004	*	*	1	0	*	Enforce
IMS	*	1004	*	match=3gpp.*	1	1	*	Enforce

Displaying 1 - 10 of 10

Table (CRD) Driven Rule Refresh on Rule Failure

Overview

CPS now supports the ability to install new charging rules based on the Charging rule name and its status reported in CCR-U from PCEF in Charging Rule Report AVP for a particular rule/rules.

- The rule name and rule status (ACTIVE(0)/INACTIVE(1)/TEMPORARILY_INACTIVE(2)) are derived from the session and then used as input for the new rules to be installed for the Gx session.
- If a rule status is received as NOT ACTIVE in CCR-U and if that rule is present as an input in the refresh table on which CPS should install new refresh rules, CPS will remove the rule in CCA-U and install the corresponding newly derived refresh rules from the table in CCA-U.
- Later if one of the new or derived refresh rules installed above comes with a Charging-Rule-Report as ACTIVE/INACTIVE/TEMP_INACTIVE, CPS will install the default bearer rule back again.

TableDrivenChargingRuleRefresh Service Option

The TableDrivenChargingRuleRefresh service option provides support for this functionality. The specific parameters provided in this service option are described later in Table in section Create a Table Driven Refresh Rule, on page 292.

On receiving a Charging-Rule-Report AVP in Gx CCR-U, the TableDrivenRuleRefresh service option is evaluated to find if there are rows configured for the reported rule-name and reported rule-status in the table defined in the Search Table field. If there is an entry in the table, CPS takes the entry from the Output Rule Group Column and uses that value as an input for Search Group in the Table Driven Charging Rule.

If Output Search Table is configured for TableDrivenChargingRuleRefresh, CPS performs a lookup only on those TableDrivenChargingRule objects which has the Search Table matching the Output Search Table in TableDrivenChargingRuleRefresh.

If multiple rules are reported in a Gx-CCR U, then all the corresponding groups in the table are used as an input to TableDrivenChargingRule service option and all the rules from all the groups are evaluated.

The following table shows an example configuration:

Table 132: TableDrivenChargingRuleRefresh Example Configuration

Rule Name	Rule Status	Rule Group
Rule-A	2	Group-1
Rule-B	2	Group-2
Rule-C	0	Group-3

In this example, if CPS receives Rule-A and Rule-B in the ChargingRule Report AVP, then the corresponding groups, Group-1 and Group-2 are evaluated. This is then used to query the TableDrivenChargingRule table with Search Group as Group-1 and Group-2. So all the rules with Group as Group-1 and Group-2 would be installed in CCA-U.

Note

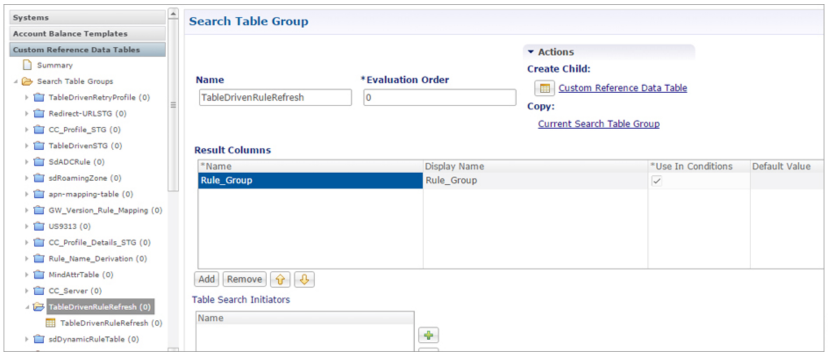
- The TableDrivenChargingRule would have the Search Table and Search Column configured as described above. The Search Group would come as an output of the query done using TableDrivenRuleRefresh service option. Even if the Search Group is blank, if there are Output Rule Groups evaluated due to TableDrivenChargingRuleRefresh, CPS queries the TableDrivenChargingRule with the Search Group value as the Output Rule Groups. (If more than one are configured, CPS queries them one by one.)
- In case there is a value in Search Group in the TableDrivenChargingRule, CPS first evaluates the TableDrivenChargingRules with the mentioned Search Group. After finishing the above query, CPS then proceeds to look up the Output Search Groups retrieved as a result of TableDrivenChargingRuleRefresh queries.
- If the refresh rule and the default bearer rule come as OUT_OF_CREDIT immediately or simultaneously, it can create a loop. To prevent a loop, refer to Prevention of a Refresh Loop, on page 294. However, this is not an ideal situation and it is agreed upon that in production we won't encounter looping. Also CPS cannot guarantee stopping of loops in such scenario as the session may connect and disconnect and may go into loop each time.
- Also, the feature does not actually look at the event trigger but only on the rule name and status reported.

Policy Builder Configuration

Create a Table Driven Rule Refresh CRD Table

Step 1 In Policy Builder, create and configure a Search Table Group (STG).

Figure 127: Search Table Group (STG)



Search Table Group

Name: TableDrivenRuleRefresh

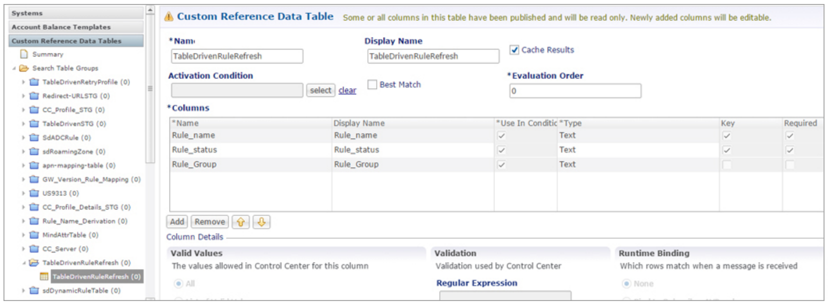
*Evaluation Order: 0

Result Columns

*Name	Display Name	*Use In Conditions	Default Value
Rule_Group	Rule_Group	✓	

Step 2 Create and configure a **Custom Reference Data Table** under this STG.

Figure 128: Custom Reference Data Table



Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

*Nam: TableDrivenRuleRefresh

Display Name: TableDrivenRuleRefresh

☑ Cache Results

Activation Condition:

□ Best Match

*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditic	*Type	Key	Required
Rule_name	Rule_name	✓	Text	✓	✓
Rule_status	Rule_status	✓	Text	✓	✓
Rule_Group	Rule_Group	✓	Text	□	□

The Rule_Group output column shown above is used as an input to evaluate TableDrivenChargingRule service option.

Create a Table Driven Refresh Rule

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *TableDrivenChargingRuleRefresh*.

Step 4 Select **Services** > **Summary**. Click **Service Option** link from the right side under **Actions** to create a service option using Use Case Template created above.

Step 5 In the Search Table row, select the ‘TableDrivenRuleRefresh’ CRD table created in the previous section to bind it to this service option.

To bind the value, select the name from the Display Name column and in Value column click **....** to open **Please select a 'CustomerReferenceDataTable' object**.

Note For usage of common parameters, see Common Parameter Descriptions, on page 508. Other parameters can be configured as follows:

Table 133: TableDrivenChargingRuleRefresh Parameters

Parameter	Description
Search Table	The search table to lookup from.
Input Rule Name Column	The input column for the SearchTableGroup (STG), which contains the rule name.
Output Rule Status Column	The input column for the STG, which contains the rule status against which new rules are to be added.
Output Rule Group Column	The output column for the STG, which contains the rule group, which would be used as a group to search the TableDrivenChargingRule.
Output Search Table	In case there are multiple TableDrivenChargingRules mapped with multiple Search Tables, and if we want to use only one table to be looked upon for new rules installation on rule failure, we can give the table as Output Search Table so that only one TableDrivenChargingRule object, which has the 'Search Table' matching the 'Output Search Table' in TableDrivenChargingRuleRefresh, is evaluated for refresh rules and not all the objects.

The Output Search Table in TableDrivenChargingRuleRefresh should match with the Search Table in the TableDrivenChargingRule for looking up the output groups in the table for deriving the table driven charging rules.

The Search Group in TableDrivenChargingRules is not bound to anything. The output Rule_Group from the Refresh Table is automatically taken as input to the TableDrivenChargingRules service option.

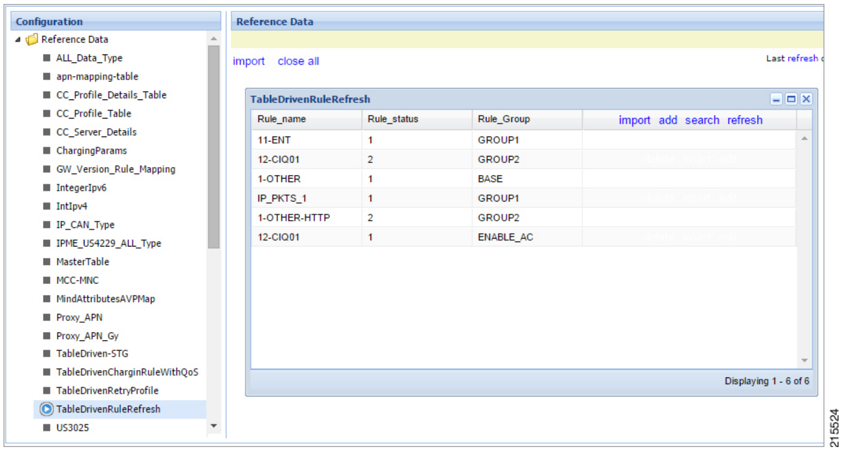
Control Center Configuration

Step 1 Log into Control Center.

Step 2 Select **Configuration** > **Configuration** > **Reference Data**.

Step 3 Select the STG created in Policy Builder and add data by creating new rows.

Figure 129: Configuring Reference Data



Rule_name	Rule_status	Rule_Group
11-ENT	1	GROUP1
12-CIQ01	2	GROUP2
1-OTHER	1	BASE
IP_PKTS_1	1	GROUP1
1-OTHER-HTTP	2	GROUP2
12-CIQ01	1	ENABLE_AC

Prevention of a Refresh Loop

To prevent a scenario where successive INACTIVE statuses would cause CPS to repeatedly attempt to install the same 2 rules, CPS tracks the number of times a refresh rule is installed within a specific time period. If a loop is detected, CPS will skip the rule installation.

The settings which control the loop detection can be customized. Contact your Cisco representative for more information.

Custom Features

Service Group QoS

Overview

The goal of Service Group QoS is to provide support within PCRF in ASR5K to define and enforce Fair-Usage-Policy (FUP) per subscriber. CPS provides support for CISCO Service Group QoS in ASR5K based deployment of PCEF. Service Group QoS is sent over the Gx interface when CPS (PCRF) tries to install or remove rules for a subscription based on various triggers. These attributes are CISCO deployment specific and are enabled only for the “Gx clients” which support Service Group QoS Rules.

Policy Builder Configuration

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *CiscoQoSGroupRule*.

a) Enter the name for use case template. For example, name the new template as **CiscoQoSGroupRule**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.

Select Service Configuration dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select **CiscoQoSGroupRule**.

User can configure various QoS Group Rule parameters depending on the network requirements. For configuration/usage of different parameters, refer to Common Steps, on page 285

Step 4 Select **CiscoQoSGroupRule** and click required service configuration parameters that need to be configured. Click **OK** to add the service in **Service Configuration** pane.

Step 5 In **Services** tab, click **Services** > **Service Options** to create a service option and add the configured Use Case Template in CiscoQoSGroupRule to configure Service Option.

Step 6 In **Services** tab, click **Services** > **Services** to create a service and add the configured Use Case Template in CiscoQoSGroupRule to configure Service.

Content Filtering

Overview

The goal of Content Filtering is to provide support for content filtering within the network by use of Policy ID's. Policy identifiers (Policy IDs) are rules that are configured on the ASR 5000 platform and invoked by the CPS. Policy IDs are used to implement the required Content Filtering policies defined for the subscriber. The Policy IDs are selected at the ASR 5000 by provisioning their values through the Gx interface by the PCRF.

When a user initiates a session, the ASR5K communicates with the CPS to initialize the defined policies. CPS provides the Policy ID to the ASR5K to provide the necessary Content Filtering services for the user.

The main aim of this feature is for CPS to provide Policy ID's configured in the subscriber's service to the PCEF (ASR5K).

Policy Builder Configuration

There are three sequential procedures to configure the Policy IDs using the CPS.

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

Step 4 Provide a name for the template in the **Name** field.

Step 5 Select **Actions** tab.

Step 6 To define the basic template, under Service Configurations, click **Add**. Select the required configurations from the popup window and click **OK**.

Note
- Cisco Content Filtering Policy option must be selected along with other configurations to provide Content Filtering services.
- The check boxes in the Allow Override column are checked by default. This allows the subscriber to change the values in the Service Option. Otherwise, the value remains constant.

Step 7 Click the save icon.

Step 8 In the left column, select **Services**.

Step 9 Locate the template that was defined in the above procedure and click **Service Option** in the summary window. The configurations that had been selected appears in the window.

Step 10 Click **OK**. Define the required parameters.

Step 11 Select the configuration to define the parameters from the list of Service Configurations.

Step 12 In the Parameters columns, set the required values.

Step 13 Click **CiscoContentFilteringPolicy** and set the Policy ID value in the parameters field.

Note Value for Policy ID should not be set to zero (0). Policy IDs can be dynamically assigned to the subscriber by referring to the Custom Reference Data Tables.

Step 14 Click **Pull value from** in the parameters column to assign Policy IDs dynamically from a predefined Custom Reference Data Table.

Emergency Data Services

Overview

CPS supports Emergency Data Services as per the procedures defined in 3GPP TS 29.212. The operator has to configure a list of Emergency Access Point Names (APNs) that are valid for the operator. These APNs are then used by CPS to identify a session as an Emergency session. CPS also supports installation of QoS and Rules for emergency sessions.

Configure Diameter Gx Client for Emergency APNs

The emergency APNs have to be configured in the Diameter Gx Client configuration. So, first you need to configure a Diameter Gx Client.

For more details on how to configure the Diameter Gx Client, refer Diameter Clients, on page 119.

Step 1 Log into Policy Builder.

Step 2 Select the **Reference Data** tab.

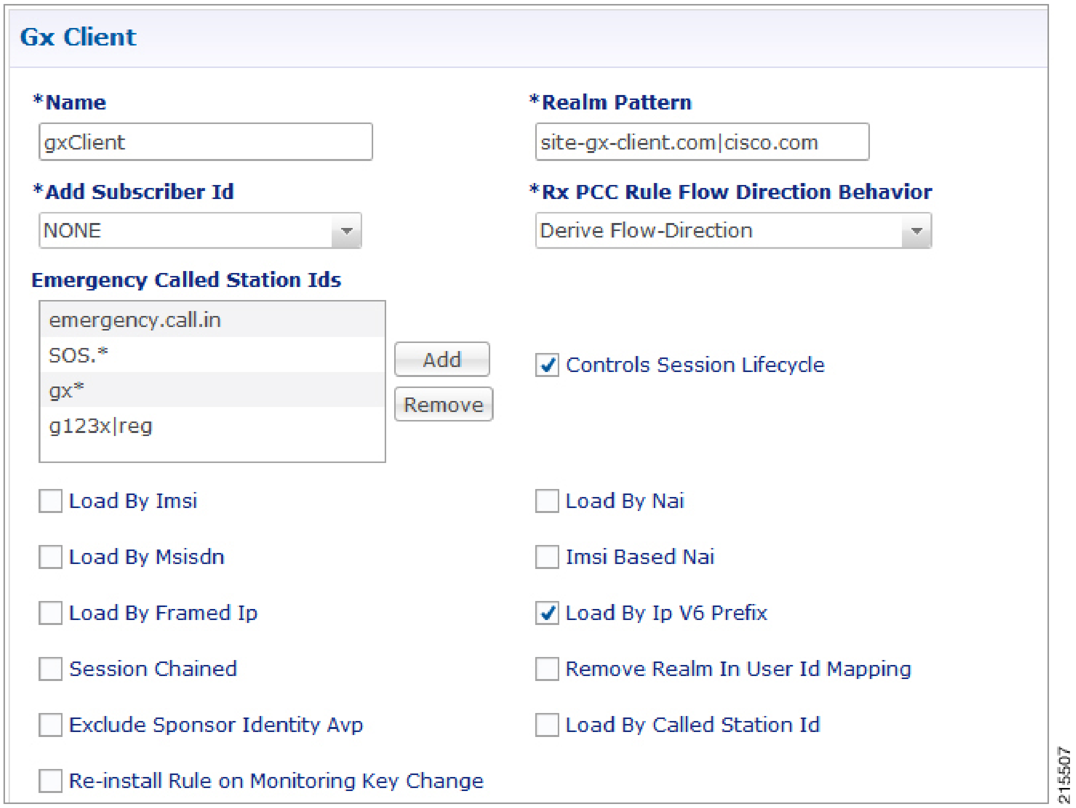
Step 3 From the left pane, select **Diameter Clients**.

Step 4 Expand the Gx Clients by clicking on the arrow right next to “Gx Clients”. If you do not see this arrow, this means the Gx Client has not been created.

Refer Diameter Clients, on page 121 to create a Gx Client.

Step 5 Select the Gx Client name created by you. Gx Client attributes as shown below will come up in the right pane.

Figure 130: Gx Client Attributes



Gx Client

*Name: gxClient

*Realm Pattern: site-gx-client.com|cisco.com

*Add Subscriber Id: NONE

*Rx PCC Rule Flow Direction Behavior: Derive Flow-Direction

Emergency Called Station Ids:

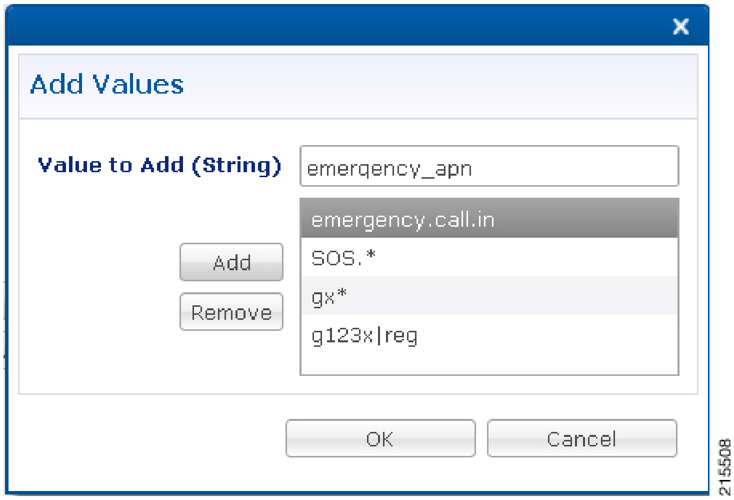
- emergency.call.in
- SOS.*
- gx*
- g123x|reg

☑ Controls Session Lifecycle

□ Load By Imsi	□ Load By Nai
□ Load By Msisdn	□ Imsi Based Nai
□ Load By Framed Ip	☑ Load By Ip V6 Prefix
□ Session Chained	□ Remove Realm In User Id Mapping
□ Exclude Sponsor Identity Avp	□ Load By Called Station Id
□ Re-install Rule on Monitoring Key Change	

Step 6 Click **Add** to configure the emergency APNs. The following window is displayed.

Figure 131: Emergency APN Configuration



Add Values

Value to Add (String): emergency_apn

- emergency.call.in
- SOS.*
- gx*
- g123x|reg

Step 7 Type the name of the emergency APN that you want to add in the **Value to Add (String)** text box and click **Add**.

Step 8 Click **OK**. In the example shown above, four APN entries are already added.To remove an APN from this list, select the APN to be removed and click Remove.

CPS supports wildcarding for the Emergency APN names. As shown in the example above, we have used '*' for wildcarding. CPS uses standard Java pattern characters for APN names. The pattern needs to follow the standard Java regular expression syntax described here.

Configure Service for Emergency Sessions

For emergency APNs, the IMSI may not be present. Hence, CPS allows emergency sessions without subscriber authentication.

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab.

Step 3 From the left pane, select **Domains**.

Step 4 Select the domain name that you want to use for emergency subscribers. Domain attributes open up in the right pane.

To create a new Domain, refer Overview, on page 197.

Step 5 Select the **Advanced Rules** tab.

Step 6 Click **select** near Anonymous Subscriber Service.

Step 7 In the new window displayed, select the service that you want to assign for emergency sessions and click **OK**.

Configure Prioritizing Emergency Sessions using APNs

Emergency calls are fast-tracked through the CPS platform by bypassing authorization logic. As a user, the CPS platform enables to prioritize these emergency calls by APN. CPS uses “Emergency Message Priority”, for this prioritization. These attributes are part of “Inbound Message Overload Handling” feature under “Diameter Configuration”.

For more details, refer Inbound Message Overload Handling, on page 79.

Step 1 Log into Policy Builder.

Step 2 Select the **Reference Data** tab.

Step 3 From the left pane, select **Systems** and expand your system name or cluster name.

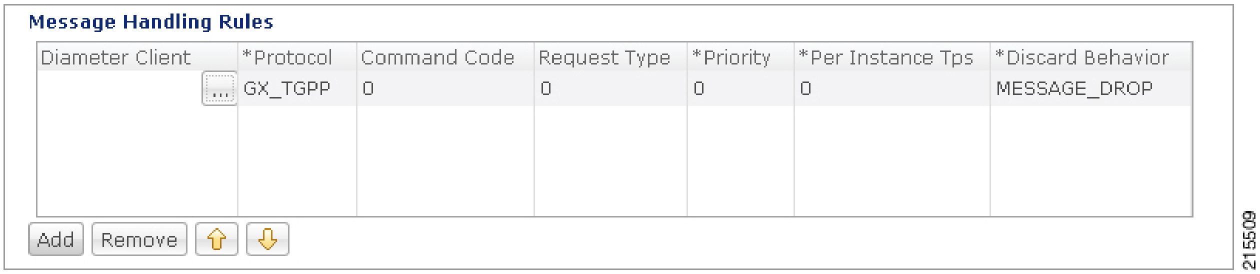
Step 4 Select and expand the **Plugin Configurations**.

Step 5 Select **Diameter Configuration**. Diameter configuration screen appears in the right pane.

Step 6 Check **Inbound Message Overload Handling** check box.

Step 7 Click **Add** under Message Handling Rules table.

Figure 132: Adding a New Row

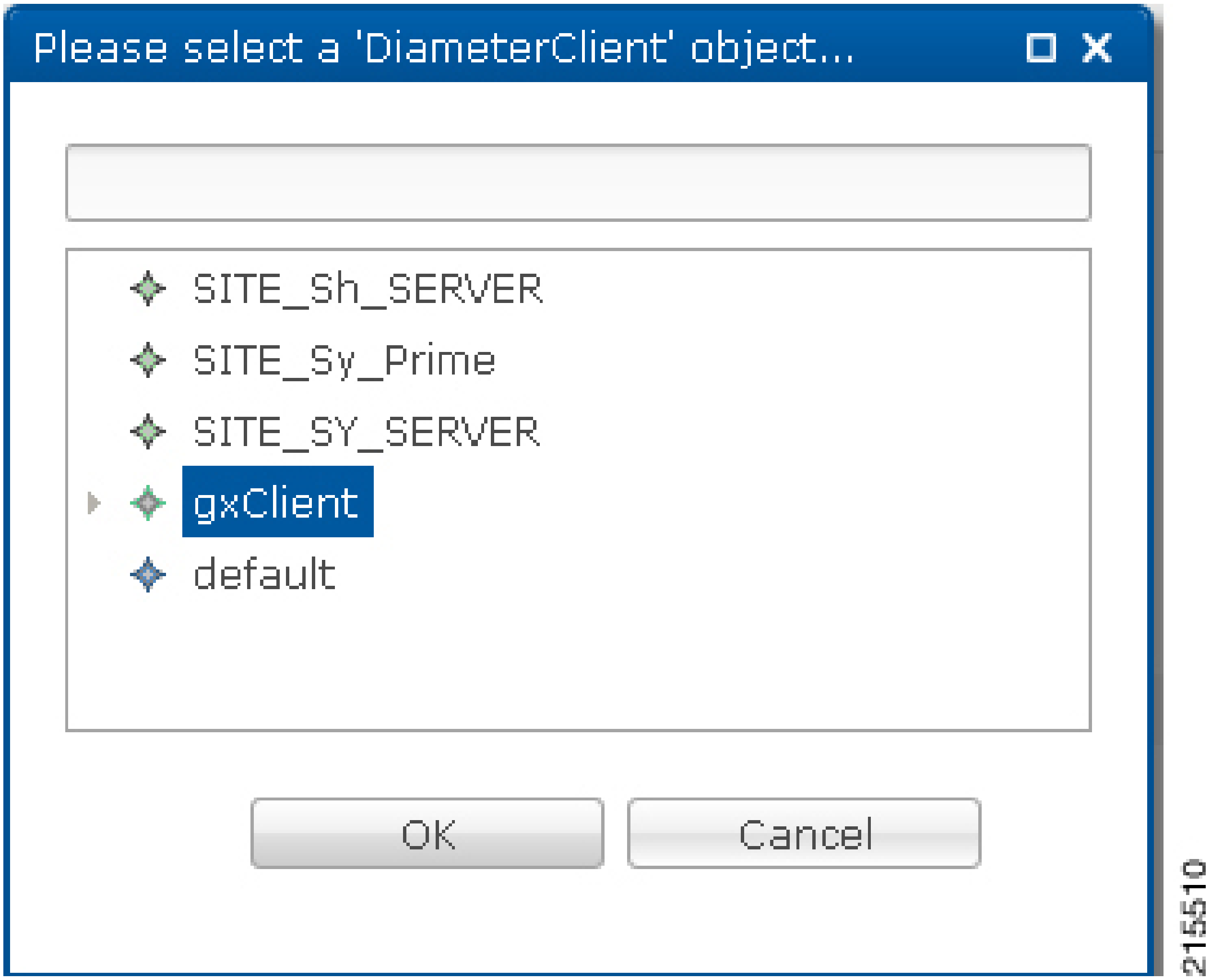


Message Handling Rules

Diameter Client	*Protocol	Command Code	Request Type	*Priority	*Per Instance Tps	*Discard Behavior
...	GX_TGPP	0	0	0	0	MESSAGE_DROP

Step 8 Click **...** in the **Diameter Client** column.

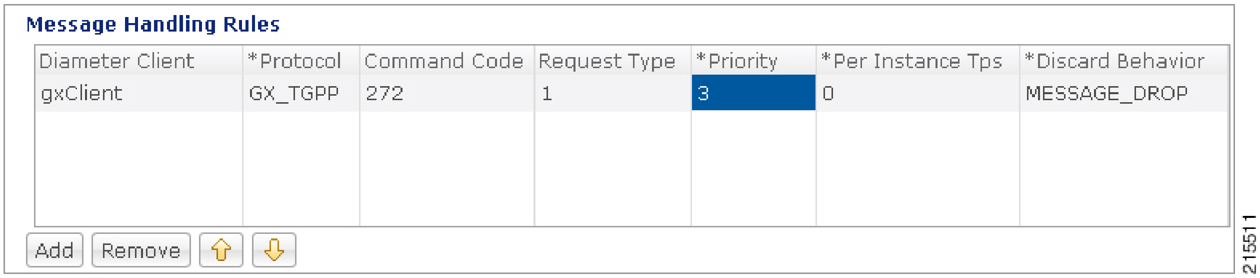
Figure 133: Selecting a DiameterClient Object



Step 9 Select the Gx Client in which we added the emergency APNs in Configure Diameter Gx Client for Emergency APNs, on page 296 and click **OK**.

Step 10 Configure the other parameters of the table.

Figure 134: Sample Configuration



Message Handling Rules

Diameter Client	*Protocol	Command Code	Request Type	*Priority	*Per Instance Tps	*Discard Behavior
gxClient	GX_TGPP	272	1	3	0	MESSAGE_DROP

Note For the detailed explanation of all the parameters of the Inbound Message Overload Handling feature, refer Inbound Message Overload Handling, on page 79. The following table explains the parameters relevant to the prioritization of emergency sessions.

Table 134: Prioritization of Emergency Session - Parameters

Parameter	Description
Default Priority	Default priority to be assigned to an incoming message, if no specific one is defined in the Message Handling Rules table. Default value is 0.
Emergency Message Priority	Default priority assigned to incoming messages related to an emergency session. Default value is 0.
Message Handling Rules	Defines specific inbound message overload handling rules based on different criteria. Message Handling Rules are generic. This means for all CCR-I messages, if you want to process with priority, user needs to set the configuration in Message Handling Rules.

Note Higher the value of the priority, the higher is the priority. User must take care that the Emergency Message Priority field value is higher than the priority column values present in the Message Handling Rules, so that the Emergency Messages are processed first than the usual messages. If we take the example values configured above, then this is how the priority is assigned to the incoming messages.

Incoming Message	Priority	Description
Any message for any emergency session/APN	5	The default emergency message priority is assigned as this is emergency APN.
A Gx CCR-I message for the non-emergency APN	3	The protocol, command code, and request type match the message handling rules.
A Gx CCR-U message for the non-emergency APN	0	Request type does not match with the value in the “Message Handling Rules”. So, the default priority is assigned.

Note By default, the emergency message priority is higher than the default priority. This means, if you do not configure the Inbound Message Overload Handling, then default priority = 0 and emergency message priority = 1.

RAN Congestion

Overview

Currently, when RAN congestion is configured, at the hour boundary there is a check for congestion level change. If the congestion level has changed then RAR is sent in which new rules corresponding to changed congestion level are applied.

The next evaluation time for session is set to the time when the congestion level changes next. At that hour boundary again the session is evaluated, and new rules applicable to changed level are applied. Since all the sessions are getting re-evaluated at applicable hour boundaries where the congestion level changes, there is a possibility of huge amount of RAR's being generated by CPS. CPS can generate this load of RARs without any issues as it is distributed among the CPS VMs. However, there might be limitation on other network elements to handle the RAR surge.

To prevent RAR burst at the hour boundary, evaluate configured services for the next hour based on the appropriate congestion levels. Also, preinstall the rules specifying Activation and Deactivation times.

Policy Builder Configuration

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *PreDefinedRuleBase*.

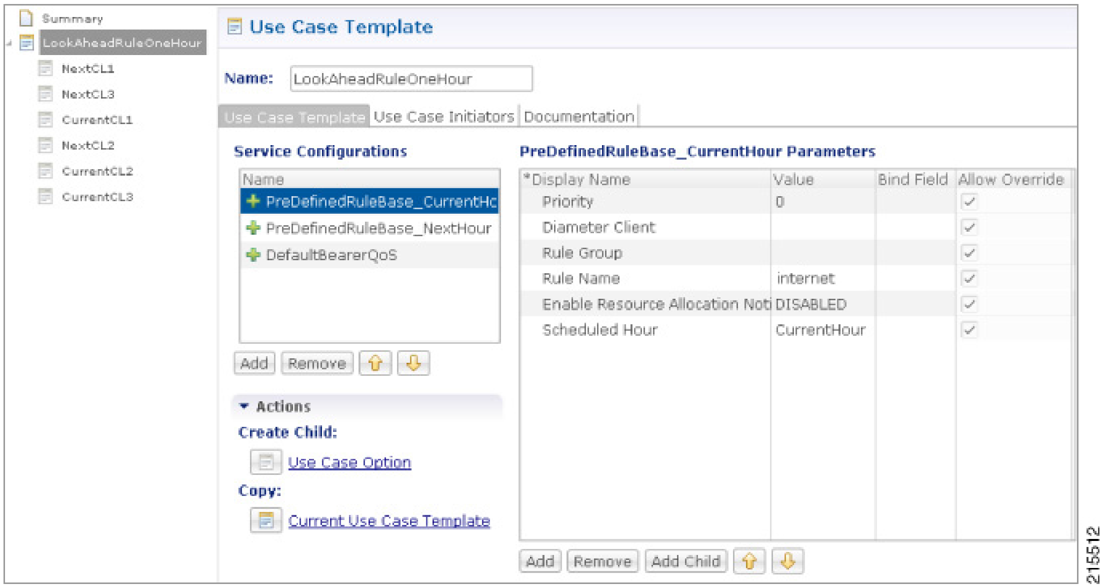
Step 4 Enter the name for use case template. For example, name the new template as **PreDefinedRuleBase**.

Step 5 Select **Actions** tab.

Step 6 Click **Add** to open **Select Service Configuration**.

Step 7 Select **PreDefinedRuleBase** and click required service configuration parameters that need to be configured. Click **OK** to add the service in Service Configuration pane.

Figure 135: Configuration for Current Hour



- Summary
- LookAheadRuleOneHour
  - NextCL1
  - NextCL3
  - CurrentCL1
  - NextCL2
  - CurrentCL2
  - CurrentCL3

Use Case Template

Name: LookAheadRuleOneHour

Use Case Template | Use Case Initiators | Documentation

Service Configurations

Name
PreDefinedRuleBase_CurrentHc
PreDefinedRuleBase_NextHour
DefaultBearerQoS

Actions

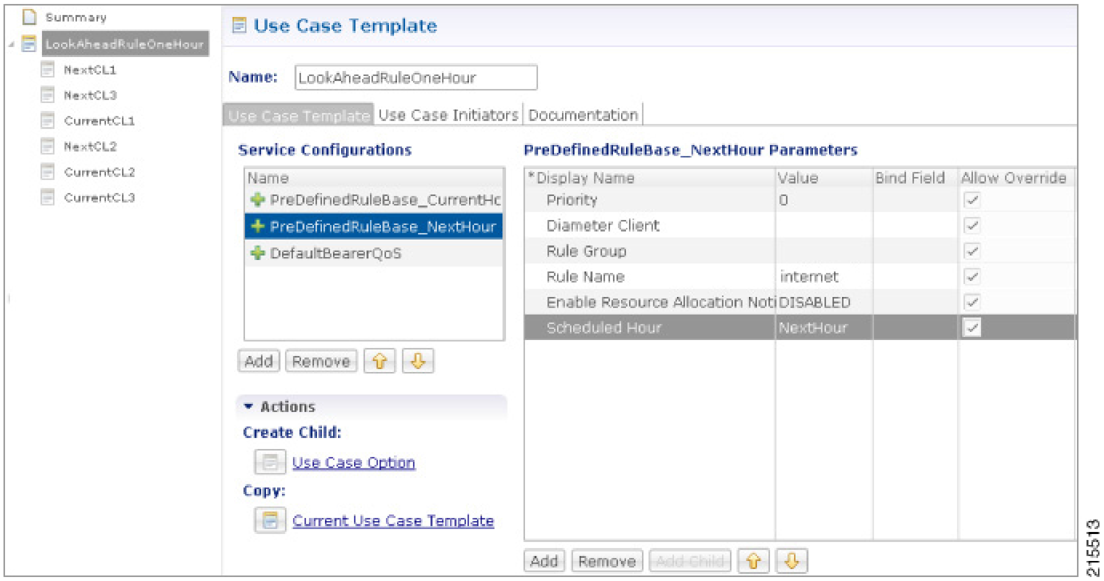
Create Child: Use Case Option

Copy: Current Use Case Template

PreDefinedRuleBase_CurrentHour Parameters

*Display Name	Value	Bind Field	Allow Override
Priority	0		✓
Diameter Client			✓
Rule Group			✓
Rule Name	internet		✓
Enable Resource Allocation Noti	DISABLED		✓
Scheduled Hour	CurrentHour		✓

Figure 136: Configuration for Next Hour



- Summary
- LookAheadRuleOneHour
  - NextCL1
  - NextCL3
  - CurrentCL1
  - NextCL2
  - CurrentCL2
  - CurrentCL3

Use Case Template

Name: LookAheadRuleOneHour

Use Case Template | Use Case Initiators | Documentation

Service Configurations

Name
PreDefinedRuleBase_CurrentHc
PreDefinedRuleBase_NextHour
DefaultBearerQoS

Actions

Create Child: Use Case Option

Copy: Current Use Case Template

PreDefinedRuleBase_NextHour Parameters

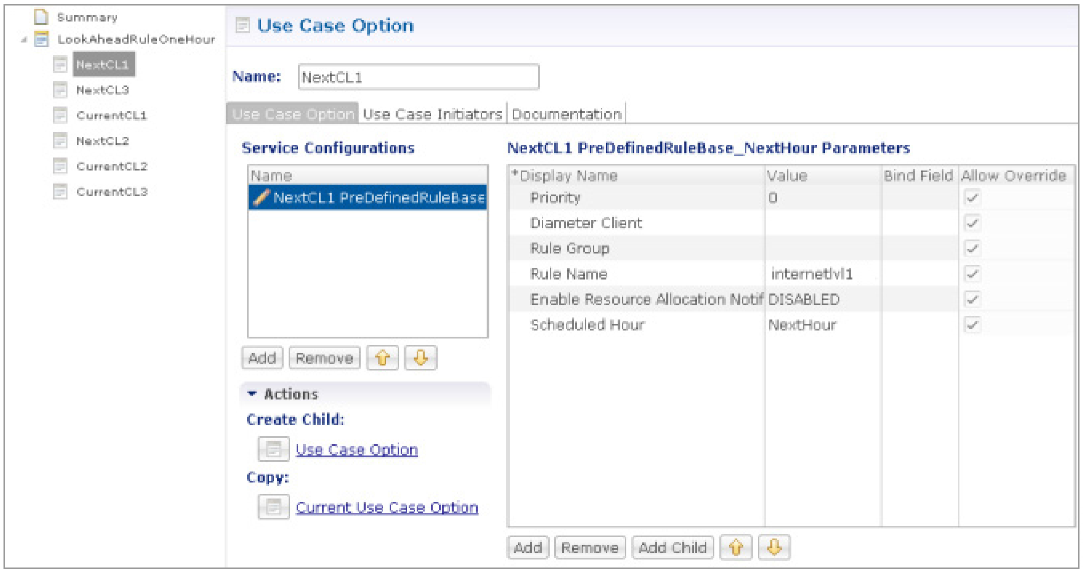
*Display Name	Value	Bind Field	Allow Override
Priority	0		✓
Diameter Client			✓
Rule Group			✓
Rule Name	internet		✓
Enable Resource Allocation Noti	DISABLED		✓
Scheduled Hour	NextHour		✓

- In order to achieve the RAN congestion use case to install rules based on congestion levels, we need to configure use case initiators to modify the rules based on congestion level.
  - Use case initiator - on condition that congestionLevel = 1, changes rulename to internetlvl1
  - Use case initiator - on condition that congestionLevel = 2, changes rulename to internetlvl2
  - Use case initiator - on condition that congestionLevel = 3, changes rulename to internetlvl3

- Assume congestionLevel is 1 for current hour and 2 for next hour. When services are evaluated for current time, this evaluates only to internetlvl1. In order to also evaluate services for the look ahead hour, we need to add corresponding modified rules for each with use case initiators as follows:
    - Use case initiator - on condition that congestionNextHourLevel = 1, changes rulename to internetlvl1
    - Use case initiator - on condition that congestionNextHourLevel = 2, changes rulename to internetlvl2
    - Use case initiator - on condition that congestionNextHourLevel = 3, changes rulename to internetlvl3

Example of configuration for one of the use case modifiers is shown below:

Figure 137: Use Case Option Tab



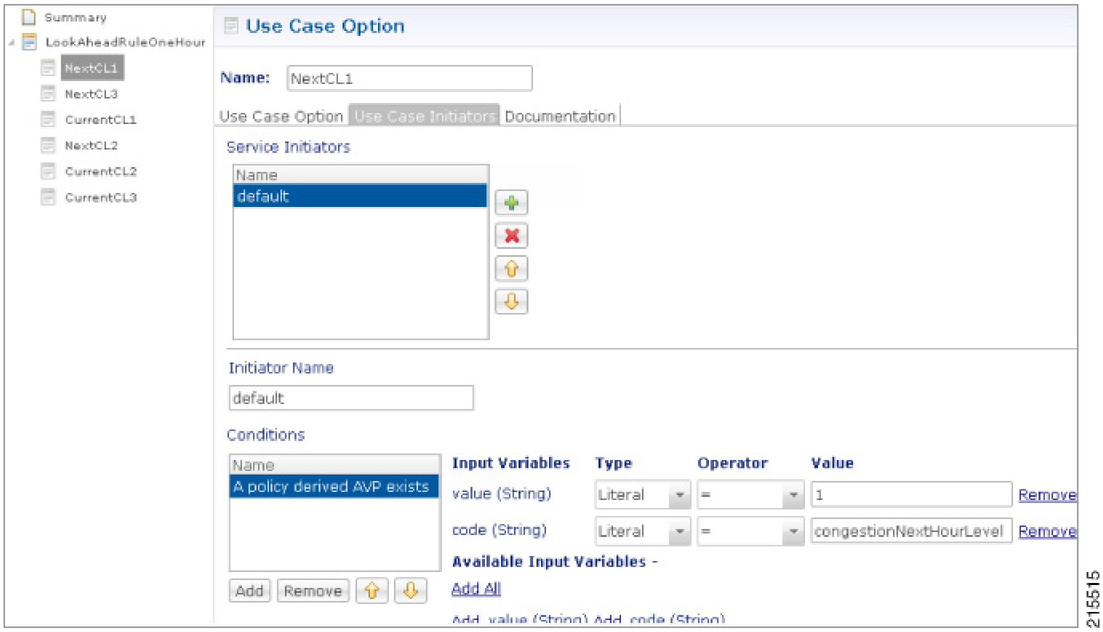
Name: NextCL1

Name
NextCL1 PreDefinedRuleBase

NextCL1 PreDefinedRuleBase_NextHour Parameters

*Display Name	Value	Bind Field	Allow Override
Priority	0		✓
Diameter Client			✓
Rule Group			✓
Rule Name	internetlvl1		✓
Enable Resource Allocation Notif	DISABLED		✓
Scheduled Hour	NextHour		✓

Figure 138: Use Case Initiators Tab



Name: NextCL1

Service Initiators

Name
default

Initiator Name: default

Conditions

Name
A policy derived AVP exists

Input Variables	Type	Operator	Value	
value (String)	Literal	=	1	Remove
code (String)	Literal	=	congestionNextHourLevel	Remove

Available Input Variables -

Control Center Configuration

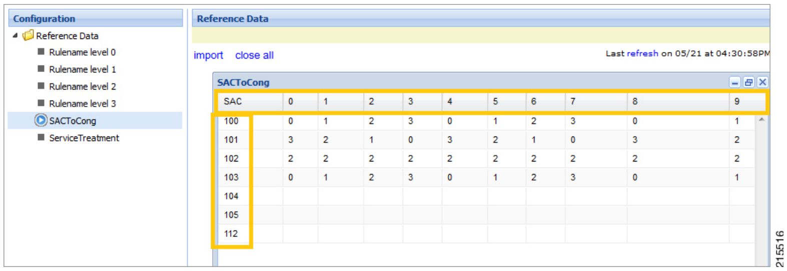
Step 1 Log into Control Center.

Step 2 Select **Configuration** > **Configuration** > **Reference Data**.

Step 3 Select the STG created in Policy Builder and add data by creating new rows.

A sample configuration is as follows:

Figure 139: Sample Configuration



Last refresh on 05/21 at 04:30:58PM

SACToCong

SAC	0	1	2	3	4	5	6	7	8	9
100	0	1	2	3	0	1	2	3	0	1
101	3	2	1	0	3	2	1	0	3	2
102	2	2	2	2	2	2	2	2	2	2
103	0	1	2	3	0	1	2	3	0	1
104										
105										
112										

Note

- 0-3 are congestion levels
- Currently, we supports only current and next level congestion.

Parameter Descriptions

The following table provides information related to RAN Congestion parameters:

Table 135: RAN Congestion Parameters

Parameter	Description
Rule Name	Any name which you want to give for rule name.
Scheduled Hour: drop-down list with three values.	Default: It turns OFF Hour Boundary RAR enhancement feature for look ahead rules installation at hour boundary and causes rules to behave in normal fashion of getting installed at hour boundary as applicable CurrentHour: For the current hour rule activation time will be current time, deactivation time will be next hour. NextHour: For the next hour rule activation time will be next hour, deactivation time will be next-next hour.

Note By default, CPS sets the next evaluation time as per the next change in congestion level. To configure CPS to do a forward lookup for multiple changes in congestion level, add the following parameter to qns.conf:

```
-DcongDataLookAhead=true
```

Usage Monitoring

Overview

CPS supports Usage-Monitoring over Diameter Gx interface with different Balance Code, Dosage and monitoring level. Usage monitoring key Identifies the usage monitoring control instance and is subscribed using Event-Trigger AVP = USAGE_REPORT.

CPS also supports time based Gx usage monitoring control and reporting based on as 3GPP 29.212 Rel 12 Sections 4.5.16 and 4.5.17. It supports the ability to configure a Gx usage monitoring key as volume, time or both.

Policy Builder Configuration

Step 1 Login to Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template for *TableDrivenCiscoQosGroupRule*.

a) Enter the name for use case template. For example, name the new template as **UsageMonitoringKey**.

b) Select **Actions** tab.

c) Click **Add** under **Service Configurations**.

Select Service Configuration dialog box opens, and all of the service configuration objects that are available on the PCRF are listed.

d) Scroll down to the **gx** area in the list of service configuration objects, and select the required usage monitoring object. For example, **UsageMonitoringKey**.

For parameter descriptions under **UsageMonitoringKey**, refer to UsageMonitoringKey, on page 464.

For parameter descriptions under **UsageMonitoringKeyDual**, refer to UsageMonitoringKeyDual, on page 465.

Step 4 In the left pane of the **Services** tab, click **Services** > **Service Options** to create a service option and add the *UsageMonitoringKey* use case template.

Step 5 In the left pane of the **Services** tab, click **Services** > **Services** to create a service and add the configured *UsageMonitoringKey* use case template.

Scheduled Usage Monitoring

To support scheduling, CPS uses Monitoring-Time AVP in Monitoring information. To use Monitoring-Time AVP CPS supports Usage Monitoring Congestion Handling (UMCH) feature on Gx. If the PCEF does not support UMCH feature, CPS uses the RAR message to request account balance usage details of the previous or older schedule. CPS will charge the account balance usage against the old schedule and further grants a new dosage value as per the new schedule.

CPS uses the next evaluation time set on the diameter session to trigger the RAR message for requesting the usage-report on schedule's time boundary. The current Usage-Monitoring information in the Gx session is added with monitoring schedules to grant and track the usage for the PCEF, based on current and adjacent schedules. It also provides support to bind different balance code to each schedule. CPS grants, reserves and charges the respective balance as per the usage monitoring schedule defined. CPS defines dosage on each schedule and accordingly grants single units to PCEF in Granted-Service-Units AVP. It also defines charging rate on each schedule. The default charging rate is 1.

This feature provides support to configure multiple schedules in monitoring-key service configuration.

Configure Scheduled Usage Monitoring

Scheduled Usage Monitoring is configured in the Service Options section of the Services tab. The Service Configuration UsageMonitoringKey allows scheduled monitoring in the Monitoring Schedule (List) parameter.

Before configuring a scheduled monitoring, the following configuration must be completed in the Policy Builder:

- Configure the Account Balance Templates in the **Reference Data** tab.

  For more information, see Account Balance Templates, on page 363.

- Configure a Use Case Template in the **Services** tab.

  For more information, see Use Case Templates, on page 231.

Configuration restrictions while defining Monitoring schedule in Policy Builder:

- The time value should be entered in hh:mm format.
- Monitoring schedule should be complete for 24 hours.

- First monitoring schedule should start at midnight with start-time value as 00:00 and last schedule should end on next midnight with end-time value as 23:59.
- Time entry with 23:59 will be rounded-up to complete the 24 hour schedule.

Step 1 Select the **Services** tab.

Step 2 Click **Services** > **Service Options**, and select the corresponding Service option whose name matches the Use Case Template.

Step 3 Provide a name for the service in the **Name** field.

Step 4 In the **Service Configurations** section, click **Add**. The **Select Service Configuration** dialog box is displayed.

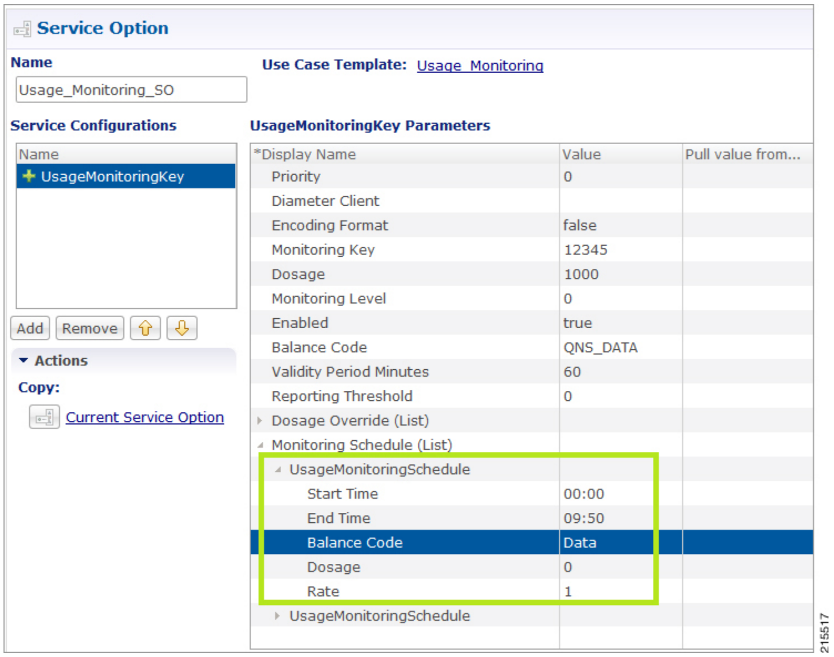
Step 5 Select **UsageMonitoringKey** and click **OK**.

For parameter descriptions under **UsageMonitoringKey**, refer to UsageMonitoringKey, on page 464.

Step 6 In the Service configuration parameters, select **Monitoring Schedule** and click **Add Child** to add a **UsageMonitoringSchedule**.

Step 7 Select the **UsageMonitoringSchedule** to provide the values as shown in the example.

Figure 140: Usage Monitoring Schedule



Service Option

Name: Usage_Monitoring_SO

Use Case Template: Usage_Monitoring

Service Configurations

Name
UsageMonitoringKey

UsageMonitoringKey Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Encoding Format	false	
Monitoring Key	12345	
Dosage	1000	
Monitoring Level	0	
Enabled	true	
Balance Code	QNS_DATA	
Validity Period Minutes	60	
Reporting Threshold	0	
Dosage Override (List)		
Monitoring Schedule (List)		
UsageMonitoringSchedule		
Start Time	00:00	
End Time	09:50	
Balance Code	Data	
Dosage	0	
Rate	1	
UsageMonitoringSchedule		

a) Enter the Start Time in 24 hrs format (00:00 to 23:59).

b) Enter the End Time in 24 hrs format (00:00 to 23:59).

c) Provide a value for the Balance Code. Click the **...** button. A window appears. Select the required **Balance Code** and click **OK**.

d) Enter the **Dosage** value.

e) Enter the **Rate** value.

To add multiple **UsageMonitoringSchedule**, click **Add Child** and add the parameters according to your requirements.

Time Usage Monitoring

CPS supports time based Gx usage monitoring control and reporting based on as 3GPP 29.212 Rel 12 Sections 4.5.16 and 4.5.17.

It supports the ability to configure a Gx usage monitoring key as volume, time or both.

Balance: This feature reuses the time related units like seconds, minutes, hours, and so on for balance that are already provided by Account Balance Templates. No new threshold types have been added. Only % thresholds can be used with Time balances.

Use Case Template: A new UsageMonitoringKeyDual service configuration has been added to support the time usage monitoring (The existing UsageMonitoringKey is still supported for Volume Usage monitoring). This new option provides a way to configure usage monitoring for both time and volume (independently as well as together under single monitoring key). To monitor usage under one key for Volume and Time, both the balance codes need to be provided in the Service Configuration. For independent monitoring, only the relevant type of fields can be set. For example, for only Volume monitoring, fields related to time monitoring can be left blank/null and vice versa. Multiple instances of UsageMonitoringKeyDual can also be included in the service configuration each corresponding to a unique monitoring key.

Gx Message Handling: The following new AVPs are now supported under this feature:

- CC-Time (within Granted-Service-Unit and Used-Service-Unit)
- Quota-Consumption-Time (within Usage-Monitoring-Information)

For configuration in Policy Builder, refer to Policy Builder Configuration, on page 305.

Bandwidth Monitoring

Overview

The purpose of this feature is to track bandwidth and apply policies based on that. Normal usage monitoring is used to track usage but not bandwidth. This feature is based on usage monitoring key being installed in order to have the usage reported by the PCEF. Using this feature, the service provider can install a monitoring key and the different thresholds that are used to flag the subscriber. This feature works in parallel with the usage monitoring feature but the usage monitoring feature has a higher priority since that one is about charging traffic. In this context 'higher priority' means that usage monitoring feature installs any usage monitoring keys it needs to do its job.

Bandwidth monitoring installs any additional monitoring keys it needs while reusing any monitoring keys that were already installed. In order to reuse a monitoring key the same monitoring key name should be used in both BandwidthMonitor and UsageMonitoringKey objects. ReportingTimeout value is in minutes and is used to set the Revalidation-Time AVP so that the subscriber has a chance to get unthrottled before the allocated dosage is used. The BandwidthThreshold Lower Value is in kbps and when the computed bandwidth used is over that value, the corresponding Label is set to the subscriber for the particular application identified by Name attribute.

Policy Builder Configuration

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab and then click **Use Case Templates**.

Step 3 If you want to create a new use case template, click **Use Case Template** in the main window under **Create Child** to open the default use case template.

Step 4 Enter the name for the template. For our example, name it as *Bandwidth Monitoring*.

Step 5 Select **Actions** tab.

Step 6 Click **Add** under **Service Configurations** to open the **Select Service Configuration** dialog box.

Step 7 Select the necessary service configuration objects and click **OK** to add the objects in **Service Configurations** pane.

Note The Bandwidth Monitoring service option includes the BaseUsageMonitoringKey that enables Gx usage monitoring for this subscriber.

Step 8 Click **Services** > **Service Options** > ***name of the Use Case Template***.

Step 9 Click **Service Options** in the main window under **Create Child** to open the **Select Service Configuration** dialog box, which contains already defined Service Configurations, and click **OK**.

Step 10 Select **BandwidthMonitor** from the **Service Configurations** pane.

a) We can monitor the Bandwidth usage on a per session rule base or per PCC rule base. For example, let us name this bandwidth monitor per session base as SESSION.
b) Under **Monitoring Key**, enter the values for Monitoring Key, Dosage, and Monitoring Level. For session level, the Monitoring Level should be 0.
c) Also enable the BaseUsageMonotoringKey.
d) Under **Bandwidth Threshold**, define three levels for bandwidth - Low, Medium and High.

Step 11 Click **Services** > **Service Options** > ***name of the Use Case Template***.

Step 12 Click **Use Case Option** in the main window under **Create Child** to open the **Use Case Option** pane and name it as **Low Bandwidth Usage**.

Step 13 Click **Add** to open the **Select Service Configuration** dialog box, select **DefaultBearerQoS** and click **OK** to add the service.

Step 14 Rename the configured service as **LowDefaultBearerQoS**.

Step 15 Click **Use Case Initiators** tab. Click plus sign (+) to add a service initiator. Rename the initiator as **Low**.

Step 16 Under **Conditions**, click **Add** to open the **Select the Condition Phrase which you would like to use** dialog box, select the required condition and click **OK**.

The added condition is displayed in **Conditions** pane.

Step 17 Click **Add All** under **Available Input Variables**.

a) In the **Value** column under name (String), enter the name for the bandwidth monitor that you specified in 10.a, on page 309.
b) In the **Value** column under label (String), enter the Bandwidth threshold value defined in 10.d, on page 309.

Step 18 Create another initiator and add the condition **A bandwidth monitor status does not exist to it**. Add the name (String) to the condition.

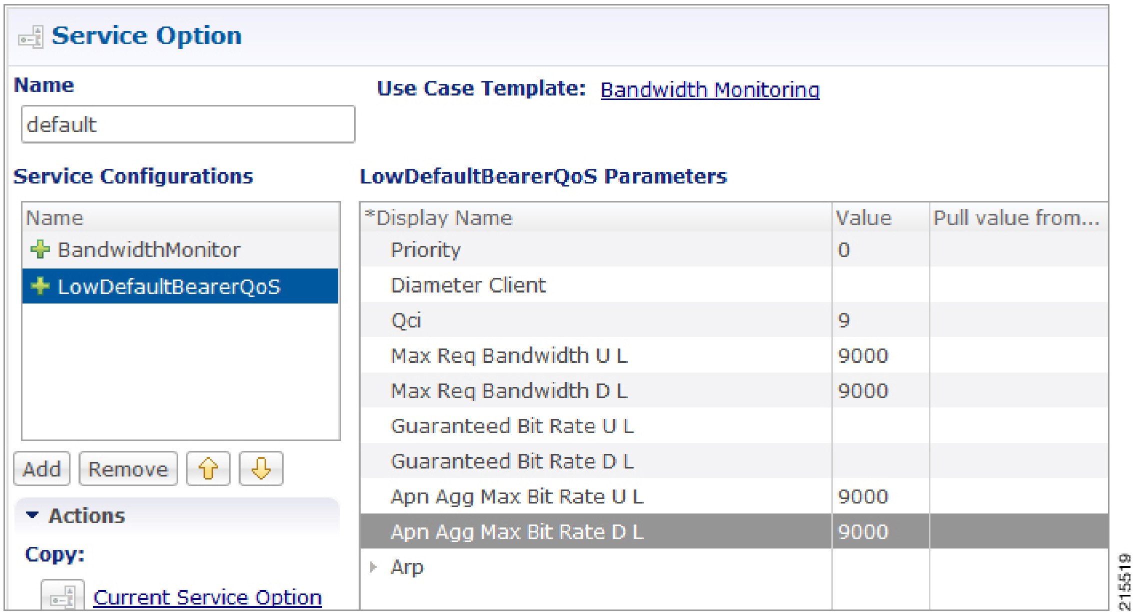
Step 19 Repeat the steps from Step 12, on page 309 to Step 17, on page 309 for Medium and High bandwidth usage.

Step 20 Click **Services** > **Service Options** > ***name of the Use Case Template*** provided in Step 4, on page 309. Add all the service configurations.

Step 21 Define the different parameters for low, medium and high bandwidth usage monitoring in the **Service Configurations** pane according to the customer requirements.

A sample configuration for Low Bandwidth Usage Monitoring is shown below.

Figure 141: Low Bandwidth Usage Monitoring



Service Option

Name: default

Use Case Template: Bandwidth Monitoring

Service Configurations

Name
BandwidthMonitor
LowDefaultBearerQoS

LowDefaultBearerQoS Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Qci	9	
Max Req Bandwidth U L	9000	
Max Req Bandwidth D L	9000	
Guaranteed Bit Rate U L		
Guaranteed Bit Rate D L		
Apn Agg Max Bit Rate U L	9000	
Apn Agg Max Bit Rate D L	9000	
Arp		

Step 22 Click **Services** > **Services**, and the click **Service** under **Create Child** to open the **Service** dialog box.

Step 23 Enter the name in **Code** and **Name** text fields.

Step 24 Click **Add** to open the **Select Service Configuration** dialog box. Select the service that you configured in Step 4, on page 309, and click **OK**.

Step 25 Select **Use V9 Event Trigger Mapping and Rel8 Usage Monitoring Supported** under **Diameter Configuration**.

- If Use V9 Event Trigger Mapping check box is not selected, the event trigger mapping ID (33) from 3GPP TS 29.212 V11.10.0 (2013-09) is used.
- If Use V9 Event Trigger Mapping check box is selected, the event trigger mapping ID (26) from 3GPP TS 29.212 V9.5.0 (2013-09) is used.

Parameter Descriptions

The following parameters can be configured in Bandwidth Monitoring:

Parameter	Description
Name	Any name you can give.
Reporting Timeout	The revalidation timer for defined dosage.
Lower Value	The minimum bandwidth value that you can give for that particular Label. This value is not standard and defined as per requirement and should be an integer.

Parameter	Description
Label	The name of label, which can depend upon the user's requirement.

Override Control AVP

Overview

CPS supports Override-Control specific AVPs in CCA-i and CCA-u responses to the PCEF on the Gx Interface and Gx RAR message. These AVPs are used to override charging parameters for predefined and static rules on the PCEF.

Policy Builder Configuration

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 3 Click **Use Case Template** link from the right side under **Create Child** to create a use case template.

Step 4 Enter the name for the template. For our example, name the new template as *CiscoOverrideControl*.

Step 5 Select **Actions** tab.

Step 6 In the newly created template, click **Add** under the **Service Configurations** pane. This will list all the service configuration objects available on the PCRF. Select the **CiscoOverrideControl** object from the **gx** section.

Step 7 After selecting the necessary service configuration object, click **OK** to add the object in **Service Configurations** pane.

The following parameters can be configured for Override Control AVP.

Table 136: Override Control AVP Parameters

Parameter	Description
Override Rule Name	Specifies the name of the rule (predefined or static) for which the override values are sent. **Note** The "Charging-Action-Name” and “Exclude-Rule” AVPs should not be sent and shall be ignored if this AVP is present.
Charging-Action-Name	Specifies the name of the charging action for which override values are sent.
Override Charging Action Exclude Rule (List)	Defines the rule name where the override will not be applied.
Override Service Identifier	Used to override the value of Service Identifier configured in the charging action.
Override Rating Group	Defines the value of the rating group configured for a static/predefined rule.
Override Reporitng Level	Used to override the value of reporting level configured in the charging action.

Parameter	Description
Override Online	If Enabled, it overrides the online value configured for static/predefined rule. Default value is Enable.
Override Offline	If Enabled, it overrides the offline value configured for static/predefined rule. Default value is Enable.
Override Metering Method	Used to override the value of Metering Method configured in the charging action.
Override QoS	This AVP is used to Override QoS-Information for a predefined rule or charging action. These values are ignored (if present) while applying override values to a static rule.
Override-Max-Requested-Bandwidth-UL	Defines the maximum bit rate allowed for the uplink direction.
Override-Max-Requested-Bandwidth-DL	Defines the maximum bit rate allowed for the downlink direction.
Override-Guaranteed-Bitrate-UL	Defines the guaranteed bit rate allowed for Uplink direction. This AVP should be included only for rules on dedicated bearers.
Override-Guaranteed-Bitrate-DL	Defines the guaranteed bit rate allowed for downlink direction. This AVP should be included only for rules on dedicated bearers.
Override-Allocation-Retention-Priority	This AVP is of type grouped and is used to override the pre-configured value of ARP.
Override Merge Wildcard	Used to merge override control charging/policy parameters between override control with specific charging action and wildcard override control.

AVP Structure in response/request message:

```
Override-Control
  *Override-Rule-Name
  Override-Charging-Action-Parameters
                    Override-Control-Merge-Wildcard
   Charging-Action-Name
   *Online-Charging-Action-Exclude-Rule
   Override-Charging-Parameters
   Override-Service-Identifier
    Override-Rating-Group
    Override-Reporting-Level
    Override-Online
    Override-Offline
    Override-Metering-Method
   Override-Policy-Parameters
    Override-QoS-Information
     Override-QoS-Class-Identifier
     Override-Max-Requested-Bandwidth-UL
     Override-Max-Requested-Bandwidth-DL
     Override-Guaranteed-Bitrate-UL
     Override-Guaranteed-Bitrate-DL
```

```
Override-Allocation-Retention-Priority
 Override-Priority-Level
 Override-Pre-emption-Capability
 Override-Pre-emption-Vulnerability
```

Name	Code	Vendor-ID	Flags		
			M	V	P
Override-Control	132017	9	0	1	0
Override-Rule-Name	132018	9	0	1	0
Override-Charging-Action-Parameters	132019	9	0	1	0
Override-Charging-Action-Exclude-Rule	132021	9	0	1	0
Override-Charging-Parameters	132022	9	0	1	0
Override-Service-Identifier	132023	9	0	1	0
Override-Rating-Group	132024	9	0	1	0
Override-Reporting-Level	132025	9	0	1	0
Override-Online	132026	9	0	1	0
Override-Offline	132027	9	0	1	0
Override-Metering-Method	132028	9	0	1	0
Override-Policy-Parameters	132029	9	0	1	0
Override-QoS-Information	132030	9	0	1	0
Override-QoS-Class-Identifier	132031	9	0	1	0
Override-Max-Requested-Bandwidth-UL	132032	9	0	1	0
Override-Max-Requested-Bandwidth-DL	132033	9	0	1	0
Override-Guaranteed-Bitrate-UL	132034	9	0	1	0
Override-Guaranteed-Bitrate-DL	132035	9	0	1	0
Override-Allocation-Retention-Priority	132036	9	0	1	0
Override-Priority-Level	132037	9	0	1	0
Override-Pre-Emption-Capability	132038	9	0	1	0
Override-Pre-Emption-Vulnerability	132039	9	0	1	0
Override Merge Wildcard	132079	9	0	1	0

Gx RAR Traffic

CPS is enhanced to support certain call flows and reduce Gx-RAR traffic towards PCEF as follows:

- Gx CCR-U reports all Rx Charging-Rule as inactive in which case PCRF terminates the Rx Session and avoids sending Gx-RAR to remove rules already reported as inactive.
- Gx CCR-U reports one or more Rx Charging Rule as inactive in which case PCRF would trigger a Rx RAR to PCSF which if responded with a DIAMETER_UNKNOWN_SESSION_ID (5002) terminates the Rx Session and avoids sending Gx RAR with Charging-Rule-Remove AVPS for rules already reported as inactive.
- Gx CCR-U reports one or more Rx Charging Rule as inactive in which case PCRF would trigger a Rx RAR to PCSF which is responded with a DIAMETER_SUCCESS (2001). Any subsequent AAR-U with MCD/MSC flow status reported as removed, removes the corresponding Rx Charging-Rule and does not trigger a Gx RAR with Charging-Rule-Remove AVP.

Configuring Policies Based on Gx Events

This section covers the following topics:

- Overview, on page 314
- Policy Builder Configuration, on page 315

Overview

CPS supports the ability to make policy decisions based on the following event triggers received over the Gx interface:

- OUT_OF_CREDIT
- REALLOCATION_OF_CREDIT
- CREDIT_MANAGEMENT_SESSION_FAILURE
- CISCO_EVENT_TRIGGER

The policy decisions based on the above event triggers could be the following:

For Gx interface:

- Switch the UE from ONLINE to OFFLINE or vice versa
- Change the Charging-Rule-Base-Name of the UE
- Change (add/delete) the Charging-Rule-Name (predefined) of the UE
- Change (add/modify/delete) the Charging-Rule-Name (Dynamic) of the UE
- Ability to retry the impacted rule, number of retries, and the unique retries between each retry

For Rx interface:

- Initiate a tear down/removal of the IMS rule over Rx
- Inform the Rx client of the impacted rule and the reason for impact

For Sy interface:

- Ability to terminate or reinitiate Sy session

For Sd interface:

- Ability to terminate Sd session

Policy Builder Configuration

The following procedure is an example of how to configure Policy Builder to use the ActionBasedOnGxEventTrigger service configuration object to make policy decisions based on event triggers and associated rule failure codes received over the Gx interface.

Step 1 Log into Policy Builder.

Step 2 Click **REFERENCE DATA** > **Custom Reference Data Tables** > **Search Table Groups**.

Step 3 Click **Search Table Group**.

Step 4 Under Table Search Initiators do the following to evaluate the CRD such that the condition is always false and table is not evaluated every time on any event by the policy engine:

a) Click the **+** sign to add an initiator.
b) Enter a name for the initiator in the Initiator Name field.
c) Select **A customer reference data AVP exists** as the initiator conditions.
d) Select **A customer reference data AVP exists**, click the **Add code**, and then enter **CRD-CODE** (dummy value to restrict CRD evaluation) as the code value. Similarly, click **Add value**, and then enter **true** as the value.

Step 5 Click the **Custom Reference Data Table** link.

Step 6 Under Columns, click **Add** and enter the following input and output values:

- CHARGING-RULE-NAME: This input value should be set to **Key** and **Runtime Binding** should be set to **None**.
- RULE-FAILURE-CODE: This input value should be set to **Key** and **Runtime Binding** should be set to **None**.
- CISCO-CC-FAILURE-TYPE: This input value should be set to **Key** and **Runtime Binding** should be set to **None**.
- Credit-Management-Status: This input value should be set to **Key**. For **Runtime Binding**, select **Bind to Diameter request AVP code** and enter **`Credit-Management-Status`**.
- Rx-Rule-Remove: Output value. Possible values are true and false.
- Session-ReInitiate: Output value. Possible value is SY_V11.
- Session-Terminate: Output value. Possible values are: SY_V11, SD_V11, or SY_V11;SD_V11.

The input AVPs and their corresponding CRD input columns must be configured in the ActionBasedOnGxEventTrigger service configuration object. When CPS receives a Gx CCR message with the Charging-Rule-Report AVP or the Credit-Management-Status AVP, CPS performs a one-time query on this CRD table.

A one-time query on this CRD is also performed when CPS receives Charging-Rule-Report AVP with ACTIVE_WITHOUT_CREDIT_CONTROL(10) for PCC-Rule-Status and Cisco-Event with Cisco-CC-Failure-Type.

If the Remove-Rx-Rule AVP exists in the output with value = true, the following conditions can occur:

- In case the query is based on Charging-Rule-Report AVP, then the rule status is updated as INACTIVE for all the reported rules and CPS sends Rx RAR for those rules.

Note Rx RAR will only be sent if Specific-Action = INDICATION_OF_FAILED_RESOURCES_ALLOCATION is subscribed by the AF or Specific-Action = INDICATION_OF_OUT_OF_CREDIT is subscribed by the AF and OUT_OF_CREDIT event trigger (Gx) is received in CCR-U.

- In case the query is based on Credit-Management-Status AVP, then all Rx rules are removed and Rx session is terminated by sending Rx ASR.

Step 7 Select the **Services** tab, and then click **Use Case Templates** > **Summary**.

Step 8 Click the **Use Case Template** link from the right side under **Create Child** to create a use case template.

Step 9 Enter the name for the template. In this example, name the new template as *ActionBasedOnGxEventTrigger* .

Step 10 Click the **Actions** tab.

Step 11 In the newly created template, click **Add** under the **Service Configurations** pane. This will list all the service configuration objects available on PCRF. Select the **ActionBasedOnGxEventTrigger** object under the **gx** section.

Step 12 Click **OK** to add the object in **Service Configurations** pane.

For the list of configurable parameters see ActionBasedOnGxEventTrigger , on page 423

Important The **AVP Name** must be the same as mentioned in the following table while defining parameter values for ActionBasedOnGxEventTrigger Service Configuration object. The **Column** values are referenced from example CRD table columns created in Step 6, on page 315. The other values mentioned in the table are used for example purpose only.

Table 137: Parameter Values for ActionBasedOnGxEventTrigger Service Configuration Object

Parameter	Value
Stg Reference	Event-Rule-Failure-Mapping
List of Input Column Avp Pairs	
Avp Name	Charging-Rule-Name
Column	CHARGING-RULE-NAME
Avp Name	Rule-Failure-Code
Column	RULE-FAILURE-CODE
Avp Name	Cisco-CC-Failure-Type
Column	CISCO-CC-FAILURE-TYPE
List of Output Column Avp Pairs	
Avp Name	Remove-Rx-Rule
Column	Rx-Rule-Remove
Avp Name	Terminate-Session
Column	Session-Terminate

Parameter	Value
Avp Name	Reinitiate-Session
Column	Session-ReInitiate

Important For any Gx action, a generic output column can be added which can be used as an input to any other CRD table.

Step 13 Click **Use Case Initiators** and do the following so that the use case is true only in the following conditions:

When CPS receives event trigger CREDIT_MANAGEMENT_SESSION_FAILURE:

a) Click the + sign to add a service initiator.
b) Enter a name for the initiator in the Initiator Name field.
c) Select **A Gx Event Triggr exists** as the initiator conditions.
d) Select **A Gx Event Triggr exists**, click the **Add All**, and then enter **46** as the **eventTrigger** value.

When CPS receives event trigger CREDIT_MANAGEMENT_SESSION_FAILURE (46) and/or Cisco-Event with CREDIT-CONTROL-FAILURE (5):

a) Click the + sign to add a service initiator.
b) Enter a name for the initiator in the Initiator Name field.
c) Select **CustomCiscoEvent** as the initiator conditions.
d) Select **A Cisco Custom Gx Event Trigger exists**, click the **Add All**, and then enter **5** as the **eventTrigger** value.
e) Select **A Gx Event Trigger exists** as the initiator conditions.
f) Select **A Gx Event Trigger exists**, click the **Add All**, and then enter **46** as the **eventTrigger** value.

Common Parameters Used

The following table contains the common parameters that can be configured under all the sections mentioned in this chapter:

Table 138: Common Parameters

Parameter	Description
Qci	The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0, 10 – 255 are divided for usage as follows: • 0: Reserved • 10-127: Reserved • 128-254: Operator specific • 255: Reserved
Max Req Bandwidth UL	It defines the maximum bit rate allowed for the uplink direction.

Parameter	Description
Max Req Bandwidth DL	It defines the maximum bit rate allowed for the downlink direction.
Guaranteed Bit Rate UL	It defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bit Rate DL	It defines the guaranteed bit rate allowed for the downlink direction.
Apn Agg Max Bit Rate UL	It defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN.
Apn Agg Max Bit Rate DL	It defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN.
Priority Level Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.	The priority level is used to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest level of priority. • Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. • Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.
Preemption Capability	If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can get resources that were already assigned to another bearer with a lower priority level. • 0: This value indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. • 1: This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.

Parameter	Description
Preemption Vulnerability	If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can lose the resources assigned to it in order to admit a pre-emption capable bearer with a higher priority level. • 0: This value indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied. • 1: This value indicates that the resources assigned to the service data flow or bearer shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level.
Monitoring Key	Identifies a usage monitoring control instance. Any value can be given.
Priority	It is priority of the service option within the service.
Diameter Client	The client configuration is used to apply different policies based on PCEF type. This is optional parameter.
Rule Group	Rule Group is to classify rules at PCRF to change set of predefined rules based on policy. This is an optional parameter.
Enable Resource Allocation Notification	This is having two values Enabled and Disabled. Default value is disabled.
Dual Stack Session	This is having two values Enabled and Disabled. Default value is disabled.
Framed I P Type	It is having four options. Default option is ANY_ONE. • ANY_ONE • BOTH • IPv4_ADDRESS • IPv6_ADDRESS
ToD Schedule	Identifies the schedule for rule activation and deactivation.

Sd Services

Overview

The Sd reference point is located between the Policy and Charging Rules Function (PCRF) and the Traffic Detection Function (TDF). The Diameter session on Sd is established either at the request of the PCRF in case of solicited application reporting by initiating a (TSR - TDF Session Request) or at the request of the TDF by initiating an (CCR-I) in case of unsolicited application reporting. Session modifications may be initiated by either TDF or PCRF.

Solicited Application

For the solicited application reporting, the Sd reference point is used for:

- Establishment and termination of TDF session between PCRF and TDF.
- Provisioning of Application Detection and Control rules from the PCRF for the purpose of traffic detection and enforcement at the TDF.
- Usage monitoring control of TDF session and of detected applications.
- Reporting of the start and the stop of a detected application's traffic and transfer of service data flow descriptions for detected applications, if deducible, from the TDF to the PCRF.

Unsolicited Application

For the unsolicited application reporting, the Sd reference point is used for:

- Establishment and termination of TDF session between PCRF and TDF.
- Reporting of the start and the stop of a detected application's traffic.
- Transfer of service data flow descriptions for detected applications, if deducible, and transfer of Application instance identifier, if service data flow descriptions are deducible, from the TDF to the PCRF.

As part of the IP-CAN Session Establishment or Modification procedure, in case of solicited application reporting with a TDF, the PCRF initiates a TDF Session Establishment with the selected TDF. The TDF is selected based on data received from the PCEF or a local configuration at the PCRF and or SPR data for the subscriber.

TDF Session Termination happens in any of the following cases:

- The corresponding IP-CAN session is terminated.
- At any point of time when the PCRF decides that the session with TDF is to be terminated (for example, subscriber profile changes).

Policy Builder Configuration

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab, and then click **Use Case Templates**. Click **Summary** and select **Use Case Template**.

Step 3 Click **Actions** tab.

Step 4 Click **Add** to open the **Select Service Configuration** dialog box.

Step 5 Select **ADC-Predefined-Rule** and click required service configuration parameters that need to be configured. Click **OK** to add the service in **Service Configuration** pane.

Step 6 In the **Services** tab, click **Services** > **Service Options** to create a service option and add the Use Case Template that you just configured.

Step 7 In the **Services** tab, click **Services** > **Services** to create a service and add the Use Case Template that you just configured.

Common Parameters Used

The following table contains the common parameters configured for Sd Services:

Table 139: Common Parameters

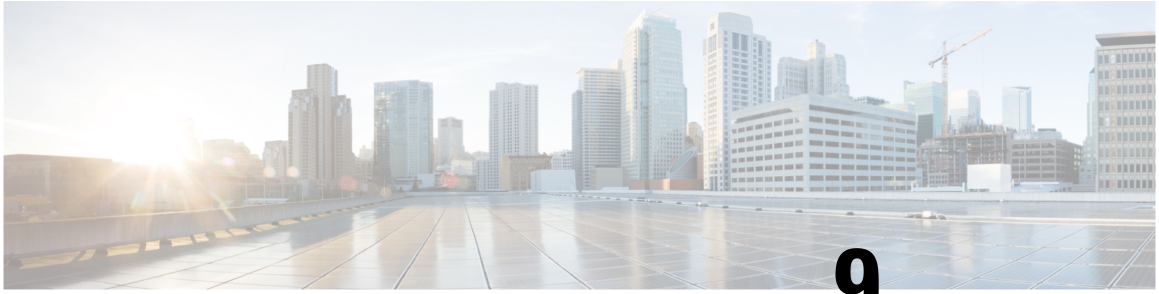
Parameter	Description
Qci	The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0, 10 – 255 are divided for usage as follows: • 0: Reserved • 10-127: Reserved • 128-254: Operator specific • 255: Reserved
Max Req Bandwidth UL	It defines the maximum bit rate allowed for the uplink direction.
Max Req Bandwidth DL	It defines the maximum bit rate allowed for the downlink direction.
Guaranteed Bit Rate UL	It defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bit Rate DL	It defines the guaranteed bit rate allowed for the downlink direction.
Apn Agg Max Bit Rate UL	It defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN.
Apn Agg Max Bit Rate DL	It defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN.
Priority Level Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.	The priority level is used to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest level of priority. • Values: 1 to 8 - assigned for services that are authorized to receive prioritized treatment within an operator domain. • Values: 9 to 15 - Can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.

Parameter	Description
Preemption Capability	If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can get resources that were already assigned to another bearer with a lower priority level. • 0: This value indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. • 1: This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.
Preemption Vulnerability	If it is provided within the QoS-Information AVP, the AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the default bearer can lose the resources assigned to it in order to admit a preemption capable bearer with a higher priority level. • 0: This value indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied. • 1: This value indicates that the resources assigned to the service data flow or bearer shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level.
Monitoring Key	Identifies a usage monitoring control instance. Any value can be given.
Priority	It is priority of the service option within the service.
Diameter Client	The client configuration is used to apply different policies based on PCEF type. This is optional parameter.
Rule Group	Rule Group is to classify rules at PCRF to change set of predefined rules based on policy. This is an optional parameter.
Flow Status	Defines whether the service data flow is enabled or disabled.
Redirect Address Type	Defines the address type of the address given in the Redirect-Server-Address AVP.
Redirect Support	This value indicates that redirection is enabled for a detected application's traffic.
Redirect Server Address	This value indicates the target for redirected application traffic.

Parameter	Description
Event-Trigger	This is not to re-request rules. Primarily to notify start/stop of applications or report usage.

Table 140: Sd Parameters

Parameter	Description
Tdf Application Identifier	This references the application detection filter (for example, its value may represent an application such as a list of URLs, etc.), which the PCC rule for application detection and control in the PCEF applies.
Mute Notification	An indication whether application start/stop notification is to be muted for ADC Rule by the TDF.



CHAPTER 9

Rx Services

Overview

CPS is a carrier-grade policy, charging, and subscriber data management solution. It helps service providers rapidly create and bring services to market, deliver a positive user experience, and optimize network resources. It also generates monetization opportunities across 3G, 4G, and LTE access networks as well as IP Multimedia Subsystem (IMS) service architectures.

CPS supports various carrier-based multi-media services by acting as a gateway between the IMS core and Packet core network. CPS PCRF supports 3GPP standard Rx interface and comply with related specifications (29.214, 29.213 and 29.212). With these capabilities CPS supports VoLTE, VoLTE emergency calls, Dynamic PCC, MPS, Sponsored Data, QoS enhancements, SRVCC, Access network information reporting and many more such functionalities.

This chapter covers information on various services and policies related to Rx interface mentioned above. It gives functional information, configuration details and troubleshooting steps for setting up Rx related services and features in CPS.

VoLTE

This section explains CPS policy management configuration for Voice over LTE (VoLTE). VoLTE requires a policy management solution to:

- Establish and release the bearer for voice traffic on behalf of the IP multimedia system (IMS) domain.

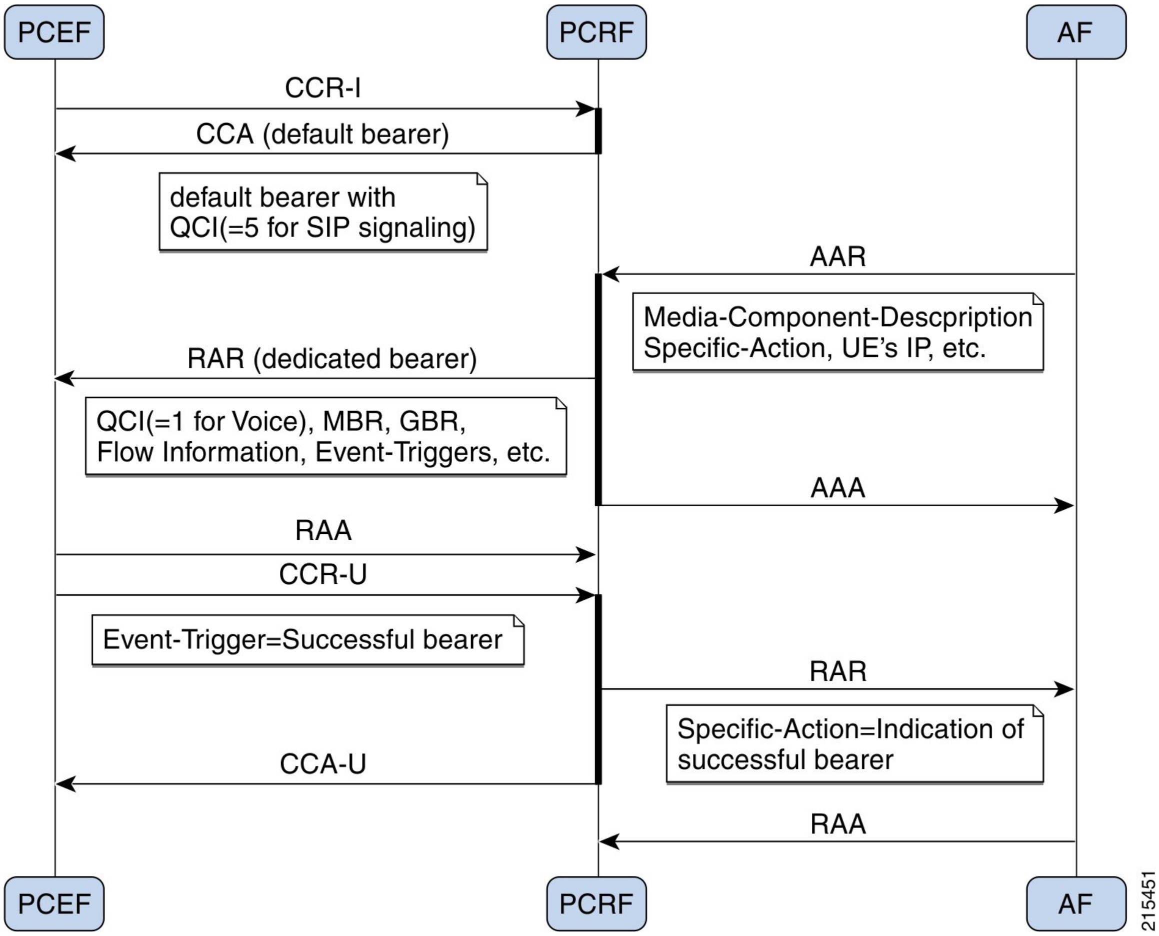
- Forward the bearer allocation status and subscriber location from the packet core to the IMS domain.
- Forward charging information from the IMS domain to the evolved packet core.
- Handle supplementary services, such as call forwarding and call holding, that are delivered in the IMS domain.

A normal VoLTE call includes:

1. Creating a Gx session with default bearer activation (for example, QCI=5 for SIP signaling).
2. UE IMS (SIP) registration.
3. P-CSCF (AF) initiates dedicated bearer requests to CPS (AAR with Media-Component-Description, Specific-Action, and so on.
4. Creating a Rx session and session binding at CPS (bind to Gx session).
5. PCRF authorizes QoS and dedicated bearer activation (for example, QCI=1 for VoLTE voice bearer, MBR, GBR, and so on).
6. QoS information is derived based on algorithm defined in section 6.3 of 3GPP 29.213 specifications.
7. QoS information is updated based on QoS policies or services configured in CPS (for example, Dynamic QoS).
8. PCEF reports bearer creation status and same is indicated to P-CSCF by CPS.

The following diagram shows the above steps with an example for dedicated bearer establishment in VoLTE call flow:

Figure 142: Example VoLTE Call


PCEF
PCRF
AF
CCR-I
CCA (default bearer)
default bearer with
QCI(=5 for SIP signaling)
AAR
Media-Component-Descpription
Specific-Action, UE's IP, etc.
RAR (dedicated bearer)
QCI(=1 for Voice), MBR, GBR,
Flow Information, Event-Triggers, etc.
AAA
RAA
CCR-U
Event-Trigger=Successful bearer
RAR
Specific-Action=Indication of
successful bearer
CCA-U
RAA
PCEF
PCRF
AF
215451

Policy Builder Configuration

Diameter Stack for Rx

To enable VoLTE services in CPS following diameter configuration is required in Policy Builder:

- Local endpoints to bind and bring up the diameter server for Rx interface.
- Entry in the 'Inbound Peers' for realms and peers that will interact with CPS over Rx interface.

See Diameter Configuration, on page 75 for information on configuring the diameter stack for Rx interface.

Service Configuration for VoLTE

Domain Configuration

A dedicated "IMS" APN may be used for VoLTE traffic. Typically, established during initial attach as default APN. In CPS, operator may define a separate domain to authorize VoLTE calls based on the APN (Called-Station-Id) received in the CCR-I message.

See Basic Systems Configuration, on page 9 for information on configuring a domain.

The following example shows a sample domain configuration:

Step 1 Log into Policy Builder.

Step 2 Click the **Services** tab.

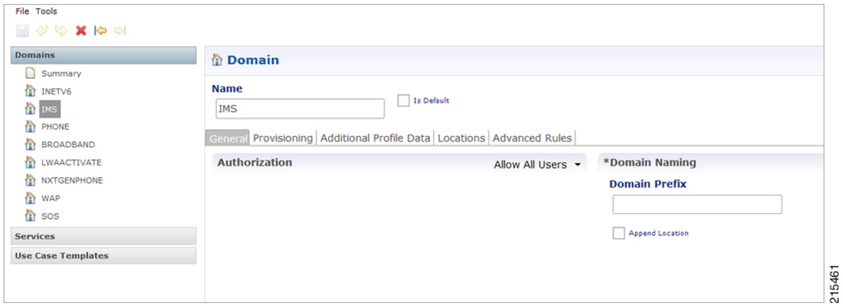
Step 3 Under **Domains**, click **Summary** and then create a child domain.

Step 4 Configure the domain by setting the required configuration for Authorization, Location and default service details as shown in example below.

In this example the domain is configured for messages received with “IMS” APN (Called-Station-Id), it authorizes all user and attaches a default service (with name “IMS”) to the subscriber.

Select **Allow all Users for Authorization**:

Figure 143: General Domain Information



Name: IMS

□ Is Default

Authorization: Allow All Users

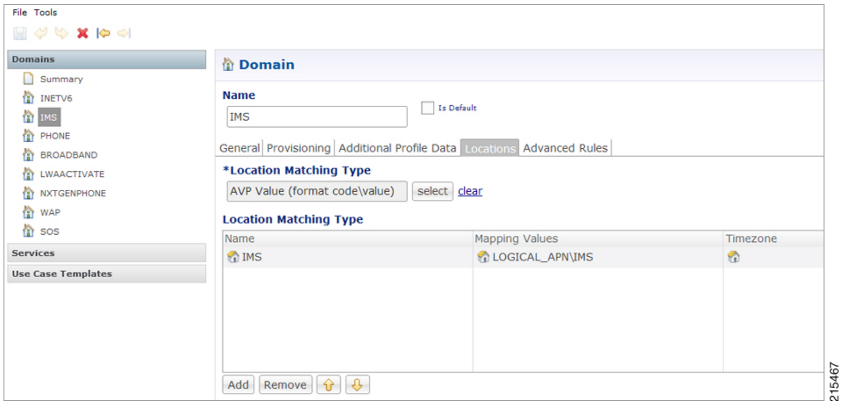
*Domain Naming

Domain Prefix:

□ Append Location

Use this domain for calls received for “IMS” APN (APN is derived from 'Called-Station-Id' AVP received in CCR-I message and mapped to a LOGICAL_APN AVP):

Figure 144: Domain Locations



Name: IMS

□ Is Default

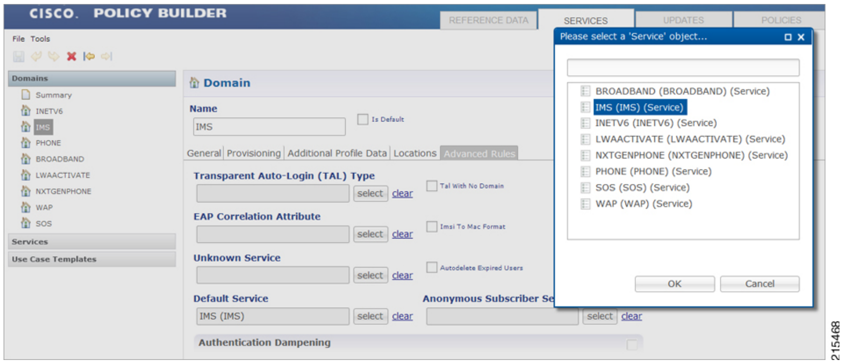
*Location Matching Type: AVP Value (format code\value)

Location Matching Type

Name	Mapping Values	Timezone
IMS	LOGICAL_APN\IMS	

Defining a default service:

Figure 145: Default Service



Domain

Name: IMS

□ Is Default

Transparent Auto-Login (TAL) Type

□ Tal With No Domain

EAP Correlation Attribute

□ Imsi To Mac Format

Unknown Service

□ Autodelete Expired Users

Default Service: IMS (IMS)

Anonymous Subscriber Se

Authentication Dampening

Please select a 'Service' object...

- BROADBAND (BROADBAND) (Service)
- IMS (IMS) (Service)
- INETV6 (INETV6) (Service)
- LWAACTIVATE (LWAACTIVATE) (Service)
- NXTGENPHONE (NXTGENPHONE) (Service)
- PHONE (PHONE) (Service)
- SOS (SOS) (Service)
- WAP (WAP) (Service)

See Basic Systems Configuration, on page 9 for more information on Domain configuration.

Service Configuration

While defining the service for VoLTE call, following service options can be used.

RxQoSInformation Service Configuration

This service configuration provides an option to define QoS values at service level to be used for dedicated bearer. It provides values to be used during the derivation of the Maximum Authorized Data Rates Authorized Guaranteed Data Rates and Maximum Authorized QoS Class Id in the PCRF whenever the “operator special policy exists” phrase is used in the algorithm (3GPP 29.213) description.

The service configuration provides only the QoS AVP output values. It does not have any key parameters. So the QoS values are applied based upon the service (code) enabled for the subscriber.

Table 141: RxQosInformation Service Configuration Parameters

Parameter	Description
Qci	QoS-Class-Identifier AVP value
Max Requested Bandwidth U L	Max-Requested-Bandwidth-UL AVP value
Max Requested Bandwidth D L	Max-Requested-Bandwidth-DL AVP value
Guaranteed Bitrate UL	Guaranteed-Bitrate-UL AVP value
Guaranteed Bitrate DL	Guaranteed-Bitrate-DL AVP value
ARP (Allocation Retention Priority)	
Priority-Level	Priority-Level AVP value
Preemption-Capability	Pre-emption-Capability AVP value
Preemption-Vulnerability	Pre-emption-Vulnerability AVP value

For more information on these parameters, see Diameter Configuration, on page 75.

RxAppQosInformation Service Configuration

This service configuration provides an option to define authorized QoS values at service level for a combination of 'Application-id' and 'Media-Type' value. It provides values to be used during the derivation of the Maximum Authorized Data Rates Authorized Guaranteed Data Rates and Maximum Authorized QoS Class Id in the PCRF whenever the “operator special policy exists” phrase is used in the algorithm (3GPP 29.213) description.

The service configuration uses the Af-Application-Id and Media-Type as keys (inputs) for selecting the QoS information AVP values. So the QoS values are selected based upon the Af-Application-Id Media-Type (received in the AAR message) and the service (code) enabled for the subscriber.

Table 142: RxAppQosInformation Service Configuration Parameters

Parameter	Description
Af Application Id (Input)	Specify the AF-Application-Id for which the QoS values should be applied.
Media Type (Input)	Specify the Media-Type for which the QoS values should be applied. (Integer value as per 3GPP specifications).
Qci	QoS-Class-Identifier AVP value
Max Requested Bandwidth U L	Max-Requested-Bandwidth-UL AVP value
Max Requested Bandwidth D L	Max-Requested-Bandwidth-DL AVP value
Guaranteed Bitrate UL	Guaranteed-Bitrate-UL AVP value
Guaranteed Bitrate DL	Guaranteed-Bitrate-DL AVP value
ARP (Allocation Retention Priority)	
Priority-Level	Priority-Level AVP value
Preemption-Capability	Pre-emption-Capability AVP value
Preemption-Vulnerability	Pre-emption-Vulnerability AVP value

For more information on these parameters see Diameter Configuration, on page 75.

Note When both RxQosInformation and RxAppQosInformation service configuration are configured, then CPS derives QoS values based on RxAppQosInformation and if not found then it uses RxQosInformation values.

RxGaranteedBitRateOverride Service Configuration

This service configuration provides a configuration option for copying the Max Requested Bit-rate values into Guaranteed Bit-rate. This configuration is applicable when CPS is not able to derive Guaranteed Bitrate values based on the QoS derivation algorithm defined in 3GPP 29.213 specification. So if GBR is not derived and this service option is configured then CPS will copy the values derived for Max Requested Bitrates into Guranteed Bitrates (applicable for both UL and DL).

Table 143: RxGaranteedBitRateOverride Parameter

Parameter	Description
Set Guaranteed Bitrates from Max requested Bitrates	Flag that indicates whether to copy the MBR values into GBR values when GBR is not derived Default value is checked (true).

Note In a VoLTE specific service Operator can also define basic Gx specific services configurations like DefaultBearerQos Event-Trigger and so on. For more information on these services configuration, see Gx/Sd Services, on page 267.

The following steps configure the Service options details (RxAppQosInformation RxAppQosInformation) for setting up a sample VoLTE specific service.

Step 1 Log into Policy Builder.

Step 2 Go to the **Services** tab.

Step 3 Under **Use Case Templates**, click **Summary** and then create a child Use Case Template.

Step 4 Add a name to the template, for example, `Rx_VoLTE`.

Step 5 Click **Actions** tab.

Step 6 Click **Add** in the **Service Configuration** pane and add “RxQosInfomration” service configurations listed under the 'rx' section.

Similarly, operator can optionally add other service configurations like RxAppQosInformation, RxGuaranteedBitrateOverride, listed under 'rx' section as well as DefaultBearerQos, Event-Trigger, and so on. listed under 'gx' section.

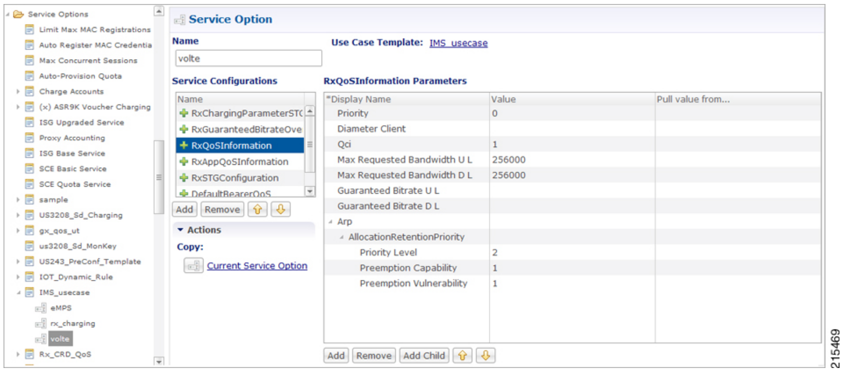
Step 7 Click **Services Options**. The newly created template is available here.

Step 8 Create a child **Service Option**, for example, `volte`.

Step 9 Click **OK**. The newly created service options should have the service configuration objects that were added previously at the template level.

Step 10 Select the **RxQoSInfomration** service configuration and configure it as per your requirements.

Figure 146: RxQoSInformation Service



Name: volte

Use Case Template: IMS_usecase

Service Configurations

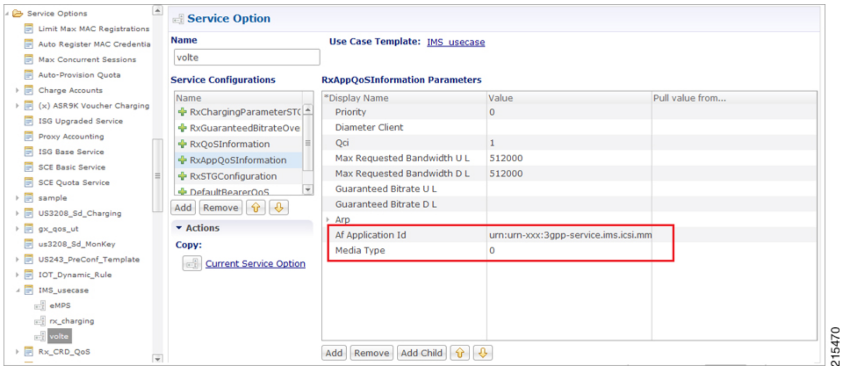
Name
RxChargingParameterSTC
RxGuaranteedBitrateOve
RxQoSInformation
RxAppQoSInformation
RxSTGConfiguration
DefaultBearerQoS

RxQoSInformation Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Qci	1	
Max Requested Bandwidth U L	256000	
Max Requested Bandwidth D L	256000	
Guaranteed Bitrate U L		
Guaranteed Bitrate D L		
Arp		
AllocationRetentionPriority		
Priority Level	2	
Preemption Capability	1	
Preemption Vulnerability	1	

Step 11 Select the **RxAppQoSInfomration** service configuration and configure it as per your requirements.

Figure 147: RxAppQoSInformation Service



Name: volte

Use Case Template: IMS_usecase

Service Configurations

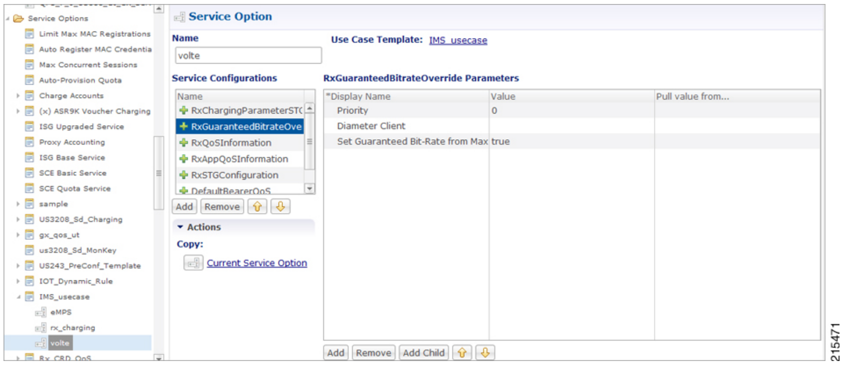
Name
RxChargingParameterSTC
RxGuaranteedBitrateOve
RxQoSInformation
RxAppQoSInformation
RxSTGConfiguration
DefaultBearerQoS

RxAppQoSInformation Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Qci	1	
Max Requested Bandwidth U L	512000	
Max Requested Bandwidth D L	512000	
Guaranteed Bitrate U L		
Guaranteed Bitrate D L		
Arp		
Af Application Id	urn:urn-xxx:3gpp-service.ims.icsi.mm	
Media Type	0	

Step 12 Select the **RxGuaranteedBitrateOverride** service configuration and configure it as per your requirements.

Figure 148: RxGuaranteedBitrateOverride Service



Name: volte

Use Case Template: IMS_usecase

Service Configurations

Name
RxChargingParameterSTC
RxGuaranteedBitrateOve
RxQoSInformation
RxAppQoSInformation
RxSTGConfiguration
DefaultBearerQoS

RxGuaranteedBitrateOverride Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Set Guaranteed Bit-Rate from Max	true	

Step 13 Click **Services** and create a child service, for example, `volte_service`.

Step 14 Update the **Code** and **Name** as `volte_service`.

Step 15 Click **Add** and select the Service Option **volte** created earlier.

Service Configuration to Handle VoLTE Issues

Dedicated Bearer Creation Fails

In case VoLTE setup fails, that is, the dedicated bearer creation fails with some RAN/NAS cause code, CPS receives the rule failure report with a RAN/NAS cause code from PCEF. CPS can retry the dedicated bearer setup based on these RAN/NAS cause codes, so that the failure to create the dedicated bearer can be minimized.

Use the RxRanNasCauseRetry service option to handle this issue. For this, create the following list of RAN/NAS Search Table Groups (STGs):

Table 144: STG Name Reference Mapping

Stg Reference	Stg Name
Ran_Nas_Cause_Mapping_Table	Ran_Nas_Cause_Mapping
Rx_Parameters_Table	Rx_Parameters
Gx_Parameters_Table	Gx_Parameters
Sy_Parameters_Table	Sy_Parameters
Ran_Nas_Retry_Mapping_Table	Ran_Nas_Retry_Mapping

Note

- Stg Reference is bound to the CRD table created by the user.
- Stg Name is the corresponding CRD table name entered by the user in the RxRanNasCauseRetry service option. The STG name should be same as the Stg Name values in the above table.
- For more information on how to create Search Table Groups, refer to RxSTGConfiguration Service Configuration, on page 342.
- CPS supports wildcarding for all the input values in the CRD tables. To use wildcarding, select the **Best Match** check box in the STG table. CPS supports wildcarding as per the standard Java regex patterns.

Step 1 Create the Ran_Nas_Cause_Mapping CRD table as follows:

a) This table is used to find the RAN/NAS Cause group from Protocol type and Cause type.

Note The Protocol Type and Cause Type are decoded from the RAN-NAS-Release-Cause AVP. For example, if the system receives 1234 as the RAN-NAS-Release-Cause AVP, 1 is decoded as the Protocol Type and 2 is decoded as the Cause Type. Cause value 34 can be ignored.

If multiple instances of RAN-NAS-Release-Cause AVP are received in a message, CPS runs a CRD query for each RAN/NAS cause code and gets the corresponding RAN/NAS cause group. The group with the highest priority is chosen.

b) Refer to the following table for its parameters.

Note Avp Name column is the corresponding AVP name entered by the user in the RxRanNasCauseRetry service option. The AVP name should be same as the Avp Name values shown in the following table.

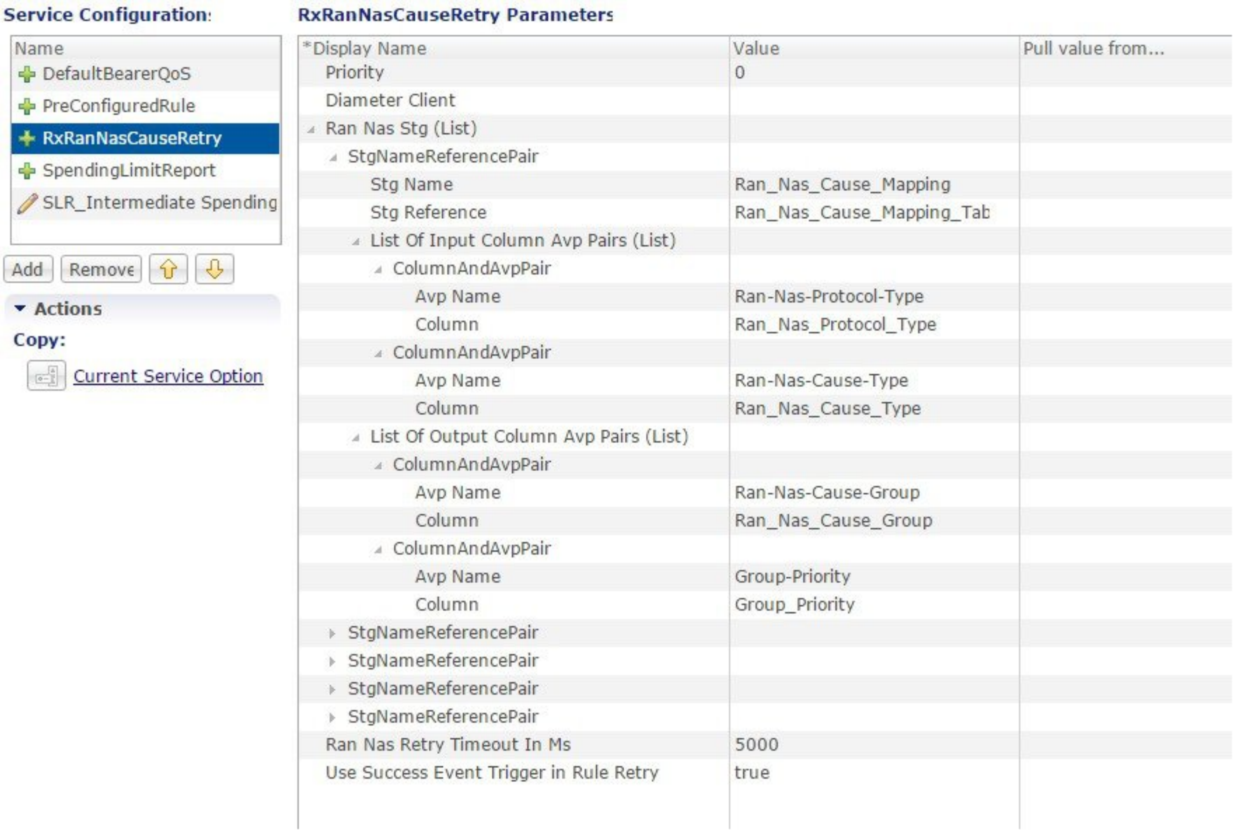
Table 145: Ran_Nas_Cause_Mapping CRD Table

Column Name	Avp Name	Binding/Retriever	Column Type
Ran_Nas_Protocol_Type	Ran-Nas-Protocol-Type	None	Input
Ran_Nas_Cause_Type	Ran-Nas-Cause-Type	None	Input
Group_Priority	Group-Priority	Not Applicable	Output

Column Name	Avp Name	Binding/Retriever	Column Type
Ran_Nas_Cause_Group	Ran-Nas-Cause-Group	Not Applicable	Output

c) Configure the Ran_Nas_Cause_Mapping table in the RxRanNasCauseRetry service option.

Figure 149: RxRanNasCauseRetry Service Option for Ran_Nas_Cause_Mapping



*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Ran Nas Stg (List)		
StgNameReferencePair		
Stg Name	Ran_Nas_Cause_Mapping	
Stg Reference	Ran_Nas_Cause_Mapping_Tab	
List Of Input Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Ran-Nas-Protocol-Type	
Column	Ran_Nas_Protocol_Type	
ColumnAndAvpPair		
Avp Name	Ran-Nas-Cause-Type	
Column	Ran_Nas_Cause_Type	
List Of Output Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Ran-Nas-Cause-Group	
Column	Ran_Nas_Cause_Group	
ColumnAndAvpPair		
Avp Name	Group-Priority	
Column	Group_Priority	
StgNameReferencePair		
StgNameReferencePair		
StgNameReferencePair		
StgNameReferencePair		
Ran Nas Retry Timeout In Ms	5000	
Use Success Event Trigger in Rule Retry	true	

Where,

- **Use Success Event Trigger in Rule Retry**:
  - When set to `true`: CPS adds the SUCCESSFUL_RESOURCE_ALLOCATION event trigger in rule retry CCA message. This is added so that PCEF can notify the successful allocation of the rule. On receipt of successful resource event for the rule from PCEF, CPS sends success Rx RAR to AF with success RAN/NAS cause and all last known RAN/NAS cause AVPs received from PCEF for this rule.
  - When set to `false`: CPS does not use SUCCESSFUL_RESOURCE_ALLOCATION event trigger. So, on Ran Nas Retry timer expiry, CPS treats it as successful installation of the rule and sends success Rx RAR to AF with success RAN/NAS cause and all last known RAN/NAS cause AVPs received from PCEF for this rule.

  Note CPS sends success Rx RAR only if Rx-Message-On-Retry-Success is true in the CRD data.

- **Ran Nas Retry Timeout in Ms**: The time (in milliseconds) after which the TimerExpired message is pushed into policy engine to evaluate rule retry as success or failure and also send RAR on Rx and Gx.

Note

- If **Use Success Event Trigger in Rule Retry** is `true`, rule retry is treated as failure on this timer expiry.
- If **Use Success Event Trigger in Rule Retry** is `false`, rule retry is treated as success on this timer expiry.

Step 2 Create the Rx_Parameters CRD table as follows:

a) This table is used to configure Rx parameters to be used in RAN/NAS retry algorithm. Input is one or more of the following supported **Rx Parameters** and Output is **Rx_Parameters_Group**.

b) Refer to the following table for the list of currently supported input parameters on the Rx interface.

Note

- Avp Name column is the corresponding AVP name entered by the user in the RxRanNasCauseRetry service option. The AVP name should be same as the Avp Name values shown in the following table.
- Not all parameters are mandatory. Choose the parameters as per your requirement.

Table 146: Rx_Parameters CRD Table

Column Name	Avp Name	Binding/Retriever	Column Type
AF_Application_Identifier	AF-Application-Identifier	None	Input
Media_Type	Media-Type	None	Input
Bearer_Setup	Bearer-Setup	None	Input
Rx_Session_Number	Rx-Session-Number	None	Input
Sponsor_Identity	Sponsor-Identity	None	Input
Application_Service_ Provider_Identity	Application-Service- Provider-Identity	None	Input
Service_URN	Service-URN	None	Input
Rx_Request_Type	Rx-Request-Type	None	Input
Ran_Nas_Cause_Group	Ran-Nas-Cause-Group	None	Input
Rx_Parameters_Group	Rx-Parameters-Group	Not Applicable	Output

c) Configure the Rx Parameters table in the RxRanNasCauseRetry service option as shown in Figure 149: RxRanNasCauseRetry Service Option for Ran_Nas_Cause_Mapping, on page 334.

Step 3 Create the Gx_Parameters CRD table as follows:

a) This table is optional and is used to configure Gx parameters to be used in RAN/NAS retry algorithm. Inputs are one or more of the following supported Gx**Parameters** and Output is **Gx_Parameters_Group**.

b) Refer to the following table for the list of currently supported input parameters on the Gx interface.

Note Avp Name column is the corresponding AVP name entered by the user in the RxRanNasCauseRetry service option. The AVP name should be same as the Avp Name values shown in the following table.

Table 147: Gx_Parameters CRD Table

Column Name	Avp Name	Binding/Retriever	Column Type
IMSI	IMSI	Session MSISDN	Input
MSISDN	MSISDN	Session IMSI	Input
Called_Station_Id	Called-Station-Id	Gx APN	Input
3GPP_SGSN_MCC_MNC	3GPP-SGSN-MCC-MNC	Gx MCCMNC Location Based	Input
Location	Location	Gx User Location Information	Input
IP_CAN_Type	IP-CAN-Type	Gx IP CAN Type	Input
RAT_Type	RAT-Type	Gx RAT Type	Input
Online	Online	None	Input
Offline	Offline	None	Input
PCC_Rule_Status	PCC-Rule-Status	None	Input
Rule_Failure_Code	Rule-Failure-Code	None	Input
Gx_Parameters_Group	Gx-Parameters-Group	Not Applicable	Output

c) Configure the Gx Parameters table in the RxRanNasCauseRetry service option as shown in Figure 149: RxRanNasCauseRetry Service Option for Ran_Nas_Cause_Mapping, on page 334.

Step 4 Create the Sy_Parameters CRD table as follows:

a) This table is optional and is used to configure Sy parameters to be used in RAN/NAS retry algorithm. Input is one or more of the following supported **Sy Parameters** and Output is **Sy_Parameters_Group**.

b) Refer to the following table for the list of currently supported input parameters on the Sy interface.

Note Avp Name column is the corresponding AVP name entered by the user in the RxRanNasCauseRetry service option. The AVP name should be same as the Avp Name values shown in the following table.

Table 148: Sy_Parameters CRD Table

Column Name	Avp Name	Binding/Retriever	Column Type
Policy_Counter_Identifier	Policy-Counter-Identifier	None	Input
Policy_Counter_Status	Policy-Counter-Status	None	Input
Command_Code	Command-Code	None	Input
SL_Request_Type	SL-Request-Type	None	Input
Result_Code	Result-Code	None	Input
Sy_Parameters_Group	Sy-Parameters-Group	Not Applicable	Output
Group_Priority	Group-Priority	None	Output

c) Configure the Sy Parameters table in the RxRanNasCauseRetry service option as shown in Figure 149: RxRanNasCauseRetry Service Option for Ran_Nas_Cause_Mapping, on page 334.

Step 5 Create the Ran_Nas_Retry_Mapping CRD table as follows:

a) This is the final table that uses the output values from the above tables.

b) Refer to the following table for its parameters.

Note Avp Name column is the corresponding AVP name entered by the user in the RxRanNasCauseRetry service option. The AVP name should be same as the Avp Name values shown in the following table.

Table 149: Ran_Nas_Retry_Mapping CRD Table

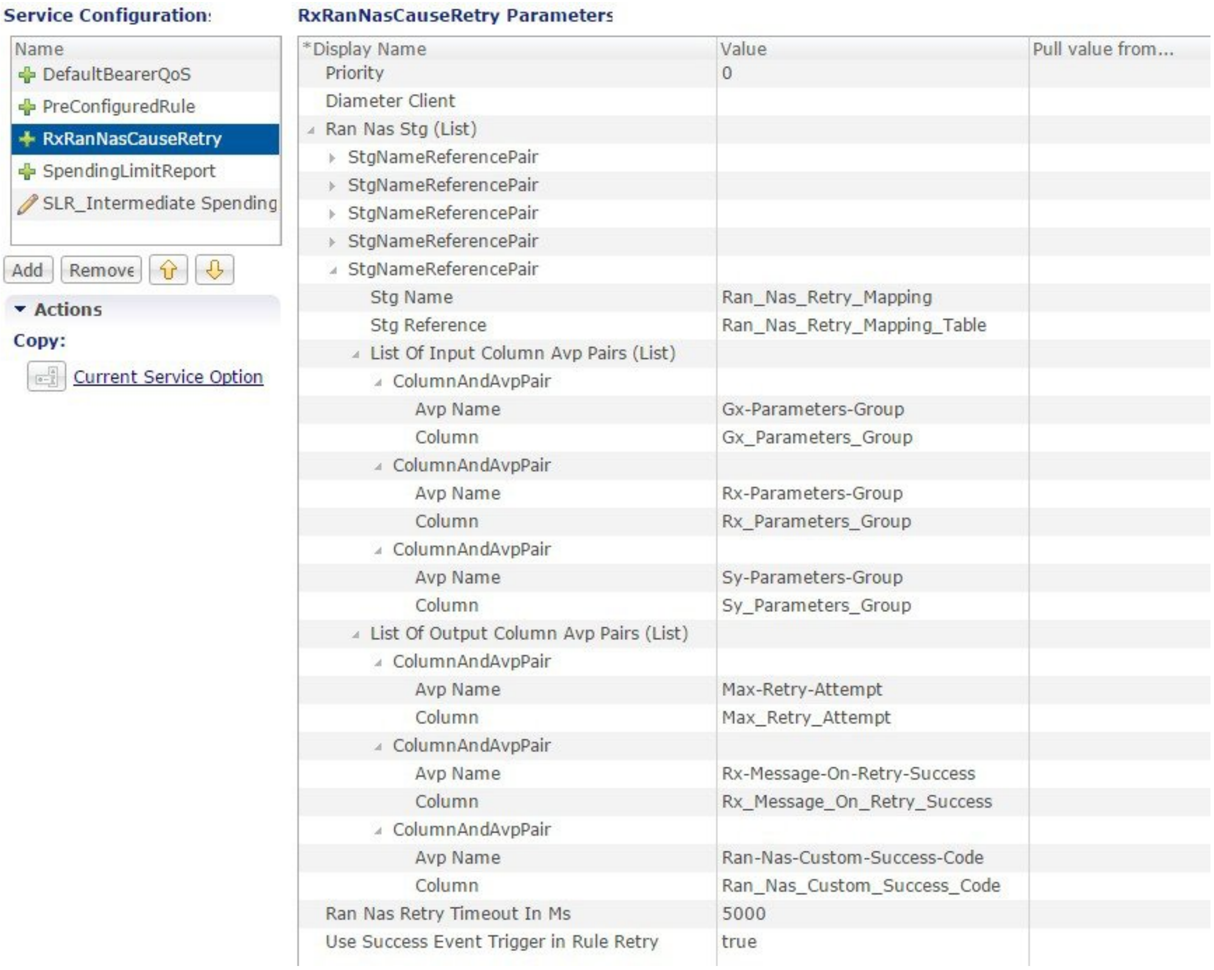
Column Name	Avp Name	Binding/Retriever	Column Type
Gx_Parameters_Group	Gx-Parameters-Group	None	Input
Rx_Parameters_Group	Rx-Parameters-Group	None	Input
Sy_Parameters_Group	Sy-Parameters-Group	None	Input
Max_Retry_Attempt	Max-Retry-Attempt	Not Applicable	Output
Rx_Message_On_Retry_Success	Rx-Message-On-Retry-Success	Not Applicable	Output
Ran_Nas_Custom_Success_Code	Ran-Nas-Custom-Success-Code	Not Applicable	Output

Where,

- Max-Retry-Attempt: Maximum retry attempts to be done before considering it as failure.
- Rx_Message_On_Retry_Success: Decides whether to send Rx RAR on successful retry.
  - If value configured as true: Sends Rx RAR on successful retry with all the RAN/NAS cause codes received so far from the PCEF.
  - If value configured as false: Does not send Rx RAR on successful retry.
- Ran-Nas-Custom-Success-Code: This is one of the spare values in the RAN-NAS-Cause protocol type field. Valid values are 6 to 15. So, to indicate that the Rx RAR is sent for a successful retry, PCRF encodes one RAN-NAS-Release-Cause AVP with this protocol type value. The cause type and cause value should be ignored by the receiver.

c) Configure the Ran_Nas_Retry_Mapping table in the RxRanNasCauseRetry service option.

Figure 150: RxRanNasCauseRetry Service Option for Ran_Nas_Retry_Mapping



Service Configuration:

Name
DefaultBearerQoS
PreConfiguredRule
RxRanNasCauseRetry
SpendingLimitReport
SLR_Intermediate Spending

RxRanNasCauseRetry Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Ran Nas Stg (List)		
StgNameReferencePair		
StgNameReferencePair		
StgNameReferencePair		
StgNameReferencePair		
StgNameReferencePair		
Stg Name	Ran_Nas_Retry_Mapping	
Stg Reference	Ran_Nas_Retry_Mapping_Table	
List Of Input Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Gx-Parameters-Group	
Column	Gx_Parameters_Group	
ColumnAndAvpPair		
Avp Name	Rx-Parameters-Group	
Column	Rx_Parameters_Group	
ColumnAndAvpPair		
Avp Name	Sy-Parameters-Group	
Column	Sy_Parameters_Group	
List Of Output Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Max-Retry-Attempt	
Column	Max_Retry_Attempt	
ColumnAndAvpPair		
Avp Name	Rx-Message-On-Retry-Success	
Column	Rx_Message_On_Retry_Success	
ColumnAndAvpPair		
Avp Name	Ran-Nas-Custom-Success-Code	
Column	Ran_Nas_Custom_Success_Code	
Ran Nas Retry Timeout In Ms	5000	
Use Success Event Trigger in Rule Retry	true	

Support Stale Session for VoLTE

For VoLTE calls, CPS identifies a stale Gx session from the latest Gx session thus allowing CPS to load the latest Gx session and act accordingly. For this, the secondary key mapping stores the primary key in addition to the bucket ID and the site ID, that is, SecondaryKey = <BucketId>; <Site Id>; <Primary Key>.

To enable this feature, add the following parameter in the `/etc/broadhop/qns.conf` file:

```
-Dcache.config.version=1
```

After migration starts, QNS queries with the old format first. If secondary key mapping is not found with the old format, QNS queries with the new format. This leads to increase in query on cache ring during the data migration process. Due to this, there could be some performance impact during the migration process.

Primary keys are stored in the memcache. This increases storage on the memcache. By default, memcache has two GB memory limit. Once memory limit is reached, memcache automatically deletes old records to accommodate new records.

To accommodate more sessions, add more ringsets to distribute data among multiple ringsets.

In case no sessionmgr is available to add a ringset, memory limit can be increased on each sessionmgrs (default two GB) by changing the value of `CACHESIZE` in the `/etc/sysconfig/memcached` file on sessionmgr.

Key storage (memcache) size can be obtained using the following command on sessionmgr:

- Max Limit (in MBs): `echo "stats" | nc sessionmgr01 11211 | grep "STAT limit_maxbytes" | awk '{print $3/1024/1024}'`
- Used (in MBs): `echo "stats" | nc sessionmgr02 11211 | grep "STAT bytes " | awk '{print $3/1024/1024}'`
- Available (in MBs) = Max Limit - Used (in MBs)

Upgrading CPS to use the new mapping format

To upgrade CPS to change the mapping to the new format, do the following:

1. Add the flag `-Dcache.config.version=1` in `/etc/broadhop/qns.conf` file.
2. Copy the file to all VMs.
3. Restart the QNS service.
4. Repeat the above steps for all the sites.
5. Wait for all sites to come up.
6. Add the keys being used for the look up in **Lookaside Keys Prefixes** in **REFERENCE DATA** > **Systems** > ***<Name of Cluster>*** in Policy Builder. See Adding an HA Cluster, on page 28.
7. Run `rebuildAllSkRings` from QNS on one of the sites. This starts the data migration process and changes the mapping to the new format.
8. Once migration is complete, CPS uses the new format.

Restoring CPS to use the old mapping format

To restore CPS to use the old format, that is, disable the feature, do the following:

1. Clear scheduler and ring set in Admin DB. To do this:
   a. Log into the administration database primary member.
   b. Run the following commands in Mongo:

```
 PRIMARY> use scheduler
 PRIMARY> db.tasks.remove({"type":"migrateCache"});
 PRIMARY> use sharding
 PRIMARY> db.versions.update({"_id":"cache_config"},{$set:{"migrationStatus":
"READY"}});
 PRIMARY> db.cache_config.update({},{$unset:{migratingShards:1}},false,true);
 PRIMARY> db.config.update({},{$inc: {version:1}})
```

   c. Run the following commands to verify there is no pending task:

```
 PRIMARY> use scheduler
 PRIMARY> db.tasks.find({"type":"migrateCache"});
```

2. Set `-Dcache.config.version=0` in `/etc/broadhop/qns.conf`. Copy the file to all VMs and restart the QNS service.

3. Repeat Step 2, on page 339 for all the sites.
4. Wait for all sites to come up.
5. Once all sites are up, run `rebuildAllSkRings` from QNS on one of the sites. This starts the data migration process and changes the mapping back to the old format.
6. You can keep checking the status of data migration by running `skRingRebuildStatus`.
7. Once migration is complete, CPS uses the old format.

Dynamic Rule Naming (Multiple Dedicated Bearer QoS)

CPS supports multiple dedicated QoS Bearers (video and audio) within a subscriber's IP-CAN session includes splitting up Gx based RAR messages to provides quality video calls.

When a AAR message is received through the Rx interface with Media-Component-Description a Gx RAR request is sent with the new dynamic PCC rules for initiating new dedicated bearers. Since CPS generates these rules dynamically it automatically generates the rule-name using the following syntax:

```
_<Rx-Linked-Session-Number>_<Media-Component-Number>_<Media-Sub-ComponentFlow-Number>_<Rule-Name>_<Media-Type>
```

The items in this name are:

- Rx-Linked-Session-Number: An internal number that identifies an Rx-session bound to a Gx-session.
- Media-Component-Number: Corresponding AVP value as received in Media-Component-Description Grouped AVP for an AAR message.
- Media-Sub-ComponentFlow-Number: Corresponding AVP value as received in Media-Component-Description->Media-Sub-Component Grouped AVP for an AAR message.
- Rule-Name: A partial name configured in Policy Builder (as derived using AF-Application-Identifier and Media-Type values from 'Custom dynamic rule name' table in Gx Client. Default value “AF”).

for example, “_1_1_1_SIP_AUDIO” “_2_3_1_SIP_VIDEO” and so on.

See Gx Clients, on page 122 for more information on configuring the table in Gx client.

QoS Selection

QoS on dynamic rule (dedicated bearer) created for rx session is derived based upon the algorithm mentioned in section 6.3 of 3GPP 29.213 specification. This algorithm specifies how QoS Class (QCI) Maximum Authorized Data Rates (MBR) Authorized Guaranteed Data Rates (GBR) and Allocation Retention Policy (ARP) are derived based on the media details (Media-Component-Description) send by the AF (IMS).

Table 150: QoS Selection Parameters

Phrase mentioned in Algorithm	Policy Builder section to refer
“as defined by operator specific algorithm”	“RxQosInformation” and “RxAppQosInformation” service configuration.
“AF-Application-Identifier AVP demands application specific data rate”	“Application Qos Policy” defined in Rx Profile

Phrase mentioned in Algorithm	Policy Builder section to refer
“Codec-Data AVP provides Codec information for a codec that is supported by a specific algorithm”	“Codec Qos Policy” defined in Rx Profile

(See Rx Profile, on page 163 for more information on configuration of Rx Profile).

Dynamic QoS

Programmatic CRD (QoS Action)

CPS supports the management of Dedicated Bearer QoS attribute values for Rx IMS application sessions by applying actions QoS-Bounding QoS-Mirroring and QoS-Enforced on Dedicated Bearer QoS calculated as per specification 29.213.

CPS will set the QoS attributes values on the dedicated bearer based on the following QoS actions

- Enforce: This action for any QoS attribute will enforce the values from custom reference data (CRD) table.
- Mirror: This action will copy the QoS attributes values requested by the AF (received in the AAR message).
- Bound: This action will calculate the minimum value between the QoS defined in CRD table and AF requested values or values calculated as per QoS derivation algorithm (29.213).

The following table explains how CPS will derive dedicated bearer QoS-information attributes based on:

- The value received in AAR message (AF requested QoS)
- Value derived from QoS derivation algorithm defined in 29.213
- QoS-Action (Mirror Enforce Bound) and their respective values configured in CRD table

The pattern of the attributes in output column indicates from which input column the value is derived.

QoS-Action Mirror:

Table 151: QoS-Action Mirror

Input			Output
AAR	QoS Derivation Algorithm	CRD Value	
MBR	**MBR**	MBR	*MBR*
	GBR	GBR	*GBR*
	QCI	QCI	*QCI*
	ARP	ARP	*ARP*

QoS-Action Enforce:

Table 152: QoS-Action Enforce

Input			Output
AAR	**QoS Derivation Algorithm**	**CRD Value**	
MBR	MBR	**MBR**	MBR
	GBR	GBR	GBR
	QCI	QCI	QCI
	ARP	ARP	ARP

QoS-Action Bound:

Table 153: QoS-Action Bound

Input			Output
AAR	**QoS Derivation Algorithm**	**CRD Value**	
MBR	MBR	MBR	min(*MBR*, MBR)
	GBR	GBR	min(*GBR*, GBR)
	QCI	QCI	min[8] (*QCI*, QCI)
	ARP	ARP	min(*PL*, PL) and PV, PC based on chosen ARP

[8] As per Bound definition, we still select min value, but min value for QCI translates to max QCI value.

In order to apply the various QoS actions Enforce, Mirror and Bounding CPS needs to provide a new Rx service configuration object which can be applied to subscriber. CPS also supports custom reference data (CRD) tables where for a combination of subscriber and session attributes can be used as an input to derive the output values. These lookup can be performed by using the Input attributes and values as a key and derive a result set of Output attribute and value which can be used to calculate various applicable QoS parameters.

Policy Builder Configuration

Policy builder configuration for this feature requires configuring a CRD table in reference data section and 'RxSTGConfiguration' service configuration object in use case template.

RxSTGConfiguration Service Configuration

For RxSTGConfiguration service configuration parameter descriptions, refer to RxSTGConfiguration, on page 484.

Note The values of "AVP name" must be exact same as per specifications (for example, Media-Component-Number Flow-Number and so on) while defining input columns to RxSTGConfiguration.

Output columns can be defined for one or more of the QoS attributes. When a QoS attribute is added to output, it requires defining two column entries one for QoS action and one for QoS value. The QoS value AVP name needs to be defined as per standard (3GPP TS 29.214) QoS attribute AVP name whereas QoS action AVP name needs to be as mentioned below (for the corresponding QoS attribute):

- Qci
- Max Req Bandwidth U L
- Max Req Bandwidth D L
- Guaranteed Bit Rate U L
- Guaranteed Bit Rate D L
- Priority Level
- Preemption Capability
- Preemption Vulnerability

Similarly, when mapping the output columns for CRD values of Qos-Information attribute use the exact QoS attribute name (for example, "Qos-Class-Identifier" "Max-Requested-Bandwidth-UL" etc.)

Output columns can also be defined for flow-information attributes (Flow Description and Flow Status). When a flow-information attribute is added to output, it requires defining two column entries one for action and the other for value. The value AVP name needs to be defined as per standard (3GPP TS 29.214) attribute AVP name whereas the action AVP name needs to be as mentioned below (for the corresponding flow-information attributes):

- Flow Description
- Flow Status

Similarly when mapping the output columns for CRD values of flow-information attributes use the exact attribute name (for example, " Flow-Description" " Flow-Status".)

Note

- Bound action is not applicable for Flow-Description and Flow-Status.
- CPS does not apply the Actions if the Flow-Status is reported as 'Removed' by AF in the AAR message. CPS does not install the Charging-Rule for the corresponding Media-Sub-Component (or CPS will uninstall it if a Charging-Rule is already installed).
- If the Flow-Status received in AAR is of any value other than 'Removed' and the Action is to Enforce it with value 'Removed', the Charging-Rule for the corresponding Media-Sub-Component is not installed.
- CPS enforces the Flow-Status value as per the CRD configuration and it may override the 3GPP 29.214 specifications. For example, as per 3GPP specifications, RTCP flows are always enabled. If the CRD is configured to enforce Flow-Status with any other value, CPS overrides it with the configured value.
- Gx client 'Rx PCC Rule Flow Direction Behavior' is applicable for Flow-Description derived after applying the Action.

The following steps configure the CRD table for defining the Qos-Action details and Service options details (RxSTGConfiguration) for setting up the service.

Step 1 Log into Policy Builder.

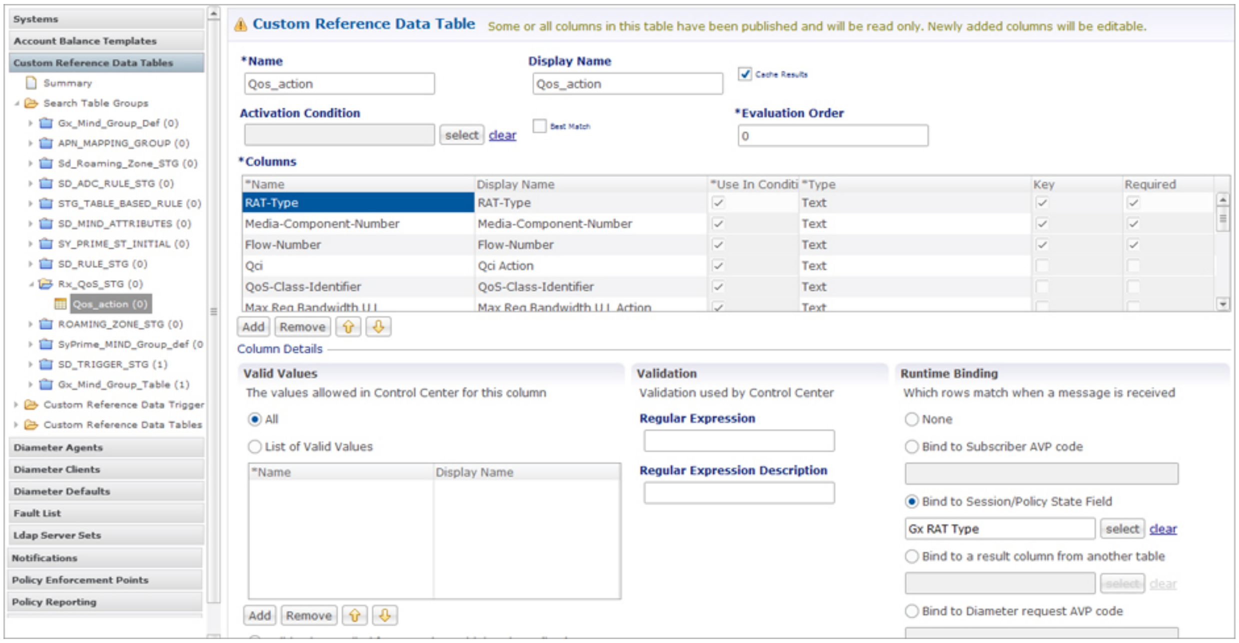
Step 2 Select the **Reference Data** tab.

Step 3 Click **Custom Reference Data Tables** and create a CRD table under Search Table Group as shown in example below.

For more information on how to configure Search Table Groups, see Services, on page 229.

The following example shows three key columns for the CRD table. 'Media-Component-Number' and 'Flow-Number' columns will be mapped to the respective AVPs by setting the respective AVP Names in service-option configuration. Whereas the additional 'RAT-Type' key column is bound to the Gx session attribute.

Figure 151: Custom Reference Data Table



Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

*Name: Qos_action

Display Name: Qos_action

☑ Cache Results

Activation Condition: select clear ☐ Best Match

*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditi	*Type	Key	Required
RAT-Type	RAT-Type	✓	Text	✓	✓
Media-Component-Number	Media-Component-Number	✓	Text	✓	✓
Flow-Number	Flow-Number	✓	Text	✓	✓
Qci	Qci Action	✓	Text	☐	☐
QoS-Class-Identifier	QoS-Class-Identifier	✓	Text	☐	☐
Max Req Bandwidth U L	Max Req Bandwidth U L Action	✓	Text	☐	☐

Add Remove

Column Details

Valid Values
The values allowed in Control Center for this column
● All
○ List of Valid Values

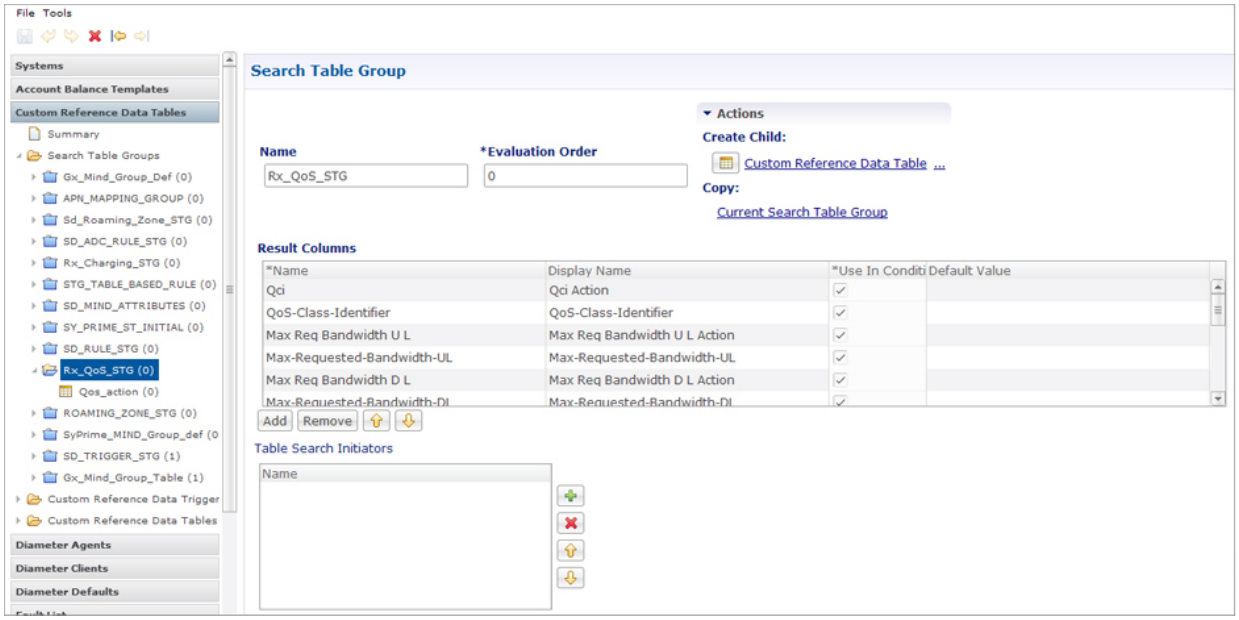
*Name	Display Name

Add Remove

Validation
Validation used by Control Center
Regular Expression:
Regular Expression Description:

Runtime Binding
Which rows match when a message is received
○ None
○ Bind to Subscriber AVP code
● Bind to Session/Policy State Field
Gx RAT Type select clear
○ Bind to a result column from another table
select clear
○ Bind to Diameter request AVP code

Figure 152: Search Table Group



Search Table Group

Name: Rx_QoS_STG

*Evaluation Order: 0

Actions
Create Child:
Custom Reference Data Table ...
Copy:
Current Search Table Group

Result Columns

*Name	Display Name	*Use In Conditi	Default Value
Qci	Qci Action	✓	
QoS-Class-Identifier	QoS-Class-Identifier	✓	
Max Req Bandwidth U L	Max Req Bandwidth U L Action	✓	
Max-Requested-Bandwidth-UL	Max-Requested-Bandwidth-UL	✓	
Max Req Bandwidth D L	Max Req Bandwidth D L Action	✓	
Max-Requested-Bandwidth-DL	Max-Requested-Bandwidth-DL	✓	

Add Remove

Table Search Initiators

Name

Step 4 Go to the **Services** tab.

Step 5 Under **Use Case Templates**, click **Summary** and then create a child Use Case Template.

Step 6 Add a name to the template, for example, `Rx_CRD_QoS`.

Step 7 Click **Actions** tab.

Step 8 Click **Add** in the **Service Configuration** pane and add RxSTGConfiguration service configurations listed under 'rx' section.

Step 9 Go to **Services Options**; the newly created template is available here.

Step 10 Create a child **Service Option** for example, `qos_enhancement`.

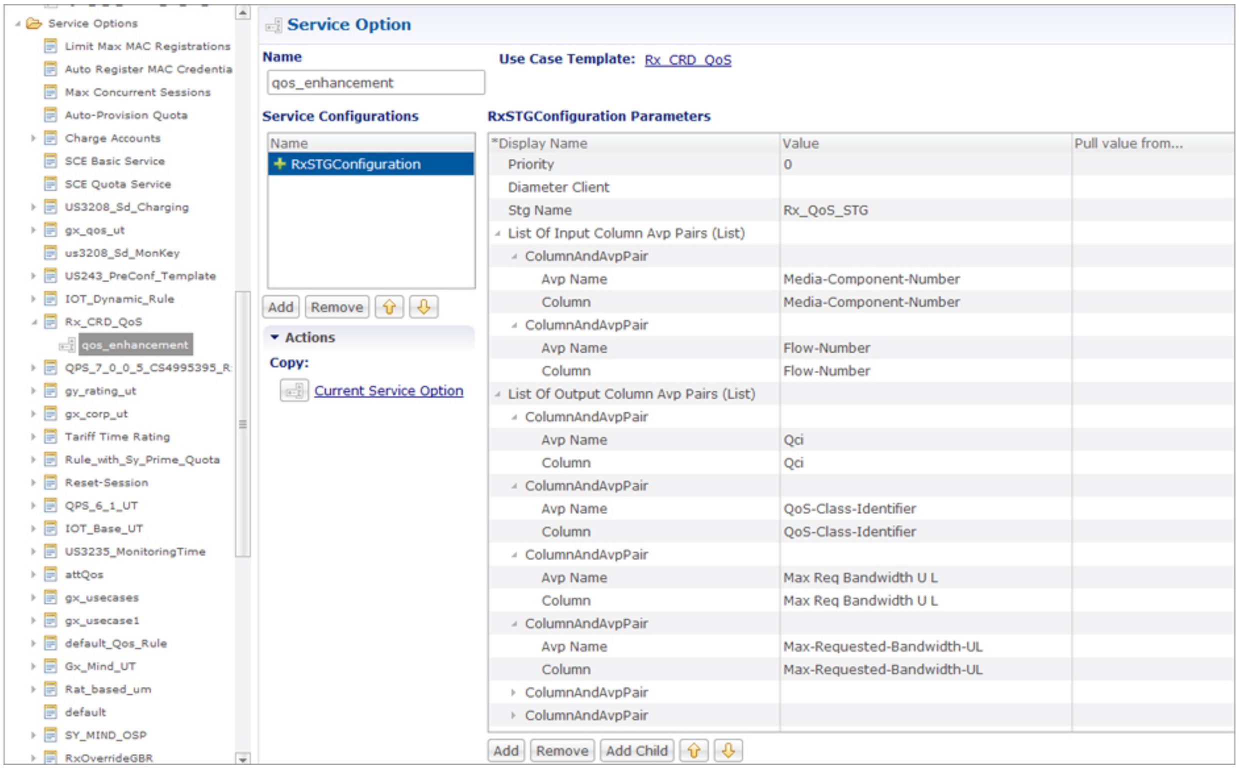
Step 11 Click **OK**. The newly created service options should have the service configuration objects which were added previously at the template level.

Step 12 Select the **RxSTGConfiguration** service configuration and configure it as per the following example:

Refer to the example configuration below that shows 'Media-Component-Number' and 'Flow-Number' Columns in CRD are bound to respective AVP names (received in 'Media-Component-Description' AVP received in AAR message). For output column pairs the sample configuration shows 'Qci' and 'Max Req Bandwidth U L' being mapped to the respective columns in CRD for QoS actions and 'Qos-Class-Identifier' and 'Max-Requested-Bandwidth-UL' columns are mapped to the respective AVPs for CRD values.

Note To add multiple input columns select **List of Input Column AVP Pairs (List)** row and click **Add Child** to create a new ColumnAndAvpPair row to add the input column details. Follow same steps to add output columns in 'List of Output Column Avp Pairs'.

Figure 153: Service Option



Name: qos_enhancement

Use Case Template: Rx_CRD_QoS

Service Configurations

Name
RxSTGConfiguration

RxSTGConfiguration Parameters

*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Stg Name	Rx_QoS_STG	
List Of Input Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Media-Component-Number	
Column	Media-Component-Number	
ColumnAndAvpPair		
Avp Name	Flow-Number	
Column	Flow-Number	
List Of Output Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Qci	
Column	Qci	
ColumnAndAvpPair		
Avp Name	QoS-Class-Identifier	
Column	QoS-Class-Identifier	
ColumnAndAvpPair		
Avp Name	Max Req Bandwidth U L	
Column	Max Req Bandwidth U L	
ColumnAndAvpPair		
Avp Name	Max-Requested-Bandwidth-UL	
Column	Max-Requested-Bandwidth-UL	
ColumnAndAvpPair		
ColumnAndAvpPair		

Step 13 Click **Services** and create a child service, for example, `rx_qos_action`.

Step 14 Update the **Code** and **Name** as `rx_qos_action`.

Step 15 Click **Add** and select the **qos_enhancement** service option created earlier.

Control Center Configuration

Setting up the CRD table in the STG

Step 1 Log into Control Center to define the values for the parameters defined in Custom Reference Data tables.

Step 2 Select the **Configuration** tab.

Step 3 Under **Reference Data**, click **Custom Reference Data Table** to open a dialog box. Select a row and edit the values according to your requirements.

Note Since QoS Action columns have fixed values (“Mirror”, “Bound”, “Enforce”), user can define these values in Valid Values section while defining the column for CRD table.

Logical Operator Support in Programmatic CRD tables for RxSTGConfiguration

CPS users can now configure the CRD table to check if the requested value is present within the range of values present in the CRD tables and fetch the matching records. CRD tables now support Maximum and Minimum columns for each AVP.

For example operator now can configure the CRD table for QoS derivation based on the range of the “Max-Requested-Bandwidth-UL” AVP value (received in AAR message). For this operator create two columns (for example, MBR_UL_Max and MBR_UL_Min) and bind them to the same attribute/AVP. CPS then uses the min and max to check the range.

Note Currently, this functionality is available for RxSTGConfiguration only.

Policy Builder Configuration

Policy Builder configuration for defining ranged columns in RxSTGConfiguration:

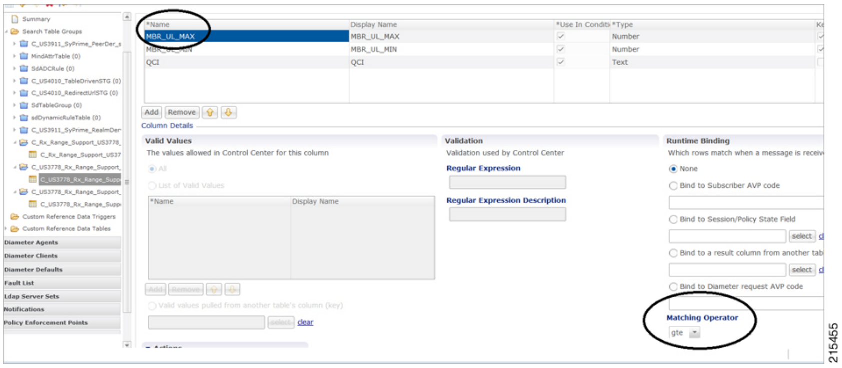
Step 1 Refer to the steps mentioned in Programmatic CRD (QoS Action), on page 341 for creating the CRD table and configuring the RxSTGConfiguration.

Step 2 For the input attribute whose range is to be checked, create two columns for Maximum and Minimum value.

This example creates a CRD table that supports deriving Qci value based on the range of “Max-Requested-Bandwidth-UL” value received in AAR message.

MBR_UL_MAX Column (represents maximum value of MBR_UL in CRD table).

Figure 154: MBR_UL_MAX Input Column



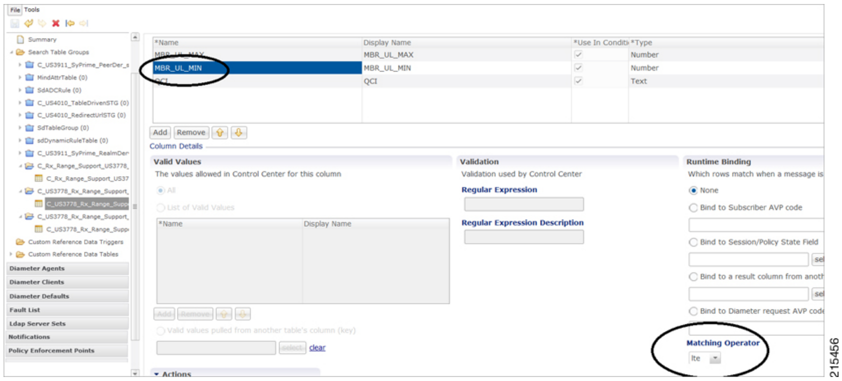
*Name	Display Name	*Use In Conditi	*Type
MBR_UL_MAX	MBR_UL_MAX	✓	Number
MBR_UL_MIN	MBR_UL_MIN	✓	Number
QCI	QCI	✓	Text

Runtime Binding: ● None

Matching Operator: gte

MBR_UL_MIN (represents minimum value of MBR_UL in CRD table).

Figure 155: MBR_UL_MIN Input Column



*Name	Display Name	*Use In Conditi	*Type
MBR_UL_MAX	MBR_UL_MAX	✓	Number
MBR_UL_MIN	MBR_UL_MIN	✓	Number
QCI	QCI	✓	Text

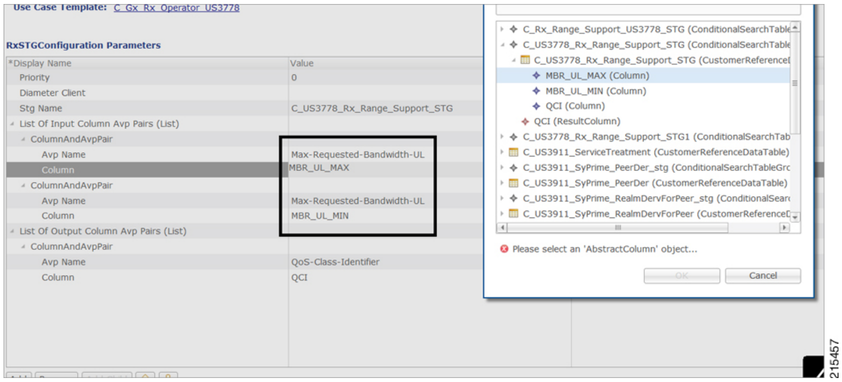
Runtime Binding: ● None

Matching Operator: lte

Make sure that Matching Operator is selected properly i.e for Maximum value column need to select 'gt' or 'gte' and for Minimum value column select 'lt' or 'lte' and QCI column is a result column need to specify that at result column section of STG table.

Step 3 In RxSTGconfiguration, map the corresponding input columns defined above with the same AVP name (Max-Requested-Bandwidth-UL) as shown below:

Figure 156: RxSTGconfiguration Column Parameter



Use Case Template: C_Gx_Rx_Operator_US3778

RxSTGConfiguration Parameters

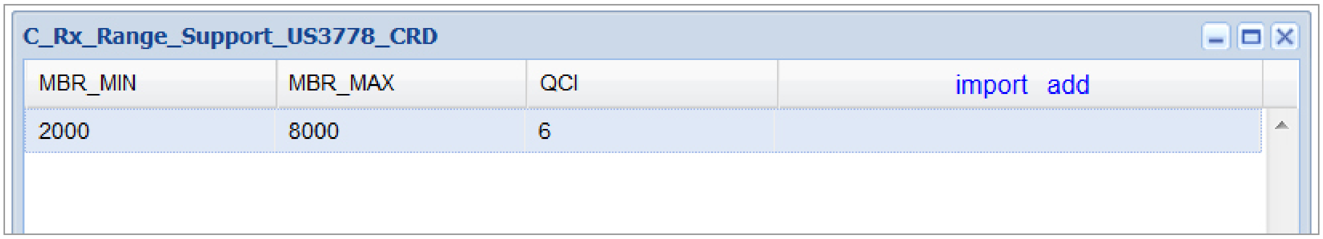
*Display Name	Value
Priority	0
Diameter Client	
Stg Name	C_US3778_Rx_Range_Support_STG
List Of Input Column Avp Pairs (List)	
ColumnAndAvpPair	
Avp Name	Max-Requested-Bandwidth-UL
Column	MBR_UL_MAX
ColumnAndAvpPair	
Avp Name	Max-Requested-Bandwidth-UL
Column	MBR_UL_MIN
List Of Output Column Avp Pairs (List)	
ColumnAndAvpPair	
Avp Name	QoS-Class-Identifier
Column	QCI

- C_Rx_Range_Support_US3778_STG (ConditionalSearchTable
- C_US3778_Rx_Range_Support_STG (ConditionalSearchTable
  - C_US3778_Rx_Range_Support_STG (CustomerReference
    - MBR_UL_MAX (Column)
    - MBR_UL_MIN (Column)
    - QCI (Column)
  - QCI (ResultColumn)
- C_US3778_Rx_Range_Support_STG1 (ConditionalSearchTab
- C_US3911_ServiceTreatment (CustomerReferenceDataTable)
- C_US3911_SyPrime_PeerDer_stg (ConditionalSearchTableGrc
- C_US3911_SyPrime_PeerDer (CustomerReferenceDataTable)
- C_US3911_SyPrime_RealmDervForPeer_stg (ConditionalSearc
- C_US3911_SyPrime_RealmDervForPeer (CustomerReferenceD

Please select an 'AbstractColumn' object...

Step 4 Set Control Center table values as follows:

Figure 157: Setting Control Center Table Values



C_Rx_Range_Support_US3778_CRD

MBR_MIN	MBR_MAX	QCI
2000	8000	6

So with the above configuration, If CPS receives an Rx-AAR message with “Max-Requested-Bandwidth-UL” AVP having value as “4000” then the dynamic rule generated will have Qci value as '6' based on following evaluation:

- 2000 (MBR Min CRD value) < 4000 (Requested value)
- 8000 (MBR Max CRD value) > 4000 (Requested value)

  Fetch the record and give the Result Column value (QCI as 6).

Step 5 Use the same AVP name in the List of Input AVP columns in the service configuration.

Support of Charging Parameters for Dynamic Rules using CRD Tables

CPS supports configurations for setting up the charging parameters on the dedicated bearer created for IMS application sessions (Rx sessions). The charging parameters (like Rating-Group Service-Identifier Metering-Method etc.) can be derived based on certain parameters in the Media-Component-Description AVP received in AAR message (for example, AF-Application-Identifier Flow-Status etc) or any session or SPR attributes. CPS supports configuration of static tables as well as CRD tables to define the criteria for selecting the desired charging parameters on the dynamic PCC rule (dedicated bearer).

CPS will first evaluate the CRD table defined in 'RxChargingParameterSTGConfig' service configuration and if no parameters are derived then CPS will look into the static table defined in 'Dynamic Rule charging parameters' section under Rx-Profile. (See Diameter Configuration, on page 75 for more information.)

CPS also supports a separate configuration for deriving the charging parameters when dedicated bearer is created for sponsored data. CPS will first evaluate the CRD table defined in 'RxSponsoredDataChargingParam' service configuration and if no parameters are derived then CPS will look into the static table defined in 'Sponsored Data Charging Parameter' section under Rx-Profile.

Policy Builder Configuration

Use RxChargingParameterSTGConfig service configuration for setting the charging parameters for dedicated bearers created for IMS session (non-sponsored data case).

RxChargingParameterSTGConfig Service Configuration

The following steps configure the STG for defining the charging parameters details and Service options details (RxChargingParameterSTGConfig) for setting up the service.

Step 1 Log into Policy Builder.

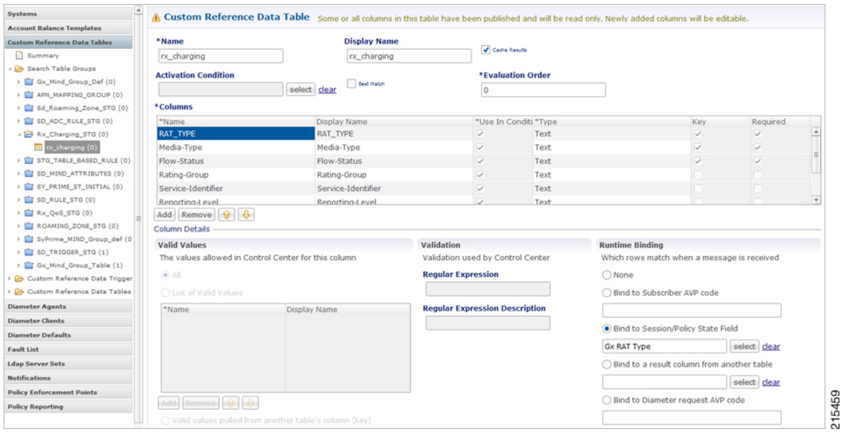
Step 2 Select the **Reference Data** tab.

Step 3 Click **Custom Reference Data Tables** and create a CRD table under **Search Table Group** as shown in the following figures.

For more information on how to configure Search Table Groups, see Services, on page 229.

The following figures show three key columns for the CRD. The Media-Type and Flow-Status columns will be mapped to the respective AVPs from AAR message (by setting the corresponding AVP Names in service-option configuration in Step 10, on page 350). And an additional RAT_Type key column is used, which is bound to the Gx session attribute.

Figure 158: RAT_Type key column



Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

*Name: rx_charging
Display Name: rx_charging
☑ Cache Results
Activation Condition:
□ Best Match
*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditi	*Type	Key	Required
RAT_TYPE	RAT_TYPE	✓	Text	✓	✓
Media-Type	Media-Type	✓	Text	✓	✓
Flow-Status	Flow-Status	✓	Text	✓	✓
Rating-Group	Rating-Group	✓	Text		
Service-Identifier	Service-Identifier	✓	Text		
Reporting-Level	Reporting-Level	✓	Text		

Column Details

Valid Values
The values allowed in Control Center for this column
● All
○ List of Valid Values

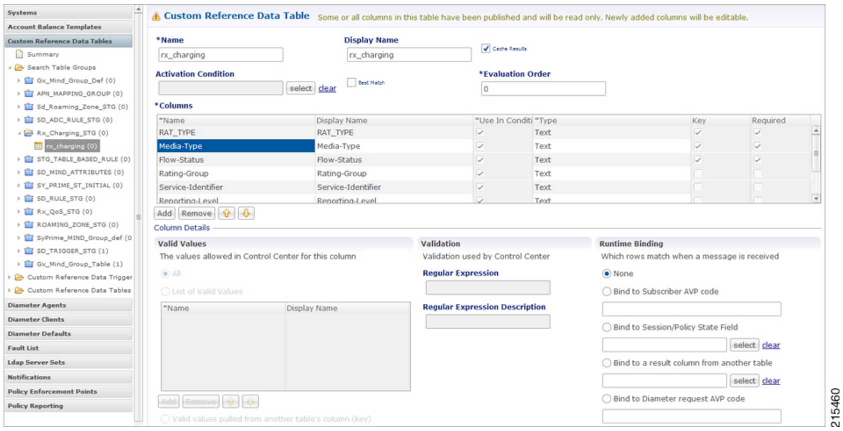
*Name	Display Name

○ Valid values pulled from another table's column (key)

Validation
Validation used by Control Center
Regular Expression:
Regular Expression Description:

Runtime Binding
Which rows match when a message is received
○ None
○ Bind to Subscriber AVP code
● Bind to Session/Policy State Field: Gx RAT Type
○ Bind to a result column from another table
○ Bind to Diameter request AVP code

Figure 159: Media Type key column



Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

*Name: rx_charging
Display Name: rx_charging
☑ Cache Results
Activation Condition:
□ Best Match
*Evaluation Order: 0

*Columns

*Name	Display Name	*Use In Conditi	*Type	Key	Required
RAT_TYPE	RAT_TYPE	✓	Text	✓	✓
Media-Type	Media-Type	✓	Text	✓	✓
Flow-Status	Flow-Status	✓	Text	✓	✓
Rating-Group	Rating-Group	✓	Text		
Service-Identifier	Service-Identifier	✓	Text		
Reporting-Level	Reporting-Level	✓	Text		

Column Details

Valid Values
The values allowed in Control Center for this column
● All
○ List of Valid Values

*Name	Display Name

○ Valid values pulled from another table's column (key)

Validation
Validation used by Control Center
Regular Expression:
Regular Expression Description:

Runtime Binding
Which rows match when a message is received
● None
○ Bind to Subscriber AVP code
○ Bind to Session/Policy State Field
○ Bind to a result column from another table
○ Bind to Diameter request AVP code

Step 4 Select the **Services** tab.

Step 5 Under **Use Case Templates**, click **Summary** and then create a child **Use Case Template**.

Step 6 Add a name to the template, for example, **`Rx_Doc`**.

Step 7 Click **Actions** tab.

Step 8 Click **Add** in the **Service Configuration** pane and add **RxChargingParameterSTGConfig** service configurations listed under 'rx' section.

Step 9 Go to **Services Options**; the newly created template is available here.

Step 10 Create a child **Service Option** for example, **`rx_charging`**.

Step 11 Click **OK**. The newly created service options should have the service configuration objects that were added previously at the template level.

Step 12 Select the **RxChargingParameterSTGConfig** service configuration and configure it as per your requirements.

Note To add multiple input columns, select the **List of Input Column AVP Pairs (List)** row and click **Add Child** to create a new ColumnAndAvpPair row to add the input column details. Follow the same steps to add output columns in List of Output Column Avp Pairs.

Note The values of "AVP name" must be same as per specifications (for example, Media-Component-Number Flow-Number etc.) while defining input columns to RxChargingParameterSTGConfig.

Whereas for output column AVP Pairs in RxChargingParameterSTGConfig while defining the charging parameter attribute use the exact AVP name for charging parameters in Charging-Rule-Definition as per specification. (for example, Rating-Group Service-Identifier etc.)

For parameter descriptions, refer to RxChargingParameterSTGConfiguration, on page 480.

Step 13 Click **Services** and create a child service, for example, `abc`.

Step 14 Update the **Code** and **Name** as `abc`.

Step 15 Click **Add** and select the **abc** service option created earlier.

Control Center Configuration

Setting Up the CRD Table in the STG

Step 1 Log into Control Center to define the values for the parameters defined in Custom Reference Data tables.

Step 2 Select the **Configuration** tab.

Step 3 Under **Reference Data**, click **Custom Reference Data Table** name to open a dialog box.

Step 4 Select a row and edit the values according to your requirements.

A few columns have fixed values (For example, value for Flow-Status column is "ENABLED-UPLINK (0)", "ENABLED-DOWNLINK (1)", "ENABLED (2)", and so on.) So, you can define these values in the Valid Values section while defining the column for the CRD table.

Charging Parameters for Sponsored Data

As explained in the previous section CPS supports defining CRD tables to set the charging parameters on dynamic rules (dedicated bearer) created for IMS session. User can define various inputs to the CRD table to define different evaluation criteria.

In case the dedicated bearer is created for a sponsored data access CPS supports a different service configuration and CRD tables to define the evaluation criteria for selecting charging parameters on dynamic rules. RxSponsoredDataChargingParam is the service configuration defined in CPS to configure the CRD details for setting charging parameters on dedicated bearer created for sponsored data. This service configuration supports defining Sponsor-Identity (provided in Sponsored-Connectivity-Data) as one of the input column in the CRD table created for charging parameters of sponsored-data.

CPS will first evaluate the CRD table defined in 'RxSponsoredDataChargingParam service configuration and if no parameters are derived then CPS will look into the static table defined in 'Sponsored Data charging parameters' section under Rx-Profile. (See Diameter Configuration, on page 75 for more information.)

Policy Builder Configuration

Refer to the policy-builder configuration in Logical Operator Support in Programmatic CRD tables for RxSTGConfiguration, on page 347. Create an extra key column for Sponsor-Identity in the CRD table. Correspondingly, in the service configuration, add an extra input AVP mapping for Sponsor-Identity AVP and its CRD column.

SRVCC

Single Radio Voice Call Continuity (SRVCC) solution seamlessly maintains voice calls as mobile users move from LTE to non-LTE coverage areas. This solution transfers VoLTE calls in progress from LTE to legacy voice networks. Without SRVCC, a VoLTE call on a device moving out of LTE coverage will be dropped.

To support SRVCC solution, CPS support notifying the AF (IMS System) when dynamic rules (created for Rx) on Gx fails because of handover from packet switched (PS) to Circuit Switched (CS).

NPLI (Access Network)

Cisco Policy Suite (CPS) provides Access Network Information (Network Provided Location Information) (for example User Location User Timezone information and so on) Reporting over Gx and Rx Interfaces.

In this feature CPS supports ACCESS_NETWORK_INFO_REPORT Event-Trigger and specific-action on Gx and Rx interface respectively to provide the necessary Access Network Information.

When AF requests the PCRF for access network information the PCRF (CPS) subscribes the requested Access Network Information from the PCEF within the Required-Access-Info AVP which is included in the Charging-Rule-Definition AVP. When the Access Network Information is available the PCEF provides the required Access Network Information to the PCRF within the 3GPP-User-Location-Info AVP or 3GPP-MS-TimeZone AVP or both as requested by the PCRF.

If CPS receives STR with 'Required-Access-Info' AVP then the same will be send in 'Charging-Rule-Remove'. Only in this case STA message will be held till CPS receives CCR-U with access-network-info AVPs (location/timezone).

Note PCEF PCRF and the AF should be compliant with the NetLOC supported feature.

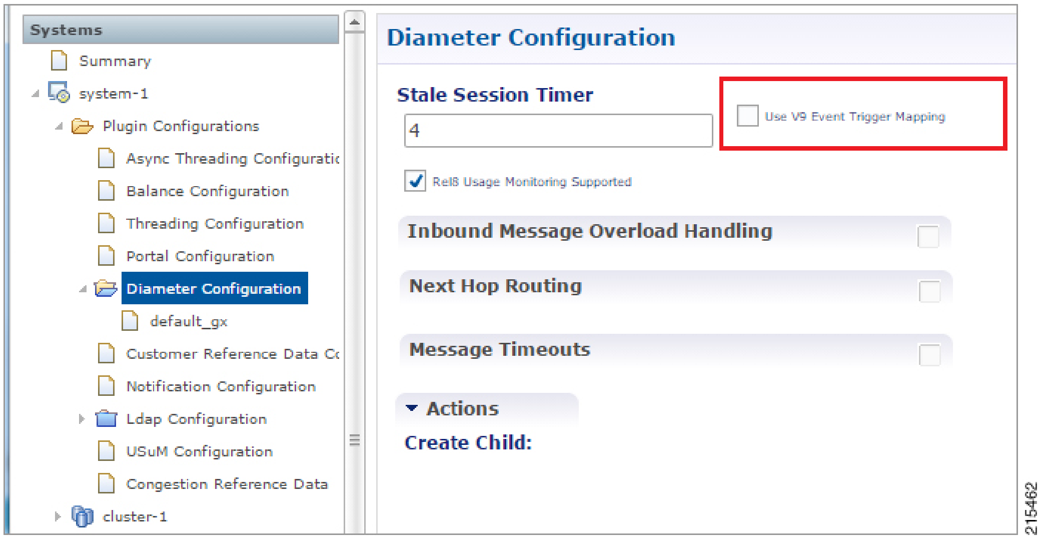
CPS will report NetLoc-Access-Support (0) AVP in AAA and STA message when it gets Required-Access-Info AVP but PCEF does not support NetLoc feature. CPS will report INDICATION_OF_ACCESS_NETWORK_INFO_REPORTING_FAILURE SpecificAction in RAR message when gateway reports NetLoc-Access-Support (0) in CCR-U.

The PCEF provides the following information during an ACCESS_NETWORK_INFO_REPORT event trigger within the Event-Trigger AVP:

- 3GPP-User-Location-Info AVP (If available)
- User-Location-Info-Time AVP (If available)
- 3GPP-SGSN-MCC-MNC AVP (If the location information is not available) or 3GPP-MS-TimeZone AVP or both.

Note The Gx Event-Trigger used in this feature is specific to 3GPP R11 specification. Make sure the CPS is not configured to use V9 Event-Triggers.

Figure 160: Diameter Configuration



Stale Session Timer: 4

□ Use V9 Event Trigger Mapping

☑ Rel8 Usage Monitoring Supported

To enable NetLoc support:

- NetLoc flag must be enabled on both Gx and Rx sessions.
- For Gx CCR(I) and CCA(I) should have Supported-Features Group AVP with Feature-List and feature bit 10 enabled.
- For Rx initial AAR should have Supported-Features Group AVP with Feature-List feature bit 5 enabled.

See Diameter Configuration, on page 75 for more information on configuring the parameters.

Dynamic PCC (MOG)

CPS supports the creation and modification of default and dedicated bearers based on attributes received from MOG over the Rx prime interface.

Default Bearer

Default bearer characteristics can be dynamically modified to support higher bit rates in run time. This is an opt-in service and allows the user to request and update (boost/throttle) in QoS on demand.

To support this functionality CPS can boost/throttle the QoS values on Default Bearer based on a trigger from the AF/MOG on the Rx prime interface. MOG initiates an Rx session with CPS as an AF to establish an Rx session by sending an AAR.

CPS parses the AAR to look for Dynamic-PCC-requested-QoS custom AVP that has the QoS values and additionally Priority and Intention values as well.

Intention values are Boost and Throttle.

- In case of boost, CPS checks if the requested QoS values (either from the AAR message or derived values from the CRD table) are higher than existing. It then uplifts the bearer. If the requested QoS values are lower than existing, CPS does not uplift the bearer.
- In case of throttle, CPS checks if the requested QoS values (either from the AAR message or derived values from the CRD table) are lower than existing. It then downgrades the bearer. If the requested values are higher than existing, CPS ignores the request.

CPS makes sure that if the uplift/downgrade of QoS attributes results in the default bearer having QCI and ARP same as any existing dedicated bearer then those rules and flows are installed on the default bearer associated with the existing dedicated bearer. That is, the dedicated bearer is removed when its QCI and ARP match the default bearer. With the removal of the dedicated bearer, all the flows and rules associated with this bearer are also removed.

QoS attributes are also derived from the CRD evaluation if the corresponding action defined in the RxSTGDefaultBearerConfiguration table for the QoS attributes is "Enforce". For the RxSTGDefaultBearerConfiguration service option parameters, see RxSTGDefaultBearerConfiguration, on page 490.

It is possible that there are multiple Rx (IMS) sessions for a single Gx session and each Rx session may influence the QoS values by sending the Dynamic-PCC-requested-QoS AVP. CPS takes into consideration the 'Priority' 'Intent' 'MOG/AF requested QoS' and 'calculated QoS' for deriving the values for modified default bearer QoS.

Dedicated Bearer

AAR message having Media-Type AVP in Media-Component-Description AVP and Service-Info-Status AVP set to value FINAL_SERVICE_INFO(0) indicates the creation of a dedicated bearer over the Rx prime interface. If Service-Info-Status AVP is not present, the Dedicated-Bearer-QoS AVP can also result in creation of the dedicated bearer.

CPS also uses the Media-Type AVP value received in the AAR message to spawn the dedicated bearer.

QoS attributes are also derived from the CRD evaluation. The default action defined in the RxSTGConfiguration table for the QoS attributes is "Enforce".

In case of multi-value QCI Media-Type, the QCI value is obtained through the Dynamic-Requested-PCC-QoS AVP.

Policy Builder Configuration

RxSTGDefaultBearerConfiguration service configuration is used for CRD evaluation of Default bearer QoS on receiving Rx AAR with Dynamic-PCC-Requested-QoS AVP. For more information on the RxSTGDefaultBearerConfiguration service option parameters, see RxSTGDefaultBearerConfiguration, on page 490.

ModifyChargingRules service configuration is used to modify the default bearer charging rule AVPs based on TDF-Application Identifier, QoS-Class-Identifier, Sponsor-Identity, and Application-Service-Provider-Identity of already installed charging rule. For more information on the ModifyChargingRules service option parameters, see ModifyChargingRules, on page 444.

In the ActionOnDefaultBearerQoSChange service configuration, if CollapseDedicatedBearer value is set to true then CPS makes sure that if the uplift or downgrade of QoS attributes results in the default bearer having QCI and ARP same as any existing dedicated bearer then it installs those rules and flows on the default bearer associated with the existing dedicated bearer. This is due to the fact that PCEF removes the dedicated bearer when QCI and ARP matches with the default bearer. With the removal of the dedicated bearer all the flows and rules associated with that bearers are removed. For more information on the ActionOnDefaultBearerQoSChange service option parameters, see ActionOnDefaultBearerQoSChange, on page 424.

When there are multiple Rx sessions with dynamic PCC requests having same priority, CPS by default selects the QoS values from the BOOST request. CPS provides a configuration flag in 'Gx Client' for overriding the default behavior of 'BOOST' with 'THROTTLE'. So:

- If the check box (Override Boost with Throttle for Similar Priority) is checked, then throttle request takes precedence over boost request.
- If the check box is unchecked, then throttle takes precedence over boost.

See Diameter Configuration, on page 75 for more information.

VoLTE Emergency Calls

VoLTE Emergency Calls can be processed only if the Rx session is linked to a Gx session which has a default bearer established towards an emergency APN. See Rx Clients, on page 138 for more information on configuring VoLTE emergency details in Rx Client.

For an emergency call Service-URN is used instead of AF Application ID and thus can be configured using all options where AF-Application-ID is used. Refer to option Override AF App Id with URN for Emergency sessions in the parameters table under Rx Clients, on page 138. The AF may include the Service-URN AVP in order to indicate that the new AF session relates to emergency traffic. If the CPS receives the Service-URN AVP indicating an emergency session then CPS can prioritizing service flows relating to the new AF session.

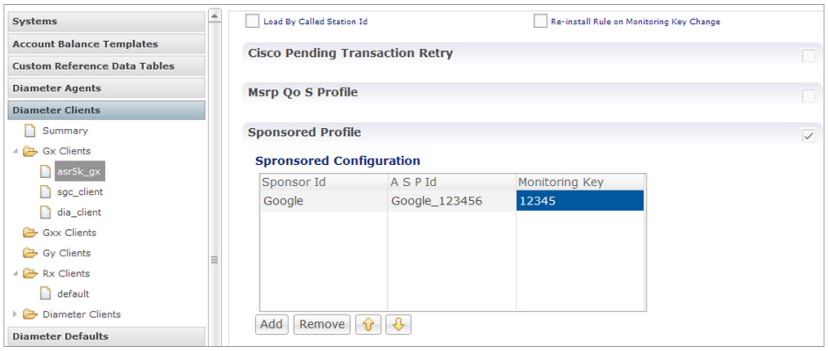
Sponsored Data

CPS supports 'Sponsored Connectivity Data' over Rx interface (IMS session). Sponsored data connectivity is supported by CPS based on service data flows associated with one or more PCC rules if the information about the sponsor the application service provider and optionally the threshold values are provided by the AF. When CPS receives the flow based usage thresholds from the AF then it uses the sponsor identity to generate a monitoring key.

Operator can override the Monitoring-Key generated by CPS by specifying the desired monitoring-keys in 'Sponsored Profile' table under Gx Client in 'Reference Data' section. Key to this table are the 'Sponsored-Id' and 'Application-Service-Provider-Identifier' AVP values received from the AF.

An example configuration is given below:

Figure 161: Sponsored Configuration



□ Load By Called Station Id   □ Re-install Rule on Monitoring Key Change

Cisco Pending Transaction Retry □

Msrp Qo S Profile □

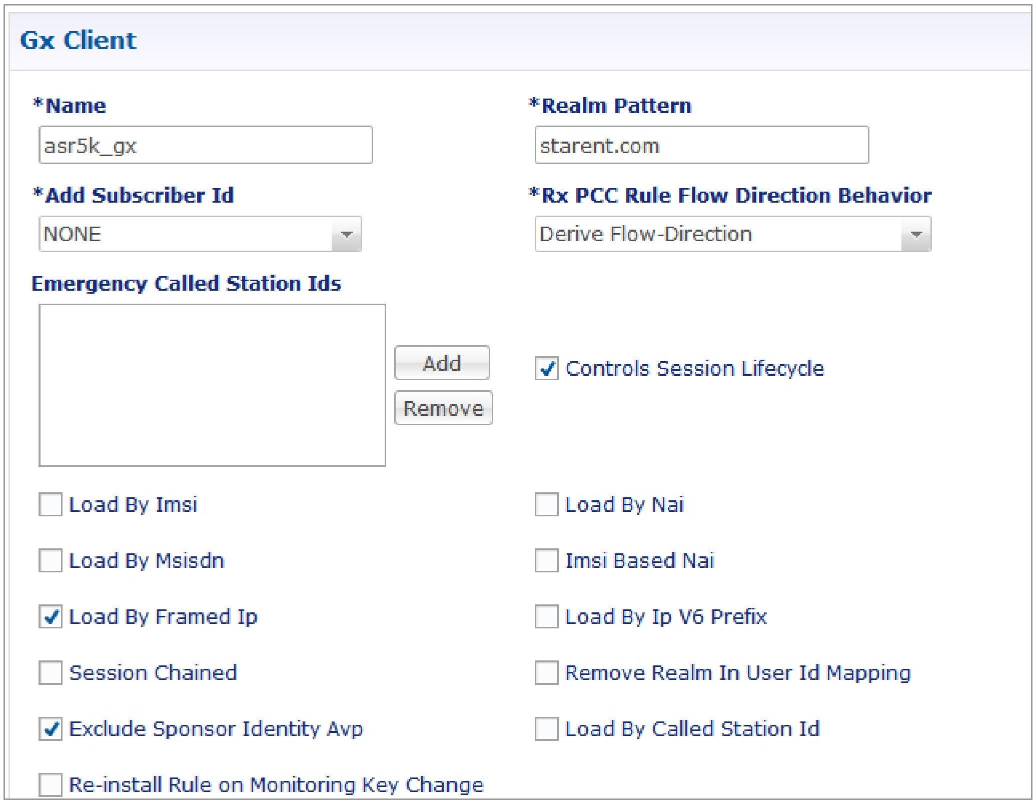
Sponsored Profile ☑

Spronsored Configuration

Sponsor Id	A S P Id	Monitoring Key
Google	Google_123456	12345

CPS also supports suppressing the 'Sponsor-Identity' AVP from PCC rules generated for Sponsored Data. This configuration is required when the PCEF does not support 'Sponsor-Identity' AVP. In this case if CPS requests a PCEF to create a dedicated bearer with Sponsor-Identity then the PCEF may reject the request because it does not support the Sponsor-Identity AVP. So by selecting the check box shown below CPS can exclude the Sponsor-Identity AVP from the PCC rule definition. (By default the value is unchecked).

Figure 162: Excluding Sponsor-Identity AVP



Gx Client

*Name: asr5k_gx

*Realm Pattern: starent.com

*Add Subscriber Id: NONE

*Rx PCC Rule Flow Direction Behavior: Derive Flow-Direction

Emergency Called Station Ids

☑ Controls Session Lifecycle

□ Load By Imsi   □ Load By Nai

□ Load By Msisdn   □ Imsi Based Nai

☑ Load By Framed Ip   □ Load By Ip V6 Prefix

□ Session Chained   □ Remove Realm In User Id Mapping

☑ Exclude Sponsor Identity Avp   □ Load By Called Station Id

□ Re-install Rule on Monitoring Key Change

See Gx Clients, on page 122 for more information on configuring Gx Client.

Multi-Media Priority Services

Cisco Policy Suite provides Enhanced Multi-Media Priority Services (eMPS) for priority subscribers. CPS also prioritizes VoLTE/IMS calls for priority subscribers. CPS provides the ability to determine priority subscribers and provide priority services. There are two types of MPS:

- Always-on: For a user with always-on MPS subscription, priority treatment is provided for all PS sessions.
- On-demand: On-demand MPS is applied when priority treatment is explicitly requested by user with specific access code (MPS-Identifier).

This feature is configured through:

- Always On
  - Gx Service Configuration, on page 357
  - Reference Data for Always-on MPS Priority, on page 358
- On Demand
  - On-demand MPS-Identifier, on page 359
  - Obtaining Highest Priority Qci Using Max Function, on page 359

Gx Service Configuration

EMPS Service Configuration

CPS provides a service configuration ('EMPS' under 'gx' service configuration) for defining the MPS EPS Priority MPS Priority Level and IMS Signaling Priority level. This is required for Always on MPS.

When a user configured with MPS subscription initiates a session the priority level from the subscription data QCI Preemption Capability and Preemption Vulnerability from MPS profile are used to set default bearer QoS. Also all preconfigured dynamic rules are updated to use the new priority level.

When the session is initiated from IMS APN the IMS Signaling Priority is used as priority level if configured under subscription data.

Table 154: EMPS Service Configuration Parameters

Parameter	Description
Mps Eps Priority Enabled	Field to invoke Priority EPS Service. • 1 enable • 0 disable
Mps Priority Level	Indicates the priority level (Integer range 1-15).
IMS Signaling Priority	IMS signaling priority level (Integer range 1-15).

The following are the steps to configure this service configuration:

Step 1 Log into Policy Builder.

Step 2 Select the **Services** tab.

Step 3 Under **Use Case Templates**, click **Summary** and then create a child **Use Case Template**.

Step 4 Add a **Name** to the template, for example, `IMS_usecase`.

Step 5 Select **Actions** tab.

Step 6 Click **Add** in the **Service Configuration** pane and add EMPS service configurations listed under 'gx' section.

Step 7 Go to **Services Options**; the newly created template would be available here.

Step 8 Create a child **Service Option** for example, `eMPS`.

Step 9 Click **OK**. The newly created service options should have the service configuration objects which were added previously at the template level.

Step 10 Select the **EMPS** service configuration and configure it as per your requirements.

Reference Data for Always-on MPS Priority

In the Policy Builder's Reference Data, a new profile Mps Profiles is added under Diameter Defaults to support eMPS priority. The MPS Profile provides MPS attributes required for priority service provisioning. The priority level value from Service configuration takes precedence over MPS Profile value.

Step 1 Log into Policy Builder.

Step 2 Select the **Reference Data** tab.

Step 3 Select **Diameter Defaults** > **Mps Profiles**.

Step 4 In the summary window, click **Mps Profile** to create an Mps Profile.

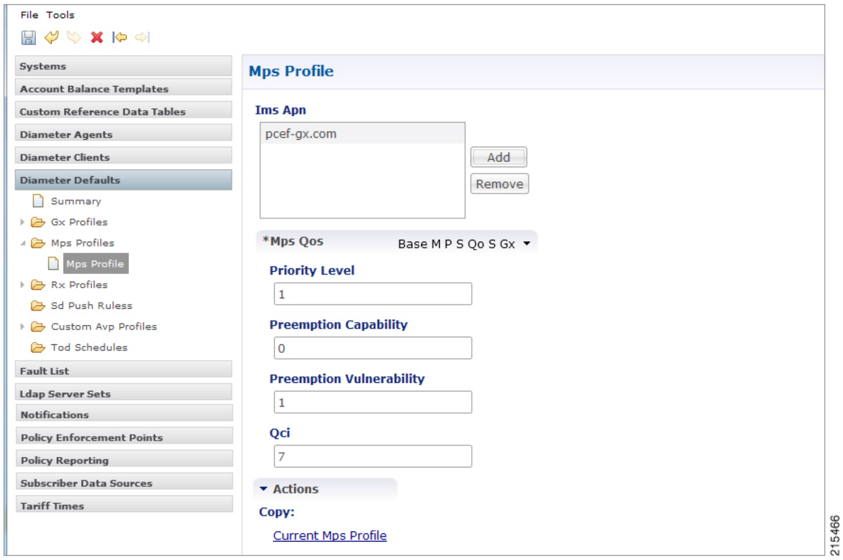
Step 5 To add an Ims Apn, click **Add**, enter the Ims Apn in the field provided and click **OK**.

This field can accommodate several Ims Apn that are used to match with the incoming service request for priority service. The values that are received by the Default Bearer QoS are looked up for a suitable Ims Apn match. If the APN value of a Gx session request matches IMS APN, IMS signaling priority from EMPS service is used as priority level.

Step 6 Assign values for Always-on MPS attributes in the MPS QoS section.

An example is given below.

Figure 163: MPS Profile Configuration



Mps Profile

Ims Apn

pcef-gx.com

*Mps Qos: Base M P S Qo S Gx

Priority Level: 1

Preemption Capability: 0

Preemption Vulnerability: 1

Qci: 7

For information on the parameters mentioned above, see MPS Profile, on page 162.

On receiving a request, the Ims Apn is checked up for a match, if there is suitable match then the values assigned in the Mps Qos section CPS selects the IMS signaling priority from EMPS service.

On-demand MPS-Identifier

The section, Reference Data > Diameter Defaults > Rx Profiles has a new table to support Rx initiated sessions. When an Rx session is initiated with an MPS-Identifier, the incoming message is mapped with input parameters such as MPS Id and Media Type, and the session is processed further. MPS QoS Policy table is the newly added table to the Rx Profiles in the Policy Builder.

The incoming message is mapped with the input parameters, which are MPS Id and Media Type, if the parameters match the corresponding value from the other columns - Priority Level, Preemption Capability, Preemption Vulnerability and Qci, are provided to provide the necessary service. For more information, see Rx Profile, on page 163.

Obtaining Highest Priority Qci Using Max Function

When an EPS subscription for a subscriber is configured to be always-on, and an Rx session is initiated with MPS-ID, the higher priority level and higher QCI is derived and applied to the default EPS. ARP of the Rx dynamic rule is derived from Reservation priority if present in the AAR, otherwise defaulted to the value in configuration.

The Max function uses the following precedence order to derive the QCI values:

2 > 1 > 4 > 3 > 5 > 6 > 7 > 8 > 9

For additional information refer to 3GPP spec 29.213 (R11).

When there are multiple Rx sessions, the default bearer and default EPS bearer QoS is updated with the highest value of QCI, ARP.

- The highest value is derived from the Rx sessions and Default Bearer if subscribed to always-on MPS.
- The highest value is derived from the Rx session if not subscribed to always-on MPS.

Rx session termination: When a Rx session terminates, and if it is the last Rx session to terminate, the default bearer and default EPS bearer QCI/ARP is reverted to:

- Single Rx session with MPS: revert Default Bearer to normal or always-on Qci or ARP.
- Multiple Rx sessions with different MPS: revert default bearer to highest Qci or ARP among the remaining Rx sessions.

There are two main scenarios that take place during an Rx Session:

- On Demand without Always-on Configuration
- On Demand with Always-on Configuration

On Demand Without Always-on Configuration

Default Bearer

- When multiple Rx sessions are initiated with MPS-ID, the highest priority level and highest QCI is derived and applied to the default EPS.
- If reservation priority is not present in AAR, the priority configured for the particular MPS-ID is used. In the Rx profile > MPS Qos Policy table, a blank value is defined in the Media Type column, which applies to the Default Bearer. If the configuration is missing, default reservation priority (0) is used.

The new Priority Level and Qci are applied to the Default Bearer QoS and also to the Gx pre-configured rules.

Dedicated Bearer

Priority Level of the Rx dynamic rule is derived from Reservation priority if present in the AAR from the media component description; otherwise the default value in the configuration is used. QCI of Rx dynamic rule is derived from the Rx profile configuration. Preemption Capability and Preemption Vulnerability are determined from Rx profile for each MPS-Id.

On Demand With Always-On Configuration

Default Bearer

When an Rx session request is received with an MPS-ID along with message level (AAR) reservation-priority:

- The ARP priority level is derived from the highest value between reservation priority and always-on priority (or IMS priority if applicable).
- The value of QCI is derived from the highest value between MPS-ID specific Qci and always-on Qci. When multiple Rx sessions are created with MPS-ID and message level (AAR) reservation priority.
- The ARP Priority Level is derived from highest value between session level reservation-priority (among active sessions) and always-on priority (or IMS priority if applicable).

- The value of Qci is derived from the highest value between MPS-ID specific Qci and always-on Qci.

In both cases, if reservation priority is not present in the AAR, the priority configured for each MPS-Id is used. In the Rx profile > MPS Qos Policy table, a blank value is defined for the Media Type column, which applies to the Default Bearer. If the configuration is missing, default reservation priority (0) is used.

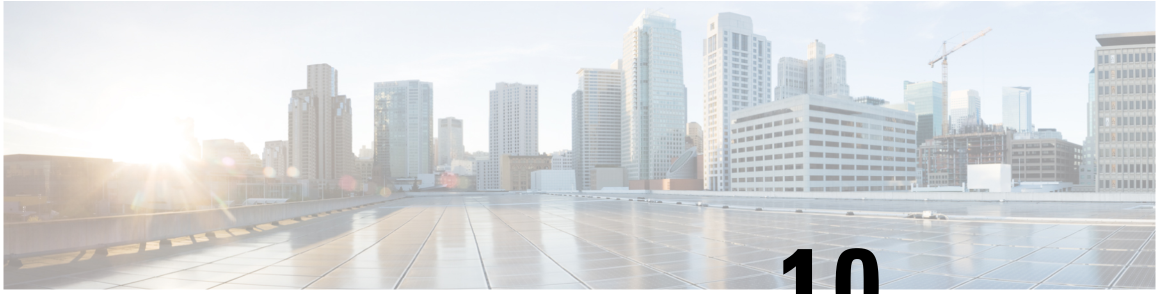
The new Priority Level and Qci is applied to the Default Bearer QoS and also to the Gx pre-configured rules.

Dedicated Bearer

Priority Level of the Rx dynamic rules is derived from the highest value between always-on MPS and the reservation priority, if the reservation priority is defined in the AAR Media component description.

If the reservation priority is not present in Media-Component-Description, the value of reservation priority is derived from the highest value between always-on MPS and from the Rx Profile configuration (based on MPS-ID and Media Type).

Preemption Capability and Preemption Vulnerability are determined from Rx profile for each MPS-Id and Media Type. QCI value is derived from the higher value between MPS profile and Rx MPS profile (based on Media Type and MPS-ID).



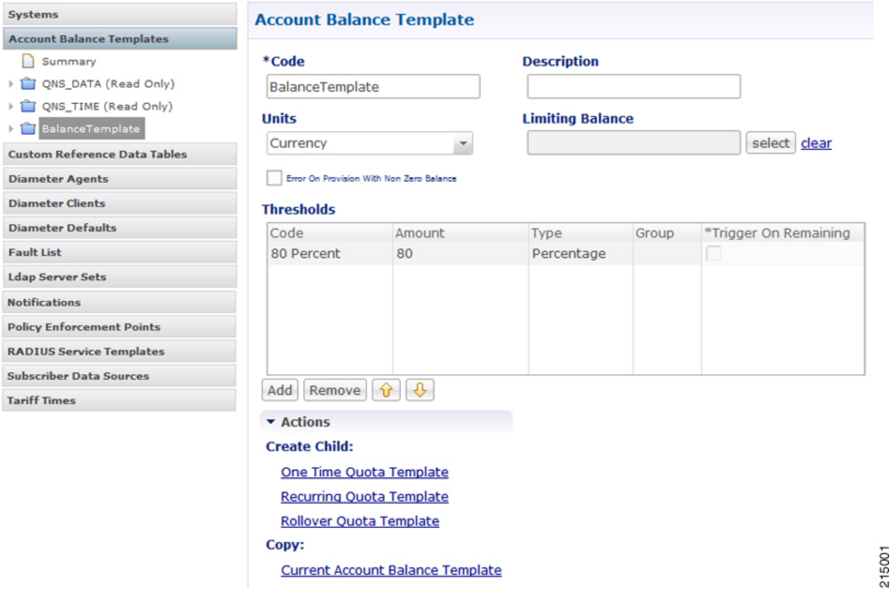
CHAPTER 10

Balance Services

Account Balance Templates

Account Balance templates provide the overall structure to the data provisioned to a given subscriber.

Figure 164: Account Balance Template



Systems
Account Balance Templates
Summary
QNS_DATA (Read Only)
QNS_TIME (Read Only)
BalanceTemplate
Custom Reference Data Tables
Diameter Agents
Diameter Clients
Diameter Defaults
Fault List
Ldap Server Sets
Notifications
Policy Enforcement Points
RADIUS Service Templates
Subscriber Data Sources
Tariff Times

Account Balance Template

*Code: BalanceTemplate

Description:

Units: Currency

Limiting Balance: select clear

□ Error On Provision With Non Zero Balance

Thresholds

Code	Amount	Type	Group	*Trigger On Remaining
80 Percent	80	Percentage		□

Add Remove ⇧ ⇩

▾ Actions

Create Child:

One Time Quota Template
Recurring Quota Template
Rollover Quota Template

Copy:

Current Account Balance Template

The following parameters can be configured under Account Balance Template:

Table 155: Account Balance Template Parameters

Parameters	Description
Code	Required unique name for the template.
Description	Optional field to contain a brief description of the template's use case.
Units	The choice of units determines functionality options within the system. For example, Time units such as seconds or minutes will cause the system to behave differently than Data units like Bytes or Megabytes. Additionally, currency is an option and can be used to account for usage credit in a direct manner. **Note** Balance does not do any type of currency exchange rate calculation. The values are stored as is and represent whatever currency the SP and their subscribers commonly use. Default value is Bytes.
Limiting Balance	Limiting Balance refers to a Balance template that is used by a shared balance template. This establishes a link from the shared balance to a “limit” balance, so that Balance Manager knows which two balance codes it needs to reserve/charge against in the shared per user limit use case. **Note** The limiting MsBM account must be the MsBM account tied to the individual subscriber's credential. The limiting MsBM balance and quota must be provisioned in separate Balance/MsBM operation from the provisioning of the shared account, balance, and quota.
Error on Provision With Non Zero Balance	If a provisioning request is made (specifically any request that credits or provisions a subscriber balance) when there is remaining balance, i.e. non-zero amount, then the Balance module throws an error and does not provision the quota. Default value is False (unchecked).
Thresholds	
Code	Unique name for the threshold object.
Amount	An integer representing the amount of quota that will trigger the threshold notification.
Type	Unit of calculation like Percentage or Bytes.
Group	Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.
Trigger on Remaining	This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.

CRD Based Account Balance Templates

CRD balance table definitions are pre-shipped (read only) as part of the Policy Builder configuration. For this, the "CRD Balance" feature (`com.broadhop.balance.crdbalance.feature`) needs to be installed. Enable this functionality by selecting the **Enable Crd Balance Template Lookups** check box. For more information, see Balance Configuration, on page 49.

The following required tables include result columns that directly map to the corresponding fields in Balance and Quota Templates. For more information on individual field description, see Account Balance Templates, on page 363.

- q_account_balance: Top Level Account Balance Template fields
- q_one_time_quota: One Time Quota Template definition
- q_recurring_quota: Recurring Quota Template definition
- q_rollover_quota: Rollover Quota Template definition
- q_threshold_definition: Threshold definitions
- q_threshold_balance_association: Balance to threshold association
- q_threshold_quota_association: Quota to threshold association

Threshold Priorities and Groups

Thresholds defined in Policy Builder (under Balance and Quota templates) have implicit top to down priority incase threshold group is defined. Same functionality is achieved using 'priority' column in `q_threshold_definition` table. Internally, thresholds defined in CRD are prioritized based on provided 'priority' column value. Higher the value, higher the priority (that is, higher in the Policy Builder list). Priority value has no effect if thresholds are not grouped.

Quota Templates

Quota templates define the specifics of how quota behaves. There are 3 basic types of quota: One Time, Recurring, and Rollover. Within that there are additional behavioral functions like BillCycle and Stackable, but those are just modifications to one of the three basic types.

Recurring

Recurring quota is refreshed periodically with a specific amount each refresh. It defaults to infinite duration meaning that it continues until the account is deleted from the system. However, it is possible to limit the duration of a recurring quota using the Recurrence Limit field. The most common time period is Monthly. Time periods defined in hours, days, weeks, months are possible. Initial credit and refreshed amounts by default expire at the end of the current time period.

The following parameters can be configured under Recurring Quota Templates:

Table 156: Recurring Quota Templates Parameters

Parameters	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.
Amount	A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration. **Note** • The upper limit on the amount is 1 Exabyte. • Future amount changes can be accomplished with the Credit API.
Priority	Priority ranks the template so when the Balance module is determining the next credit to use for reservations and debits, the template with the highest rank (Positive number Integer) wins. 1 is the highest rank. The default of no value is lowest priority. After priority, the most recent end date (Next to Expire) is used to determine the next credit. Default value is null.
Recurrence Frequency Amount	Integer used in conjunction with the Recurrence Frequency to determine the refresh period. Default value is 1. **Note** Recurrence Frequency Amount range must be between 1 – 12 when the Recurrence Frequency is configured as **Bill Cycle**. CPS takes the default value **1** when Recurrence Frequency is not configured.
Recurrence Frequency	Value used in conjunction with the Recurrence Frequency Amount to determine the refresh period. You can select the value from the drop-down list based on your requirements. The following values are supported: • Bill Cycle : Refresh interval is based on bill cycle day for each quota independently. • Day(s): Refresh interval is based on day(s). • Hour(s): Refresh interval is based on hour(s). • Minute(s): Refresh interval is based on minute(s). • Month(s): Refresh interval is based on month(s). • Week(s): Refresh interval is based on week(s). Default value is Month(s).

Parameters	Description
Rollover Quota	A Rollover Quota Template that this recurring quota rollovers unused quota to when the quota refreshes for the next recurrence period.
Calendar Type	MsBM supports both the Gregorian and Hijra calendar. The Hijri calendar is the Islamic calendar which is a moon-phase based calendar. Cisco has several customers in the Middle East who use the Hijri calendar instead of the Gregorian calendar to determine refresh dates. **Note** The data is still stored in the database as Gregorian dates, but the Balance module translates those to Hijri for any processing. SPR and the Unified API do not support Hijri dates. Default value is Gregorian.
Recurrence Limit	Integer that determines the duration for a recurring quota. When set to 0, the duration is infinite. When set to any positive number, the quota refreshes that number of times and then stop. For example, if the Recurrence Frequency is set to 1 Month, and the Recurrence Limit is set to 6, then the quota refreshes 6 times. If the quota is provisioned on January 1st, it expires on June 30th. Default value is 0.
Auto Rollover	When selected, automatically roll unexpired quota over into a Rollover quota when the refresh occurs. **Note** When not checked then rollovers can only be triggered by using the RolloverCredit API. **Note** If checked, the Recurrence Frequency for the quota must be >= 1 day. Default value is false (unchecked).
Align ROQ Validity Period With RQ BillCycle	When selected, CPS aligns the rollover quota validity period with recurring quota billing cycle. CPS ignores the Validity Period settings in the linked Rollover Quota Template and uses the next billing cycle date of RQ for Validity Period of ROQ. Default value is false (unchecked).
Use Rollover Expiration Time for Charge Priority	When selected, the Balance module uses the sum of recurring quota template's credit end date and the rollover credit's end date to determine priority for which credit to debit in the normal processing of charges. Default value is false (unchecked).
BillCycle Per Quota	When selected, BillCycle on quota level is used. When not selected, BillCycle on account level is used. Default value is false (unchecked).
Thresholds	

Parameters	Description
Code	Unique name for the threshold object.
Amount	An integer representing the amount of quota that triggers the threshold notification.
Type	Unit of calculation like Percentage or Bytes.
Group	Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group are returned.
Trigger on Remaining	This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.

Note All the dates in Balance such as start, expiration, refresh, etc. have a time element. What is set for the time element affects expiration and refresh time on the given day.

Refresh Dates

There are two important dates - Last Recurring Refresh (LRR) and Next Refresh. The LRR is used to calculate the Next Refresh. The LRR is the value stored in the database while the Next Refresh is the value that is calculated during processing and is returned in API responses.

The LRR is set to the provision date by default. For a monthly recurrence frequency that means, if provisioned on the 12th, it will refresh again on the 12th of the next month. The LRR can be overridden in a provisioning request (CreateBalance API). When creating quota with the CreateBalance API, set the LRR date to the day when the refresh would have occurred had the quota existed. For example, if the CreateBalanceRequest is sent on 01/01/2012 at 08:00:00 (January 1st, 2012) and the intention is to have the quota refresh on the 28th of the month, then the LRR (lastRecurringRefresh) should be set to 28/12/2011T00:00:00 (December 28, 2011) in the request. The Balance engine uses the LRR to calculate the Next Refresh date, so by setting the LRR to December 28th (the previous month in relation to the provision) the new refresh date of January 28th, 2012 will be calculated correctly. Please note that months have a variable amount days and will refresh accordingly.

Note Valid date formats for API requests are explained in the Unified API documentation. Contact your Cisco Technical Representative for the API documentation.

Manual LRR Override

When overriding the LRR via API, make sure that the start date and end date align properly. That is, the end date must be the same date as what the Next Refresh date would be (LRR + recurrence frequency) when calculated by the Balance engine. This means that the provisioned credit will end when the new credit is created via the refresh which is how the system operates by default.

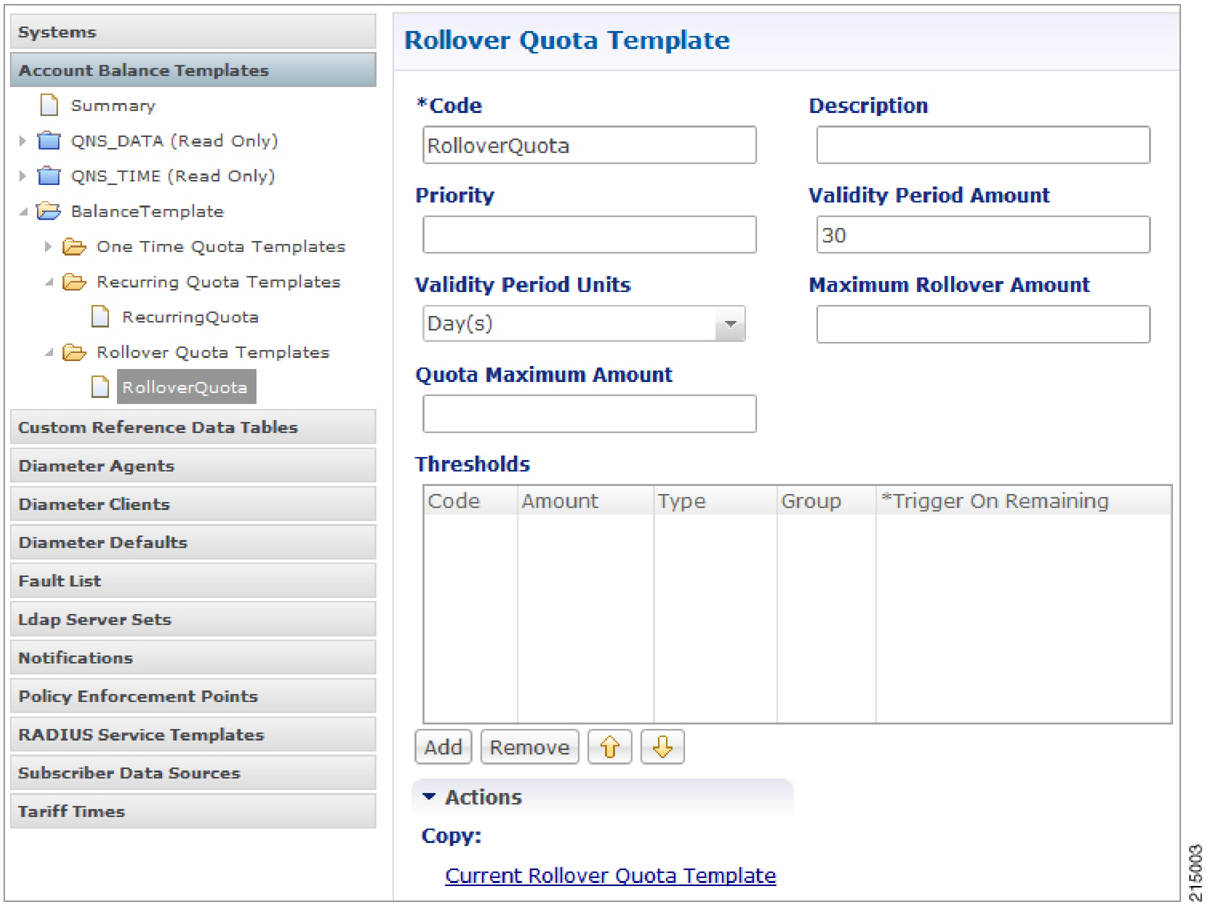
The refresh occurs on the next Balance action instead of on the actual Next Refresh date so that not all subscriber accounts refresh at the exact same moment, thus balancing load and resources. However, it should be noted that the date of the new credit created by the refresh will still have its dates based on the stored LRR and not on when it is actually refreshed by the Balance engine. The new credit will have a start date equal to the new LRR after the refresh has occurred. The new credit end date will be the start date + recurrence frequency. This value is also the new Next Refresh Date.

Rollover

Rollover quota templates are special quotas that store leftover amounts from a Recurring quota. Rollover occurs when the Recurring quota refreshes. Rollovers can also be triggered manually via API. The amount to rollover can be limited, and the total amount in the rollover quota can be limited.

Rollover quota templates behaves like One Time quota templates, but should not be provisioned directly. Unlike One Time quotas, Rollover quotas have no default/initial amount.

Figure 165: Rollover Quota Template



Rollover Quota Template

*Code: RolloverQuota

Description:

Priority:

Validity Period Amount: 30

Validity Period Units: Day(s)

Maximum Rollover Amount:

Quota Maximum Amount:

Thresholds

Code	Amount	Type	Group	*Trigger On Remaining

The following parameters can be configured under Rollover Quota Template:

Table 157: Rollover Quota Template Parameters

Parameters	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.
Amount	A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration. **Note** Future amount changes can be accomplished with the Credit API.
Priority	Priority ranks the template so when the Balance module is determining the next credit to use for reservations and debits, the template with the highest rank (Positive number Integer) wins. 1 is the highest rank. The default of no value is lowest priority. After priority, the most recent end date (Next to Expire) is used to determine the next credit. Default value is null.
Validity Period Amount	Integer used in conjunction with the Validity Period to determine the length of time for which the quota is valid. Default value is 30.
Validity Period Units	Value used in conjunction with the Validity Period Amount to determine the length of time for which the quota is valid. Default value is Days.
Maximum Rollover Amount	The maximum amount of quota that can be rolled over at any one time.
Quota Maximum Amount	The total amount of rollover the quota can contain.
Thresholds	
Code	Unique name for the threshold object.
Amount	An integer representing the amount of quota that will trigger the threshold notification.
Type	Unit of calculation like Percentage or Bytes.
Group	Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.
Trigger on Remaining	This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.

Rollover Quota Example

Assumptions:

- Assume the parent Balance Template's units are Megabytes.
- Assume the Maximum Rollover Amount is 100 MB.
- Assume the Quota Maximum Amount is 2048 MB (or 2 GB).
- Assume the current balance of the rollover quota is 1.95 GB.
- Assume the unused usage at recurring quota refresh time is 200 MB.
- Assume the Auto Rollover checkbox is checked.

Function:

- The recurring quota has 200 MB, but only 100 MB is allowed to be rolled over because the Maximum Rollover Amount is set to that value.
- Rolling over 100 MB would cause the total amount of the rollover quota to exceed 2 GB (Quota Maximum Amount is set to 2048 MB).
- Therefore, 2 GB - 1.95 GB = 50 MB, which is the amount that is actually rolled over.

Limitations and Restrictions

Rollover Quotas may experience undesirable behavior when used in conjunction with Recurring Quotas that have a recurrence frequency of less than 1 day.

The recurring quota and rollover quota involved in the rollover operation must be defined under the same Balance template. Rolling over from one Balance template to another Balance template is not supported.

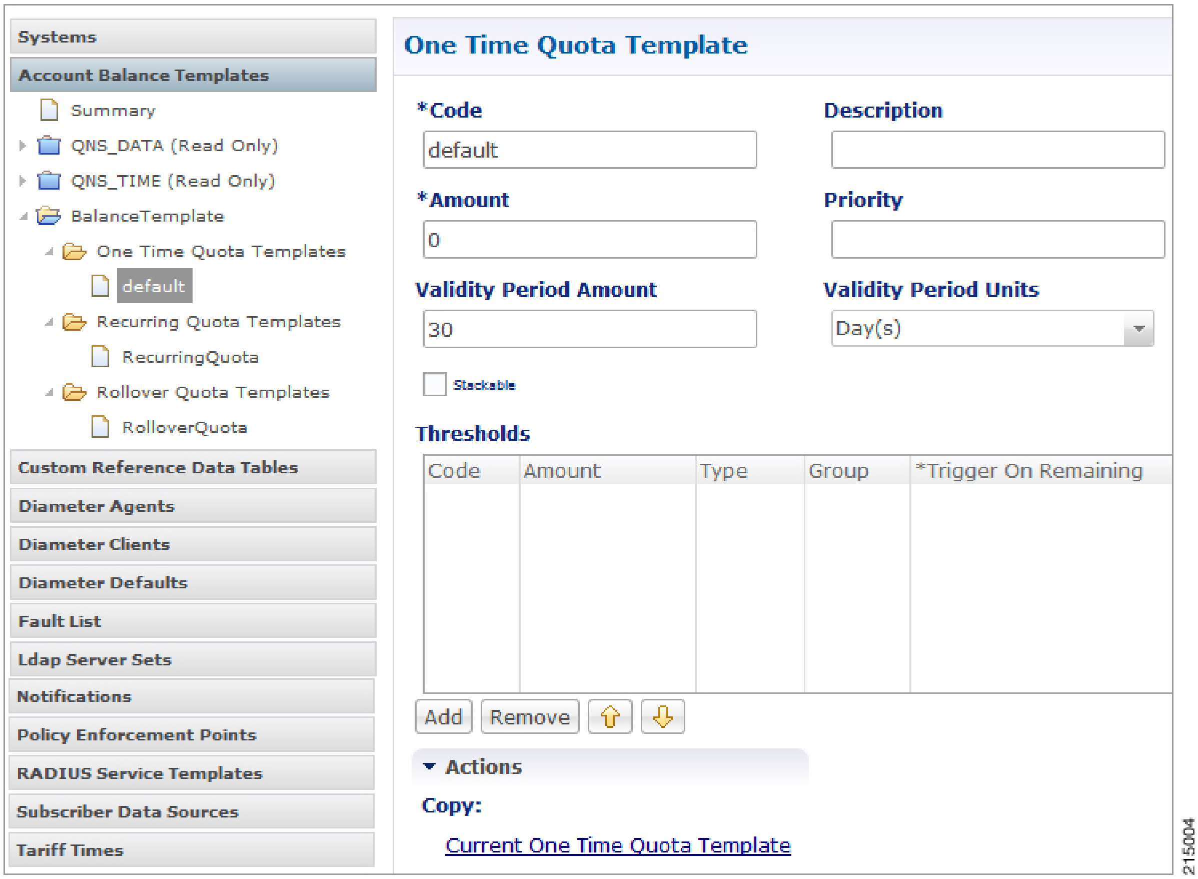
Note Do not provision rollover quotas using the Control Center. Even though Rollover quota is a special type of One Time quota, they are not designed for manual provisioning. They are designed to work with a Recurring quota and receive credits only based on the unused amounts rolled over from that Recurring quota to which they are linked.

Adjustments can be made to Rollover quota via the Credit or Debit APIs, but this is not a typical or common use case, and is not recommended by Cisco.

One Time

One Time quota templates are used for one time applications like TopUp or Bonus quota that has a finite duration (start and end date) and amount. One Time quota does not refresh automatically.

Figure 166: One Time Quota Template



One Time Quota Template

*Code: default

Description:

*Amount: 0

Priority:

Validity Period Amount: 30

Validity Period Units: Day(s)

□ Stackable

Thresholds

Code	Amount	Type	Group	*Trigger On Remaining

Copy:

The following parameters can be configured under One Time Quota Template:

Table 158: One Time Quota Template Parameters

Parameters	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.
Amount	A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration. **Note** Future amount changes can be accomplished with the Credit API.
Priority	Priority ranks the template so when the Balance module is determining the next credit to use for reservations and debits, the template with the highest rank (Positive number Integer) wins. 1 is the highest rank. The default of no value is lowest priority. After priority, the most recent end date (Next to Expire) is used to determine the next credit. Default value is null.

Parameters	Description
Validity Period Amount	Integer used in conjunction with the Validity Period to determine the length of time for which the quota is valid. Default value is 30.
Validity Period Units	Value used in conjunction with the Validity Period Amount to determine the length of time for which the quota is valid. Default value is Days.
Stackable	When selected the One Time quota becomes "stackable" which is explained Stackable Quota or MsBM Multiple Prepaid Plans. The general idea is that it is possible to provision a Stackable Quota multiple times, but only one instance will be active at any given time. The other instances will "stack up" or queue behind the active one waiting to be used. Essentially, it's a different way to configure priority of credit usage. Default value is False (unchecked).
Thresholds	
Code	Unique name for the threshold object.
Amount	An integer representing the amount of quota that will trigger the threshold notification.
Type	Unit of calculation like Percentage or Bytes.
Group	Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.
Trigger on Remaining	This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.

Stackable Quota or MsBM Multiple Prepaid Plans

The unique feature of Stackable Quota is that although a quota instance is provisioned it does not get used until the subscriber activates it via their network usage. Stackable quota does not expire if it is not used. For example, if a subscriber has an active plan and purchases a Stackable quota package. That package will never expire as long as the subscriber's current active plan stays active and has valid quota. Once the first plan expires, only then will the Stackable quota be activated and used.

Note Once a credit on a stackable quota is active, any changes made to the template validity period will not have an effect.

Priority

A Stackable quota will not activate until it is needed. This is most important in cases where Stackable and non-stackable quotas are mixed under the same Account Balance. For example, if a non-stackable quota is selected first based on Priority and the Next to Expire rules, the Stackable quota will not be activated until the non-stackable quota exhausts.

Pre-Paid Data Example

A subscriber purchases 5 pre-paid blocks of data quota with a default amount of 100MB and a validity period of 10 days. When the subscriber connects, the first instance becomes active, meaning the start date is set to the current date and time and the end date is set to 10 days later. So if the subscriber connected on January 1st, the quota became valid until January 11th (10 days from January 1st). After the subscriber uses all 100 MB or the 10 days passes, the next instance of quota is activated with the start/end dates set in the same manner - the start date is the current time at activation and the end date is set to 10 days from that time.

Pre-Paid Time Example

A subscriber purchases a time limit package that limits both "wall clock time duration" (calendar time since the package was bought) and volume of fair use quota. The package does not renew automatically, however the subscriber is able to purchase additional pre-paid plans prior to the expiration of the current package they have. Each pre-paid package will automatically start upon expiration of the previous plan just as in the data example. Like the data example, if the time limit is reached, the next package becomes active. If a subscriber reaches the volume of fair use quota limit, the current plan expires and the next plan becomes active regardless of the time remaining on the previous package. If there are no additional pre-paid plans available upon expiration of the current active package, the subscriber is redirected to a self-care portal and offered more options to purchase packages.

Provisioning

Provisioning a Stackable quota sets the start time to the current system time by default, and if a start date value is passed in, it is set to the passed in value. If the start date passed in is in the past and another Stackable quota is currently active, the new quota will not be used until the currently active Stackable quota is exhausted.

Debits and Reservations

As the accounting functions operate, reservations check for active credits. When a credit expires, the system automatically looks to find the next credit based on various criteria including the next most recent expiration date. If the found credit is part of a Stackable quota and is not currently active, the system will activate it by setting the start date to the current date and time and setting the end date to the start date plus the validity period.

If it is necessary to activate a second stackable quota to satisfy the requested reservation amount, even if you release the reservation (charge zero or less than what is remaining on the first quota), the system will maintain two active Stackable quotas.

If no quota is active for a subscriber, a Stackable quota will not get activated until a reservation is made.

QueryBalance API

The QueryBalance API displays all credits whether the Stackable quota is active or not. The API does not provide an indication of whether a quota is Stackable.

Template Definition Changes

If a quota template is changed from stackable to not stackable or from not stackable to stackable, any credits for quotas of that quota code provisioned/credited prior to this template change will behave in the following manner:

- From Stackable to Not Stackable: Any credits on quotas of that quota type that have already been provisioned/credited will have those existing credits behave as a normal one time quota's credits with no expiration date regardless of any set validity period. Future credits will have their end dates set by the validity period.
- From Not Stackable to Stackable: Any credits on quotas of that quota type that have already been provisioned/credited will have those existing credits behave as a normal one time quota's credits with the start date of the provision date or the start date that was passed in if it was specified and the end date that was specified or if not specified the start date plus validity period at provision time. Any future credits will be treated as stackable credits on a stackable quota.

BillCycle

BillCycle quotas were introduced in Balance 2.3.0. BillCycle is a special type of Recurring quota that handles end of month refresh dates better than the typical Recurring quota template. The Bill Cycle functionality aligns better with some customers' billing cycles and removes the recommended limitation of only using days 1 - 28 for Recurring quota starts/ends.

Note The “RFAmt ignored” hint that appears on BillCycle in Policy Builder is just a reminder that the Recurrence Frequency Amount field is ignored if you select a Recurrence Frequency of BillCycle. Refresh happens every 1 BillCycle regardless. The system cannot wait 2 or more BillCycles before refreshing.

Updating BillCycle

The ChangeBillCycle API is the only way to change the BillCycle value for a subscriber.

Repurposing Recurring Quota Templates

It is possible to use BillCycle by repurposing a currently existing Recurring quota that has a recurrence frequency other than BillCycle. When repurposing an existing Recurring quota template and changing it to BillCycle, existing subscribers will have the BillCycle value set automatically at the next refresh time to the day that the quota refreshes. For example, if a subscriber’s quota is scheduled to refresh on the 25th, he/she will continue to use quota until the refresh date as normal. When the quota refreshes on the 25th, the BillCycle value will be set to 25, and the subscriber’s quota will now follow the BillCycle frequency rules instead of the previous recurrence rules.

Note Repurposing works best with Recurring quota templates that have a recurrence period of 1 Month.

Monthly vs. BillCycle

Monthly and BillCycle really only differ when BillCycle is set to 29, 30, or 31. Current subscribers won’t be able to take advantage of 29, 30, 31 if you reuse a quota code. However, using the ChangeBillCycle API existing subscribers can update their BillCycle setting to 29, 30, or 31.

Any new subscribers provisioned with a repurposed quota template will start out with BillCycle functionality and a BillCycle value must be passed in with the CreateBalance API.

End Date and Last Recurring Refresh (LRR)

End Date will be set to 23:59:59.999 in the server's local time zone on the day before the BillCycle day. For example, if the BillCycle value is 15, with the server set to GMT (Zulu time), then the end date in March would be 2013-03-14T23:59:59.999Z.

The Last Recurring Refresh (LRR), which drives the Next Refresh date that appears in API responses and drives the actual quota refresh trigger, will be midnight on the BillCycle day in the previous month. For example, if the BillCycle value is 15, with the server set to GMT (Zulu time), then the LRR in the credit period before March 15th will be 2013-02-15T00:00:00.000Z, which would display a Next Refresh date in a QueryBalance response as 2013-03-15T00:00:00.000Z.

End Date Provisioning

The start date defaults to the date the provisioning call is made. The LRR defaults to the start date. The end date defaults to the start date plus one month with any necessary modifications of the day to respect the BillCycle value. The start, end, and LRR dates can be overridden if a start, end, or LRR date is passed in on the CreateBalance API request. Overriding those dates can cause Balance malfunctions if incorrectly set, so use caution!

Month End Dates Example

Recurring Quota templates are only able to use 1-28 for refresh dates. BillCycle was an enhancement for Recurring quota that allows Balance to accommodate the number of days variance of months. If the subscriber's BillCycle is set to 30, the refresh in February will be on the 28th or 29th if a leap year, and QueryBalance API responses would show the Next Refresh Date as YYYY-02-28 or YYYY-02-29. And once the refresh has occurred and it's now March the system is able to reset the Next Refresh date back to the 30th based on the BillCycle and would show as YYYY-03-30. Compare this to regular Recurring quota which would change the refresh date to the 28th or 29th permanently for the rest of the year. Even if the refresh occurred on January 30th, when February arrived, the refresh would be set to the 28th or 29th if a leap year. Unlike BillCycle, once the refresh has occurred and it's now March the system does not know how to reset the refresh back to the 30th as is occurred in January for regular Recurring quota. The Next Refresh date would show as YYYY-03-28 or YYYY-03-29.

Note All the dates in Balance such as start, expiration, refresh, etc. have a time element. What is set for the time element will affect expiration and refresh time on the given day.

Thresholds

Thresholds allow policy actions to be taken when a certain amount of quota has been used. Actions can be taken on threshold breach, unbreach, and continued breach status. Thresholds can be grouped to suppress past threshold breaches.

The threshold table in the Policy Builder sets thresholds that will be reported on when breached/unbreached and what their current amount is while breached. These messages are sent back to the policy engine from MsBM on Credit, Debit, Charge, and Provision functions so that policies can make decisions and take actions based on the threshold breach.

The basic conditions to use in policy configuration are:

- An OCSThresholdBreach exists

- An OCSThresholdUnbreach exists
- An OCSThresholdStatus exists

A typical action upon threshold breach is “Send a SMS notification”. To send an SMS notification, the Notifications feature must be installed and configured in the system.

Threshold Event Types

- OCSThresholdBreach: It occurs when a threshold is violated for the first time
- OCSThresholdUnbreach: It occurs when a credit, provision, refresh, or other action causes usage to drop back below a given threshold
- OCSThresholdStatus: It is the message that is sent every time an action is conducted against an account where a balance threshold or quota threshold is currently exceeded. This message reports the fact that the threshold is still breached and what the current level of the breach is.

Note A threshold is breached when the value is greater than or equal to the threshold value.

Balance Functions That Evaluate Thresholds

- Charge: Checks thresholds of the account balance specified in the charge request and any quotas under that account balance whose total changed due to the charge.
- Credit: Checks the thresholds of the account balance and quota specified in the credit request.
- Debit: Checks the thresholds of the account balance specified in the debit request and all quota codes under that account balance unless a quota code is specified on the debit request, in which case, it only checks the thresholds of that quota.
- Reserve: Checks all thresholds on the account.
- QuerySubscriber: Checks all thresholds on the account.

Reference Data vs. Subscriber Specific Thresholds

Reference Data Thresholds (RDT)

- Reference Data thresholds (RDT) are defined on the Balance or Quota Template in Policy Builder.
- RDTs are evaluated for all subscribers provisioned with the related balance or quota code whose template has the threshold defined.
- RDTs are stored in the reference data that the Policy Engine reads for operational configuration.

Subscriber Specific Thresholds (SST)

- Subscriber Specific Thresholds (SST) are defined via API or Policy Action.
- SSTs are only applicable for the subscriber for which the SST was defined via API or Policy Action. You must defined the SST individually for each subscriber for which you want the threshold applicable.
- SSTs contain the same types of information as RDTs, but the information is stored on the subscriber account in the database.

Unique Names

Thresholds must have unique names. SSTs and RDTs must have unique names as well. The same SST name can be used for multiple subscribers, but that value must be unique compared to the name values for the RDTs.

Important Clarifications

- Even though both kinds of thresholds share the same types of information, there is no crossover between the two sets of information. RDT definition via the Policy Builder is for RDTs only. SST definition via API is for SSTs only.
- It is important to understand that the codes and information defined in Policy Builder for RDTs have no relationship to SSTs.
- If you use an RDT code when creating an SST, the information needs to be defined for the SST and will not read the RDT information just because it's the same code.

Threshold Groups

Thresholds with the same value in the Group column will be "grouped" together. When thresholds are grouped in this manner, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.

For example, if you define a 80 percent, a 60 percent, and 50 percent threshold and they are in descending order, top to bottom in the table, and put them in a threshold group named CiscoPercents, the system will only send threshold messages about the highest threshold breached. This helps reduce duplicate messages. For example, a subscriber's usage is at 62%, the subscriber will only get messages about the 60 percent threshold's status. When the usage crosses 80% and goes to 81%, the subscriber will no longer get the 60 percent threshold's status message, but instead will get an 80 percent breach message and moving forward will only get 80 percent threshold status messages.

Note Order is very important! This functionality is not based on the highest value. If there are two thresholds in a group say at 60 percent and 80 percent and they are ordered in the table top to bottom in ascending order, that is, 60 nearest the top, the subscriber will never get 80 percent threshold notifications unless you select the amount remaining option instead of amount used (default).

Thresholds and Reduction of Reservation Granted Amounts

A Threshold defined on an Account Balance Template reduces the reservation amount as it nears the threshold. For example if the subscriber is 50 MB away from the threshold and the default reservation amount is 100 MB, the reservation will be reduced to 50 MB so as to not exceed the threshold.

Note For all Balance versions/revisions built prior to 7 Jan 2014, reservation amount reduction as a threshold is approached only works for thresholds NOT defined as Trigger On Remaining, that is, it only works for thresholds that measure the amount used.

A Threshold defined on a Quota Template does NOT reduce the reservation amount as it nears the threshold.

When the reservation granted amount is reduced from the requested amount due to a threshold, the quota granted is reduced to the amount between the current usage level and the value where the threshold would be breached. This reduction continues on each successive reservation until the Default Minimum Dosage defined on the Balance Plugin Configuration is reached. After that value is reached for the granted amount, the next reservation will go back to normal behavior and trigger the OCSThresholdBreachOccurred condition.

Soft vs. Hard Thresholds

Currently, all thresholds in CPS are “soft” thresholds.

The difference between a soft and hard cap is that the system would still grant the minimum dosage with a soft cap; however with a hard cap the system will deny the quota request if the minimum dosage would breach the threshold. The plan is that when a hard threshold is implemented, an API call or Policy Action would have to be made to “unlock” the threshold to allow reservations to breach the threshold and for normal operation to resume.

Other Threshold Information

- Thresholds are based on CHARGED amounts. Reserved amounts are not included.
- Thresholds can be defined on the Account Balance Template (monitors all child quotas as an aggregate) and the Quota Template (only monitors the credits of that quota).
- Thresholds are based on the total of all currently valid credits under the specified balance/quota. A “currently valid credit” is a credit for which its start date is before the current date and its end date is after the current date. For example:
  1. There is a credit of 1 GB that ends on Oct 15th.
  2. There is a percentage threshold at 90%.
  3. The subscriber uses 900 MB of data, which triggers the threshold.
  4. Another 1 GB credit is applied that ends on Oct 31st.
  5. The calculated percentage against the threshold is now 55%. However, if the subscriber waits to use the network until after Oct 15th, then the calculated value will be 0%.
- Percentage based balance thresholds are based on the ((amount charged divided by the original amount) * 100) across all currently valid credits of all quotas defined under the given balance. For quota thresholds only the currently valid credits of that specific quota are considered
- Using the QuerySubscriber API:
  - The original amount that a threshold is compared against can be determined using the calculation of balanceTotal + debitedTotal + reservedTotal.
  - The amount charged is the debitedTotal.
  - Therefore a percentage threshold is calculated as (debitedAmount/(balanceTotal + debitedTotal + reservedTotal)) * 100.

Depletion and Exhaustion

The Depleted flag is set when isExhausted is set to true and the granted quota is zero on the OCSCreateReservationResponse from the Balance Manager.

IsExhausted is set whenever the full requested reservation amount cannot be fulfilled.

Note Keep in mind that in both cases these conditions may not mean that the balance is completely exhausted permanently. If there is more than one reservation against the balance, one of those reservations may only be partially charged or released altogether (either through expiration or zero charge) which will release an amount of quota which will again become available for use.

Depletion and Exhaustion vs. Thresholds

Depletion and Exhaustion, as discussed above, are based on BOTH Charged and Reserved amounts.

Thresholds are ONLY based on Charged amounts.

This differentiation is particularly important when using 100% or total amount used thresholds. Just because the Depleted flag is set to True DOES NOT mean a 100% Threshold will have been breached yet. The outstanding reservations that may exist when Depleted is triggered need to be FULLY charged before the Threshold Breach will occur.

Charging Expired Reservations

The Balance Plug-in Configuration contains a field called Expired Reservations Purge Time, which when set allows the retention and charging of expired reservations. In some systems with significant lags in usage reporting, this option provides a mechanism to maintain more accurate accounting.

The Expired Reservations Purge Time is how long reservations can be charged after they expire as long as quota is not exhausted.

- A 0 value for Expired Reservations Purge Time means it doesn’t keep any expired reservations after they expire.
- A non-zero amount is the amount of time in minutes it will keep a reservation and allow charges against said expired reservation.
- There is not a recommended value other than zero which is the default for legacy reasons. The value depends on how the system is being used, what network device is being used, and how often and how late it reports usage.

Credit Selection Logic for Reservations and Debits

Determining the next active credit to reserve against is done by the following logic:

- Credits belonging to the highest priority (lowest numerical priority value; priority 1 is highest) quotas are examined first.
- Credits that are next to expire are examined next. That is, credits with the soonest end date. If there are multiple credits with the same soonest end date, then the credit will be selected from that subset as the one with the oldest start date.
- If no credits with end dates are found, credits with no end date are examined, and the credit with the oldest start date is used first.

Note This logic is restricted to a given quota code when a Debit is performed with a quota code specified as opposed to a Debit without a quota code which will check across all the quotas defined for the subscriber to find an applicable credit.

Rates and Tariff Times

Rates provide a mechanism to alter how quota is billed to a customer. Typically, it's a 1 to 1 relationship. A customer uses 1 MB and is charged an amount, say $1, for that 1 MB. By changing the rate, the SP changes the cost that the subscriber pays. For example, a rate of 0.25 will charge quota at a cost of 1 MB for every 4 MB used. A rate of 2 will charge quota at a cost of 2 MB for every 1 MB used.

The rate is specified when the system makes a reservation. The default rate is 1.

Tariff Times

Tariff Times is the CPS nomenclature for defining rates and when to apply them. To determine the current TariffSwitchTime, Balance takes the current time (using the time zone specified on the tariff time reference data configuration) and checks each switch time in order top to bottom to see if the current time matches a TariffSwitchTime. The first tariff switch time that matches (including the associated valid dates OR a holiday date) will be used. The time of the tariff switch will be the end of the current tariff period. Then the next tariff switch time is calculated, by taking the end of the current tariff switch time, adding one second and searching each tariff switch time (top to bottom) to find the first one that matches.

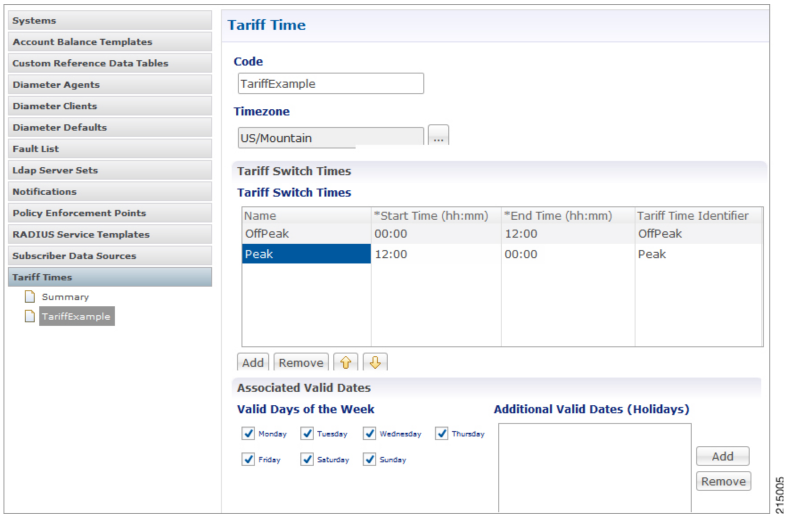
Tariff Times Configuration

This covers setting up rates for any component which uses Autowire Balance. Autowire Balance is the default blueprint for Balance that must be configured in the Policy Builder for use in the base system setup. Autowire Balance is an extension of the main system blueprint which Cisco engineering refers to as Autowire.

1. In Policy Builder, select **Reference Data** > **Tariff Times**.
2. Create a new child.
3. Set the timezone if needed.
4. Make sure that you make rows which cover all 24 hours in a day.

Note A Start Time of 00:00 (midnight) is inclusive. An End Time of 00:00 (midnight) is exclusive because 00:00 technically is the start of any given day. By using 00:00 for the end time instead of 11:59, it allows the system to account for all 86,400 seconds (24 hours) in a day.

Figure 167: Tariff Time



Tariff Time

Code: TariffExample

Timezone: US/Mountain

Tariff Switch Times

Tariff Switch Times

Name	*Start Time (hh:mm)	*End Time (hh:mm)	Tariff Time Identifier
OffPeak	00:00	12:00	OffPeak
Peak	12:00	00:00	Peak

Associated Valid Dates

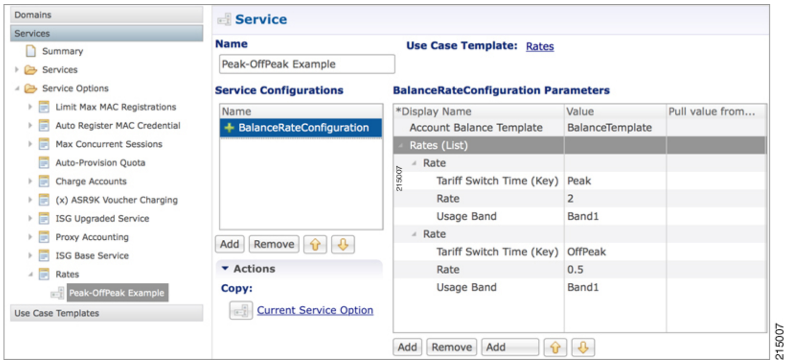
Valid Days of the Week

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday
☑ Friday ☑ Saturday ☑ Sunday

Additional Valid Dates (Holidays)

5. In Policy Builder, select **Service** > **Use Case Templates**.
6. Click **Actions** tab.
7. Select **Add** in **Service Configuration**.
8. Select **BalanceRateConfiguration**.
9. Choose an Account Balance Template.
10. Under the Rates List, choose a Tariff Switch Time (Key).
11. Under the Rates List, change the Rate as needed.
12. Click **Add Child** to add more Rate options.
13. In Policy Builder, select **Services** > **Service Options** > **Rates**.
14. Click **Create Child Service Option**.
15. Click **Add** in **Service Configuration**. Select **BalanceRateConfiguration**.

Figure 168: Service



Service

Name: Peak-OffPeak Example

Use Case Template: Rates

Service Configurations

Name
BalanceRateConfiguration

BalanceRateConfiguration Parameters

*Display Name	Value	Pull value from...
Account Balance Template	BalanceTemplate	
Rates (List)		
Rate		
Tariff Switch Time (Key)	Peak	
Rate	2	
Usage Band	Band1	
Rate		
Tariff Switch Time (Key)	OffPeak	
Rate	0.5	
Usage Band	Band1	

16. Click **File** > **Publish to Runtime**.

Edge Cases

It is strongly recommended that Tariff Switch Times cover all times during a 24 hour period and do not have gaps. Some customers use a default Tariff Switch Time entry that covers all the other times that have not been specifically defined.

Tariff Times are not allowed to cross over the midnight boundary for a given day. In practice, this means that often 2 or more tariff switch times must be created to cover a single logical period. For Example:

Table 159: Edge Case Examples

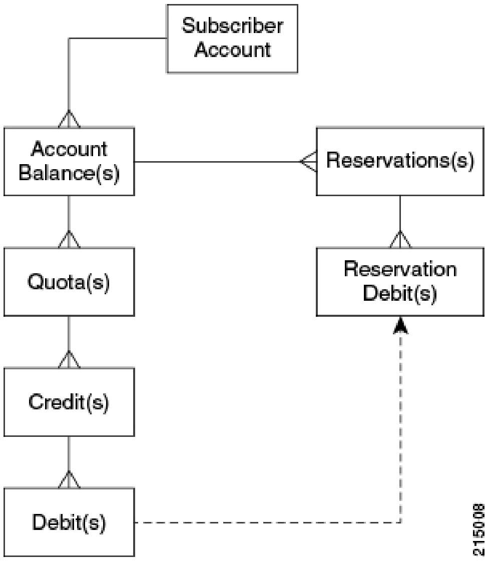
Name	Start Time	End Time	Tariff Time Identifier
Nights Before Midnight	17:00	00:00	NIGHT
Nights After Midnight	00:00	07:00	NIGHT
Days	07:00	17:00	DAY

If a Tariff Switch occurs during a daylight savings time forward switch (i.e. between 2:00am and 3:00am during 'Spring Forward' in March), an error will occur in processing during that time since that hour is lost. Therefore, it is recommended that switch times NOT occur during these times on those days.

Subscriber Record

For any given subscriber, the following illustrates the database relationship of the objects described in this chapter.

Figure 169: Subscriber Records



An important point to keep in mind when looking at the data structure for MsBM is that this is a document based database and not a relational database. The below description attempts to describe the equivalent RDMS concepts as far as primary and foreign keys are concerned; however, these concepts are not the same in a document based database, and are included merely to assist in providing understanding since most of audiences are familiar with RDMS.

For example, since Mongo stores data in a structure that is essentially a map of maps, there is no need for the concepts of a primary key (PK) or a foreign key (FK) since relationships between the data is defined by the physical structure. Conceptual PKs and FKs are only needed when interaction with the QNS system or when the querying is necessary and the full document is not retrieved.

Note This listing is not a complete listing of all fields (conceptually columns) in each map (conceptually table), but only the important fields used for data structuring or querying.

Subscriber Account

- subscriberId (PK)
  - Key field to reference a given subscriber account. This account may be shared among multiple subscribers.
  - Value is also stored as _id which is a key field for the Mongo database document. These values were different in early versions of MsBM, but have been aligned to ensure greater system stability. The _id was originally a Mongo assigned UUID.
- The Subscriber Account contains all data structures related to a specific subscriber's account as it relates to MsBM. When you retrieve a Subscriber Account, you obtain all MsBM information for a given subscriber.

Account Balance

- accountBalanceCode (PK within the scope of a given subscriber account)
  - relates to the Account Balance Template reference data information defined in Policy Builder.
  - key for Policy Engine to access this balance's information for a selected subscriber account.
- An account balance, or simply a balance as it is often referred to, is essentially a group of quotas. The idea is that a customer could create a balance (quota grouping) called Data and within that have several quotas defined, like Monthly, Topup, and Bonus. Then when the subscriber uses account, usage is charged against their Data balance and MsBM determines which underlying quota should be debited based on rules set up in Policy Server (QNS). The intent here is to simplify charging so that specific “buckets” do not need to be specified and necessary business rules can be defined once in the Policy Engine.

Quota

- quotaCode (PK within the scope of a given subscriber account)
  - relates to the Quota Template reference data information defined in Policy Builder.
  - key for Policy Engine to access this quota's information for a selected subscriber account.

- A quota defines the actual amount or "bucket" that can be drawn from for tracking of usage. This value internally is unit-less and thus can be defined to be whatever is needed in the implementation. Some units are provided in reference data in Policy Builder to assist users. Common usages for quota amounts are bytes of volume, seconds of time, but other counts can also be tracked.

Credit

- A UUID (PK) is used as a key to the map containing all the credits for a given quota.
- A UUID was selected since the data structure was defined for transactional speed and stability and was not intended to be queried directly. MsBM records are intended to be accessed using the Policy Engine, the provided APIs, and the Reporting Engine. The intent in the design of this structure was transactional usage and performance, not queryability. A sequence concept or other more predictable key was not used since a sequence would most likely be rapidly exhausted and more difficult to manage since credits are regularly created and destroyed as part of the normal operation of MsBM. Uniqueness and assurance of avoidance of deadlocking is the primary concern.
- Credits can be viewed as positive entries on an accounting balance sheet.

Debit

- A UUID (PK) is used as a key to the map containing all the debits for a given credit.
- The reasoning for selection of the UUID is the same as discussed under Credit, on page 385.
- Debits can be viewed as negative entries on an accounting balance sheet for a specific credit. Debits under a given parent credit cannot exceed the amount of the parent credit.

Reservations

- reservationId (PK)
  - Also a UUID and was selected for similar reasons as discussed under Credit, on page 385.
- Reservations describe an amount of conditional debiting of quota that is reserved until a network device reports that the quota has actually been utilized.

Reservation Debits

- reservationDebitId(PK)
  - Also a UUID and was selected for similar reasons as discussed under Credit, on page 385.
- reservationId (FK)
- debitId (FK)
- Reservation debits serve the purpose of providing a link between a reservation and an actual debit entry. When a reservation is charged, the reservation and associated reservation debits are removed and the

debit linked to those reservation debits are made permanent. That is, as long as a debit has a linked reservation debit, that debit is not permanent, but only reserved in a non-committed state.

Thresholds

The Thresholds collection contains any reference data thresholds (defined in Policy Builder) that are currently breached or any user-defined thresholds that are specific to a given subscriber account.

The thresholds map is not utilized and may not appear in all implementations. It will only appear as needed if the related functionality in Policy Server (QNS) is active.

Expired Reservations

An identical structure as Reservations is used for Expired Reservations, except that Reservation Debits do not have a link to Debits. Functionality for charging expired reservations, that is, creating debits, is handled in a different fashion.

The expired reservations map is not utilized and may not appear in all implementations. It will only appear as needed if the related functionality in Policy Server (QNS) is active.

Shared Quota

In CPS there are several ways to set up shared quota. SPR supports parent and child profiles, for example one parent in a household is the primary SPR record and all the other members of the household are set as child records of that SPR profile. This would allow for shared quota and is mostly configured through SPR data management. Because Balance and SPR can be used separately, Balance also supports shared quota use cases that are configured solely within the Balance module.

Shared Per User Limit Use Case

There will be two Balance accounts associated with a subscriber that is participating in a shared quota but also needs a per user limit on said shared quota. The first Balance account is the subscriber's personal account. This account will contain any balances/quotas that are only available to the subscriber. This account will also contain one balance that will be used for tracking the per user limit. The second Balance account is not owned by the subscriber and contains the shared balance/quotas.

Note The two Balance accounts need to be provisioned separately.

The shared balance template contains a field called Limit Balance that links the shared balance to a limit balance (the personal account), so that the Balance module knows which two balance codes it needs to reserve/charge against in the shared per user limit case. Since the per use limit is tied to a quota template, only discrete per user limits are supported. The number of balance/quota templates defined is not limited, but the templates must be defined for each per use limit level. The limit quotas must be defined in a balance/quota template.

The subscriber must be provisioned with the limit balance and an associated quota with a valid amount for the per user limit to be enforced. An AVP must added to the subscriber profile in SPR indicating the Balance account record and the Balance template name of the shared quota. This is done currently for some deployments. The subscriber must have the AVP set up prior to per user limits being available.

If the subscriber does not have the limit balance provisioned, then the subscriber will draw from the shared balance with no per user limit enforced.

Hard thresholds (meaning the subscriber cannot use more than a certain amount of the shared quota) will be enforced by the amount provisioned in the limit balance.

Soft thresholds (meaning the subscriber can continue to use more up to the hard threshold, but something should happen when the soft threshold is crossed) will be supported using the threshold mechanism defined on the limit balance.

The charge and reserve function of the Balance module were enhanced with conditional logic to make new calls to handle the shared per user limit reservations. The new calls allow charges or reservations against two Balance accounts at the same time. The two Balance accounts are the shared account, as indicated by the AVP, and the subscriber's personal balance account (the limit balance).

Policy Engine

The Balance module exposes various policy objects that can be used to monitor the status of an account. Aptly named the MsBM Account Status object, it contains information about a specific balance of a given subscriber. Each of the subscriber's balances will have its own MsBM Account Status object in the Policy Engine during policy execution.

The **Amount Remaining** value on the MsBM Account Status object DOES contain the values of any current reservations.

Proration

Balance provides some limited proration capabilities but in general, proration must be handled manually via API calls (Credit, Debit, ExtendCredit, CreateBalance).

Proration Example

A subscriber has 5 GB on the first plan and has used 3 GB of it. The subscriber then switches to a different plan with 2 GB. The subscriber will start with 2 GB of available quota UNLESS the CreateBalance API overrides the initial amount. Setting the override amount is a manual step that is handled by the calling system, i.e. customer portal or OSS/BSS application.

Quota Refresh Throttling

Balance has the ability to cause a batch of quota refreshes to be staggered over a time period, which causes session wakes up to be staggered, which not only keeps masses of subscriber accounts from being refreshed at the same exact time, but also causes any other events related to a session wake up to be staggered, i.e. RARs. This concept is called the Callback Validity Time (CBVT). The CBVT is usually set to the time where something changes in a subscriber’s balances/quotas. Typically this is the expiration date of their quota. The CBVT is that time at which a session will “wake up” and create a new reservation of quota. This "wake up" activity triggers a quota refresh if one is valid for a recurring quota.

For example, let's say that 50,000 subscribers on a monthly quota have their quota set to expire at 1 AM and all have sessions established. Normally their quota wouldn't refresh until they next accessed their account, i.e. had an active session that made a reservation or other Balance request (the refresh is retroactive however). However, some deployments have subscribers who always have a session, but it may not be actively using quota, i.e. idle cable modem. In this scenario, at 1 AM, 50,000 subscriber sessions will "wake up" and refresh their accounts which could easily cause a serious load spike for system resources.

To combat this problem, the Recurring Refresh Max Delay parameter defined in the Balance Plug-in Configuration, is used to pad the CBVT value by a random number of minutes between 0 and the parameter value. If the Recurring Refresh Max Delay param is set to 120, then the CBVT value on the session will be set to 1 AM plus a random number of minutes chosen from between 0 and 120. Now, the 50,000 sessions will not all wake up at 1 AM. Because the CBVT values are set to the range from 1 AM to 3 AM, at any given minute only a small percentage of the total 50,000 sessions will wake up and refresh.

Active Session vs. Inactive Session

Any subscriber actively using their quota will refresh immediately at 1 AM when they qualify for the refresh and will not have their quota refresh delayed. Only subscribers with sessions that are not actively using quota will have their refreshes delayed.

Sy Server Implementation in OCS

This section describes how to configure an OCS Sy server to manage policy counters that map to a subscriber's account balance template in an OCS node deployment.

Sy Client and Diameter Stack Configuration

This section describes how to configure the Diameter Sy client and the associated Diameter stack.

Step 1 In Policy Builder's **Reference Data** tab, select **Diameter Clients** in the left pane.

Step 2 Expand **Sy Clients**, and click **Sy Client** under **Create Child** in the **Sy Clients Summary** pane.

Step 3 Configure the client as needed.

Step 4 Set the **Counter Lookahead Interval Minutes** option to the number of minutes to look ahead to determine when the lookahead balance states configured for the SyServerSLRInformation service configuration object will expire, refresh, or start. It is set to 180 minutes by default.

Step 5 In the left pane, select **Systems** > **system_name** > **Plugin Configuration** > **Diameter Configuration**.

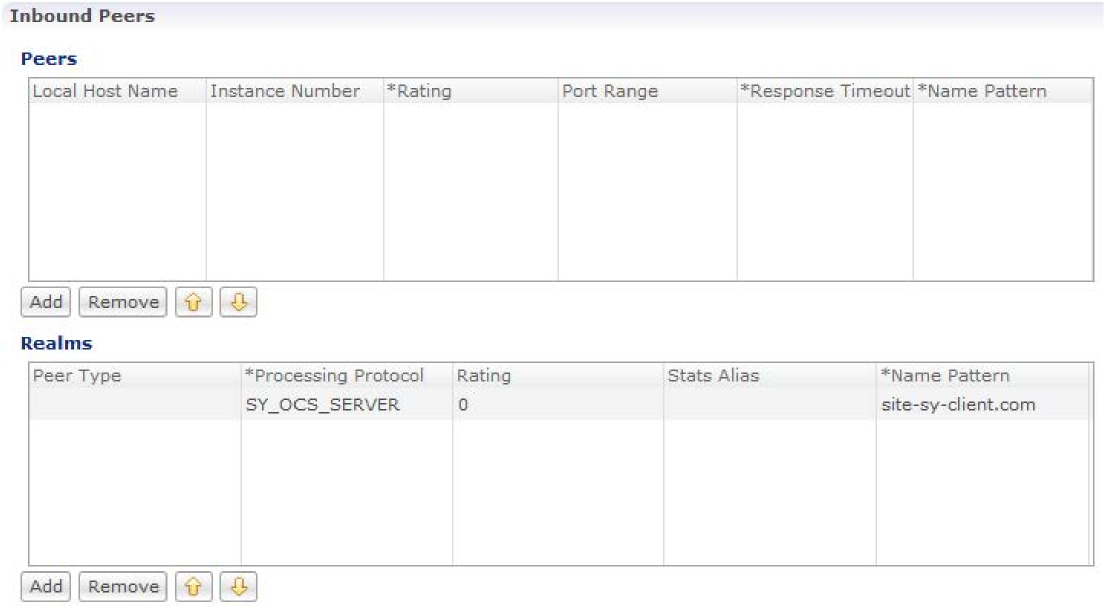
Step 6 In the **Diameter Configuration** pane, click **Create Child**, click **Diameter Stack**.

Step 7 In the **Diameter Stack** pane, type a **Name** and a **Realm**.

Step 8 Under **Inbound Peers** in the **Realms** table, select **SY_OCS_SERVER** in the **Processing Protocol** pull-down menu.

Step 9 Provide a **Rating** and a **Name Pattern** as well.

Figure 170: SY_OCS_SERVER Processing Protocol



Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern

Realms

Peer Type	*Processing Protocol	Rating	Stats Alias	*Name Pattern
	SY_OCS_SERVER	0		site-sy-client.com

Account Balance Configuration

The Sy server uses the CPS balance manager for volume/quota definition, and association to subscriber and threshold configuration. For configuration information, refer to Quota Templates, on page 365.

Use Case Template and Service Configuration

This section describes how to configure a use case template that uses the SyServerSLRInformation service configuration object. You should create a use case template using this object based on the account balance template and configured thresholds.

Step 1 Select the Policy Builder Services tab.

Step 2 In the **Summary** pane, click **Use Case Template** under **Create Child**.

Step 3 In the **Use Case Template** pane, select the **Actions** tab.

Step 4 Type a **Name**; for example, xyz_green.

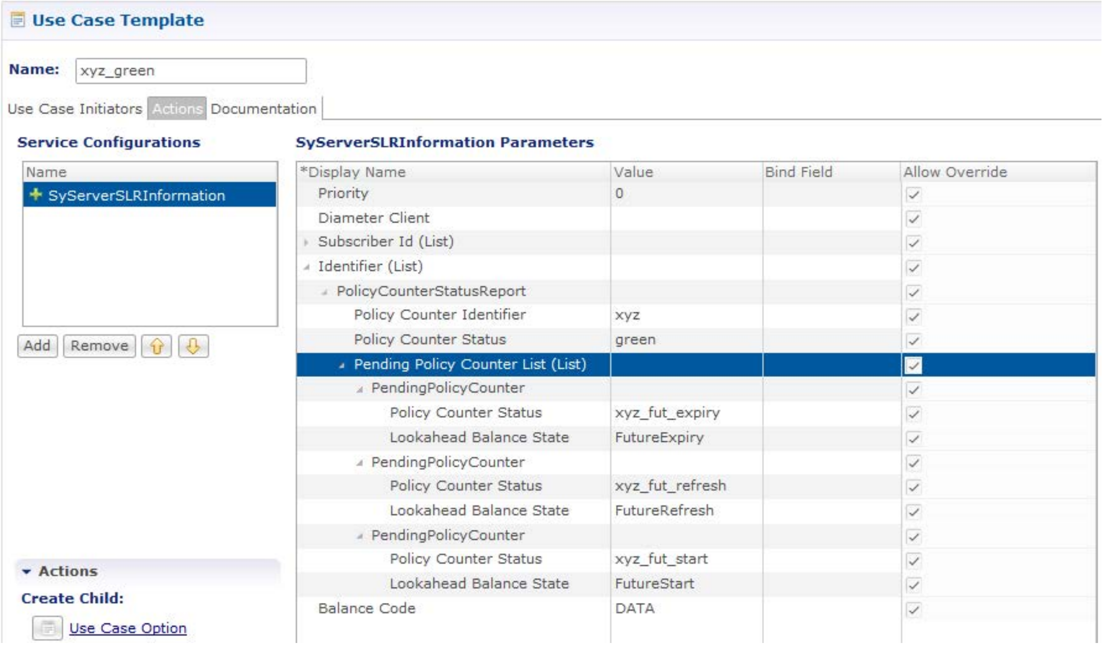
Step 5 Under **Service Configurations**, click **Add**.

Step 6 In the **Select Service Configuration** dialog box, scroll down to the **sy Server** section, select **SyServerSLRInformation**, and click **OK**.

Step 7 Configure the SyServerSLRInformation parameters.

The following figure shows an example configuration.

Figure 171: SyServerSLRInformation Service Configuration Object



Name: xyz_green

Service Configurations

Name
SyServerSLRInformation

SyServerSLRInformation Parameters

*Display Name	Value	Bind Field	Allow Override
Priority	0		☑
Diameter Client			☑
Subscriber Id (List)			☑
Identifier (List)			☑
PolicyCounterStatusReport			☑
Policy Counter Identifier	xyz		☑
Policy Counter Status	green		☑
Pending Policy Counter List (List)			☑
PendingPolicyCounter			☑
Policy Counter Status	xyz_fut_expiry		☑
Lookahead Balance State	FutureExpiry		☑
PendingPolicyCounter			☑
Policy Counter Status	xyz_fut_refresh		☑
Lookahead Balance State	FutureRefresh		☑
PendingPolicyCounter			☑
Policy Counter Status	xyz_fut_start		☑
Lookahead Balance State	FutureStart		☑
Balance Code	DATA		☑

The SyServerSLRInformation parameters are described in the following table:

Table 160: SyServerSLRInformation Parameters

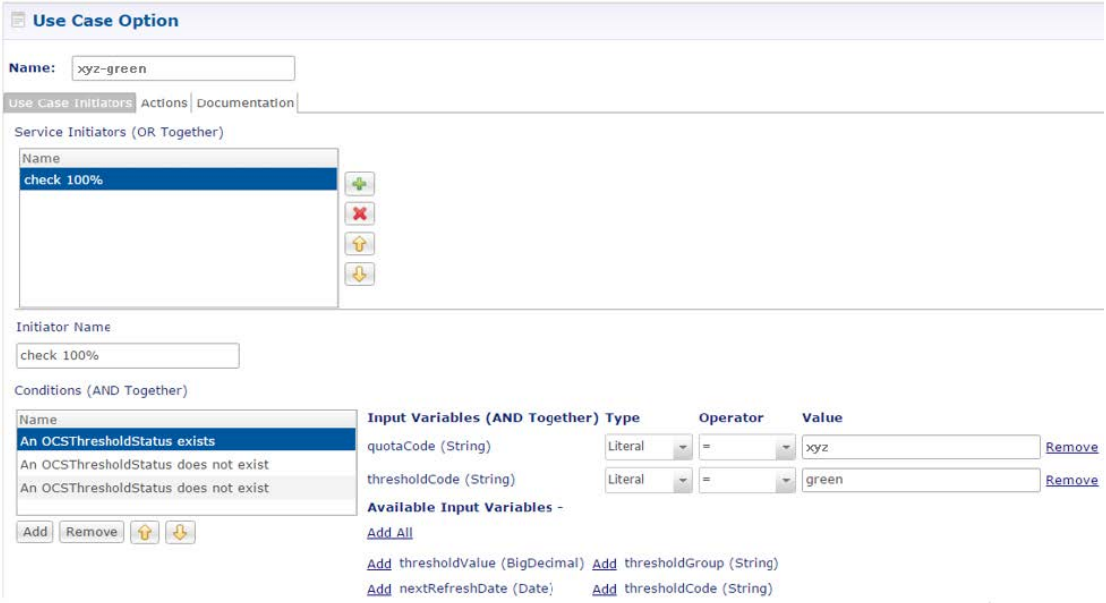
Parameter	Description
Priority	The priority of the message for processing. The higher the number, the higher the priority. Default for most settings: 0
Diameter Client	The client configuration is used to apply different policies based on PCRF type. To filter a service based on the Diameter client, specify which Diameter client you want the service to be applied to. This parameter is optional.
Subscriber ID (List)	Identifier – The user identity, which is mapped to the Subscription-Id AVP. Based on your requirements, you can configure one or more identifiers. Possible values for identifiers include: Session MSISDN – The MSISDN value of the subscriber. Session IMSI – The IMSI value of the subscriber.
Identifier (List)	Identifier Name – The subscribed Sy Policy Counter Identifier list, which maps to the Policy-Counter-Identifier AVP. OCS uses this list to send the Policy-Counter-Identifiers to the PCRF in the SLA/SSNR message.
PolicyCounterStatusReport	Contains the Policy Counter Identifier AVP, the status of this AVP, and the Pending Policy Counter List.

Parameter	Description
Pending Policy Counter List (List)	Contains the list of Pending Policy Counters. You can configure a maximum of three counters. • Policy Counter Status – You can name this anything. • Lookahead Balance State –You can select one of the following: **FutureExpiry**, **FutureRefresh** and **FutureStart**. **Note** This state is the future balance event—quota expiration, quota refresh, or quota starting in the future. Based on the look-ahead time interval, if a balance state event is going to occur within the look-ahead interval period, then the pending policy counter status is populated in the SLA/SSNR messages.

Step 8 Select the **User Case Initiator** tab, and configure a use case initiator for this use case template.

An example is shown below:

Figure 172: Use Case Initiator



Use Case Option

Name: xyz-green

Service Initiators (OR Together)

Name
check 100%

Initiator Name: check 100%

Conditions (AND Together)

Name
An OCSThresholdStatus exists
An OCSThresholdStatus does not exist
An OCSThresholdStatus does not exist

Input Variables (AND Together)	Type	Operator	Value	
quotaCode (String)	Literal	=	xyz	Remove
thresholdCode (String)	Literal	=	green	Remove

Available Input Variables -

Add All

Add thresholdValue (BigDecimal) Add thresholdGroup (String)

Add nextRefreshDate (Date) Add thresholdCode (String)

Step 9 Configure a Service Option using the use case template.

Step 10 Configure a Service using the Service Option.

Loading Sy Session When Gy Session is From Different Realm

Sy and Gy calls originate from the same realm where SY OCS Server considers Gy as a secondary session. In such a call model, Gy CCR-I is ignored if the Gy CCR-I is received before Sy SLR the Gy CCR-I.

Sy and Gy calls can originate from different realms and Gy CCR-I needs to be handled even when Sy session is not present. In this scenario, both Gy and Sy sessions are independent of each other. Gy CCR-I can be received before Sy SLR and this needs to be handled.

You need to apply policy configuration to load an Sy session to a Gy session. The MSISDNkey and USuMSubscriberIdkey are used to correlate the Gy and Sy sessions.

Perform the following steps to load an Sy session to a Gy session:

Step 1 Log in to Policy Builder.

Step 2 Navigate to **Policies**.

Step 3 Load keys to Gy session and add the following two conditions to the policy configuration:

- A Diameter Gy v8 Session exists
- There exists an USuMSubscriber

Step 4 Under **Actions**, add the following keys:

- Add a MSISDNkey
- Add an USuMSubscriberIdKey

Step 5 To load Sy session, add the following conditions:

- A Diameter Gy v8 Session exists
- There exists a MsisdnKey
- There exists an USuMSubscriberIdKey
- An OCSThresholdBreach exists

Step 6 Under **Actions**, add the following key:

Retrieve a session from the cache

CHAPTER 11

Notification Services

Apple Push Notifications

Notification Configuration

To configure CPS to send a message to a subscriber with an Apple iPhone or other iOS device, perform the following steps.

Step 1 Log in to Policy Builder.

Step 2 Go to **Reference Data tab** > **Systems** > **a system or a cluster** > **Plugin Configurations** > **Notification Configuration**.

Step 3 Click the check box next to **Apple Push Notification Configuration**.

Step 4 View the **Notification Configuration** screen.

The following parameters can be configured under Apple Push Notification Configuration:

Table 161: Apple Push Notification Parameters

Parameter	Description
APNS Server Address	• Apple Production: Connects to gateway.push.apple.com on port 2195. • Apple Test: Connects to gateway.sandbox.push.apple.com on port 2195. • Other: Uses a server address other than the standard Apple ones. It also uses the other gateway and server port fields defined in Other Server Gateway and Other Server Port fields below. Other: Uses a server address other than the standard Apple ones. It also uses the other gateway and server port fields defined in Other Server Gateway and Other Server Port fields below. Recommendation: Other
Other Server Gateway	Name of a server gateway if Other is selected as APNS Server Address.
Other Server Port	Port number of the server gateway if Other is selected as APNS Server Address.
Certificate	The certificate for the authorization to the gateway. You must provide a certificate file that is loaded into CPS.
Certificate Password	Password added to the certificate when connecting to the APNS.

Step 5 Go to Message Configuration, on page 394 to configure the message to be sent for the notification configuration done above.

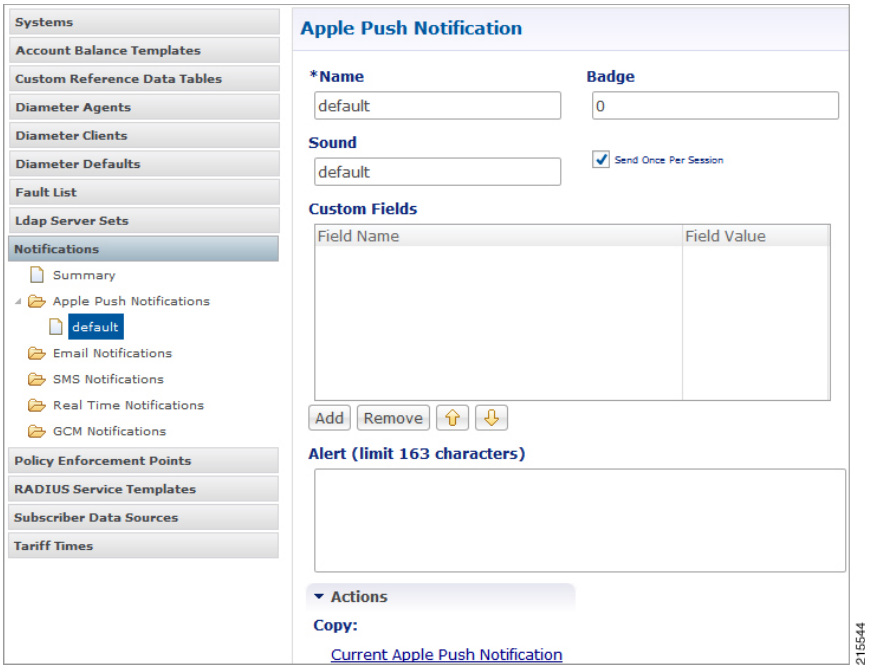
Message Configuration

To create the messages for a subscriber's Apple iPhone or the Apple iOS operating system to be sent by CPS, perform the following steps.

Step 1 Select **Reference Data tab** > **Notifications** > **Apple Push Notifications**.

Step 2 From right side, click **Apple Push Notification** under **Create Child** to open the pane.

Figure 173: Apple Push Notification Pane



Apple Push Notification

*Name: default

Badge: 0

Sound: default

☑ Send Once Per Session

Custom Fields

Field Name	Field Value

Alert (limit 163 characters)

The following parameters can be configured under Apple Push Notification:

Table 162: Apple Push Notification Message Configuration Parameters

Parameter	Description
Name	The name of the notification message. This name is used in the action phrase in the policy definition. Best practice is to make this short, but meaningful and unique.
Badge	Default is 0 (number). The number to display as the badge of the Apple Push Notification icon. If this property is absent, the badge is not changed. To remove the badge, set the value of this property to 0. Example: 1, 2, 3, ….
Sound	Default is 'default'. The name of a sound file in the application bundle. The sound in this file is played as an alert. If the sound file doesn't exist or default is specified as the value, the default alert sound is played. The audio must be in one of the audio data formats that are compatible with system sounds. For more information, see https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/IPhoneOSClientImp.html#//apple_ref/doc/uid/TP40008194-CH103-SW6. Example: sound1, alert7, buzzSound_A
Send Once Per Session	Click this check box if you want to send the notification once per session.
Custom Fields	You can add custom fields with values that can be sent to the application.

Parameter	Description
Field Name/Field Value	String Example: “high_score”: “1000” “custom_field_1”: “display1” “custom_field_2”: “false” For more information on custom fields, refer to the following links: • https://developer.apple.com/library/ios/documentation/networkinginternet/conceptual/remotenotificationspg/chapters/applepushservice.html • http://docs.appcelerator.com/platform/latest/#!/guide/Sending_and_Scheduling_Push_Notifications-section-43298780_SendingandSchedulingPushNotifications-CustomJSONpayloads
Alert	This is the text that appears on the subscriber’s iPhone. If the message is too long, it is simply truncated. Test your messages before you place into production. If you want to use a string, and substitute session information, use the syntax $Name, for example, to insert the receiver’s name in the email. Alerts are limited to 160 characters. Alerts longer than that are truncated.

To use Apple Push Notifications, you need to configure Service Options.

For more information on the configuration, see Service Option Configuration, on page 418.

Email Notifications

Configure Notifications

CPS supports sending email notifications to one primary and one secondary email server, or alternatively to a pool of email servers

(See Multiple Email Notification Configuration).

When configured for one primary and one secondary email server, CPS will send all email notifications to the primary server. If the primary fails, CPS will retry the notification to the secondary server, if configured. If the secondary server notification fails, CPS will log that the notification was unable to be delivered.

To configure the primary and secondary email server connections that CPS will use to send email notifications to subscribers:

Step 1 Login to Policy Builder.

Step 2 Go to **Reference Data** > **Systems** > ***a system or a cluster*** > **Plugin Configurations** > **Notification Configuration**.

Step 3 Click the check box next to **Email Notification Configuration**.

Step 4 View the **Notification Configuration** screen that drops down.

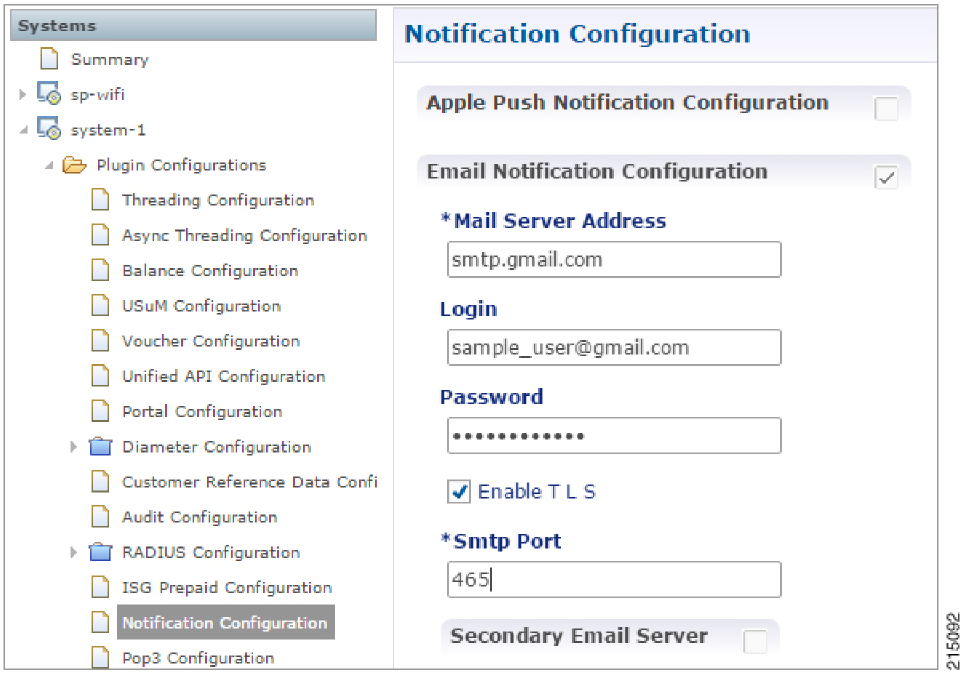
The following parameters can be configured under Email Notification Configuration:

Table 163: Email Notification Configuration Parameters

Parameter	Description
Mail Server Address	IP address or host name of the mail server to which the notification emails will be sent. Only IMAP email is supported at this time.
Login/Password	Enter any login and password information needed.
Enable TLS	Enables transport layer security. This option is used for connecting to services other than basic IMAP services, such as Google's Gmail.
Smtp Port	Specifies the SMTP port. This option is used for connecting to services other than basic IMAP services, such as Google's Gmail.

The following screen shows an example configuration using smtp.gmail.com.

Figure 174: Notification Configuration



Notification Configuration

Apple Push Notification Configuration □

Email Notification Configuration ☑

*Mail Server Address: smtp.gmail.com

Login: sample_user@gmail.com

Password: ••••••••••••

☑ Enable T L S

*Smtp Port: 465

Secondary Email Server □

Step 5 (Optional) To configure a secondary (backup) email server, click the check box next to **Secondary Email Server** and configure the parameters for the secondary server.

Step 6 Go to Configure Messages, on page 397 to configure the message to be sent for the notification configuration.

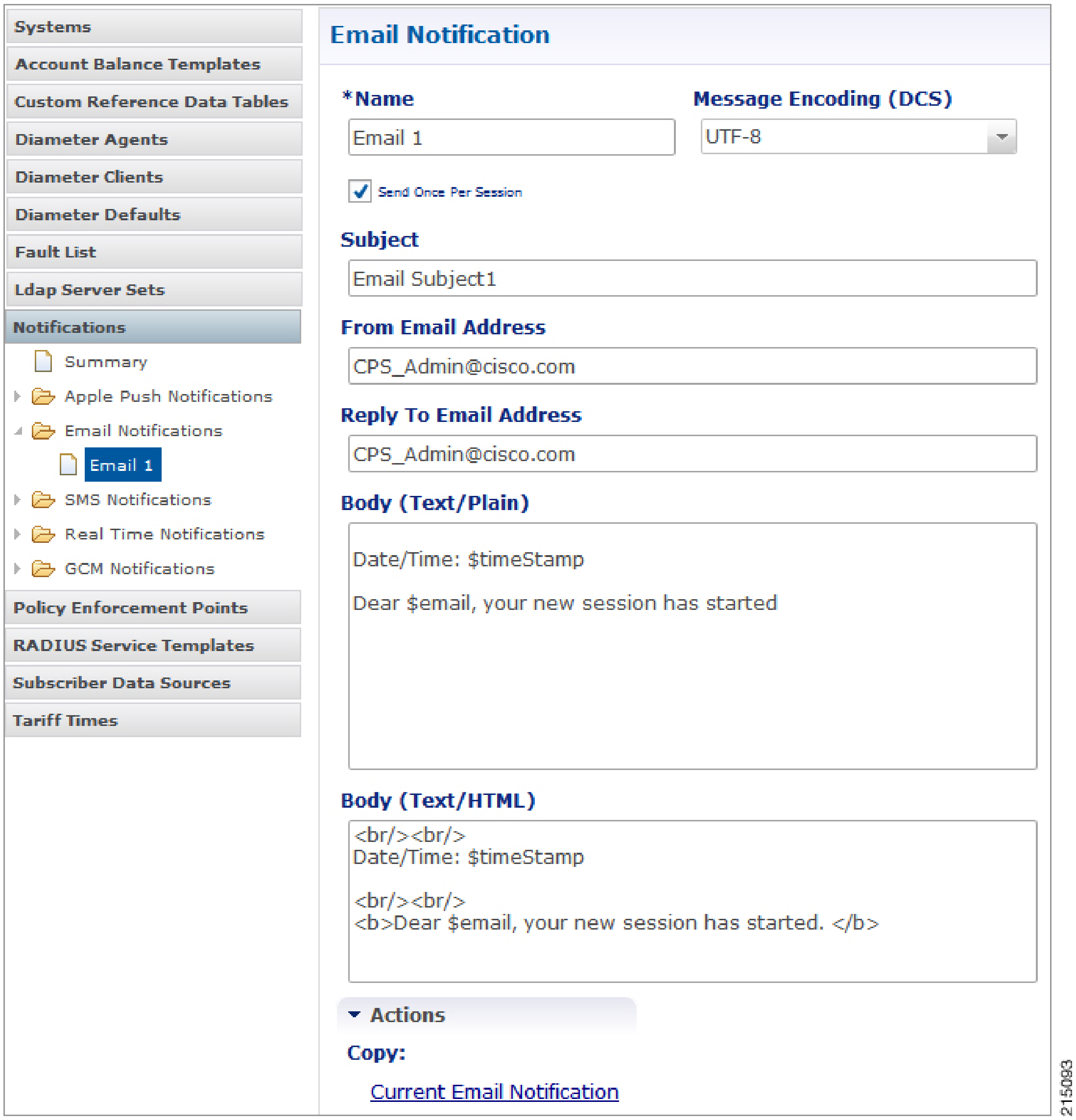
Configure Messages

Substitution value can be set from SPR, Balance, or the session and placed in the email body using $[variable].

In the following example, we are using a subscriber AVP code for email. The value "$email" is used in the body of the text and replaced then the email is sent.

We are also using $timeStamp to add the Date/Time.

Figure 175: Email Notification



Email Notification

*Name: Email 1

Message Encoding (DCS): UTF-8

☑ Send Once Per Session

Subject: Email Subject1

From Email Address: CPS_Admin@cisco.com

Reply To Email Address: CPS_Admin@cisco.com

Body (Text/Plain):

```
Date/Time: $timeStamp

Dear $email, your new session has started
```

Body (Text/HTML):

```
<br/><br/>
Date/Time: $timeStamp

<br/><br/>
<b>Dear $email, your new session has started. </b>
```

The following parameters can be configured under Email Notifications:

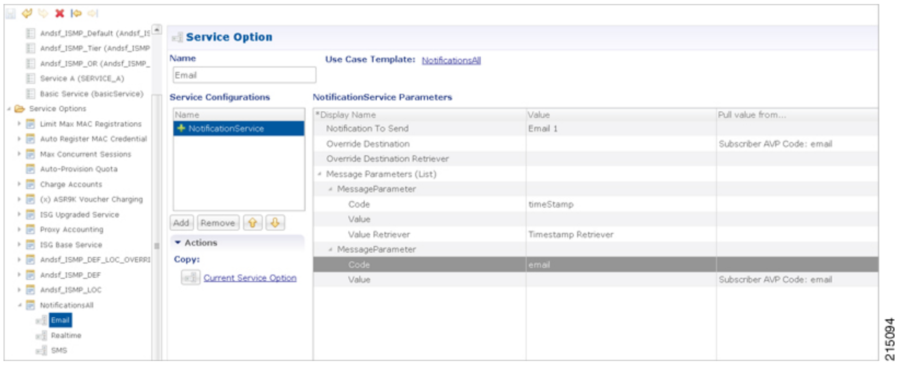
Table 164: Email Notification Message Configuration Parameters

Parameter	Description
Name	Name of the message.
Message Encoding (DCS)	Select the required message coding from drop-down list. Valid values are ISO-8859-1, US-ASCII, UTF-16 (UCS-2) and UTF-8. Default value is UTF-8.

Parameter	Description
Subject	This is the subject line of the email to the subscriber.
From Email Address	The From field in the email.
Reply To Email Address	Who the subscriber may reply to.
Body (Text/Plain)	The text of the email the subscriber receives in plain format
Body (Text/HTML)	The text of the email the subscriber receives in HTML format.

To pull the values from SPR and replace in the email, we use the service option setting from the notification:

Figure 176: Service Option



Service Option

Name: Email

Use Case Template: NotificationsAll

Service Configurations

Name
NotificationService

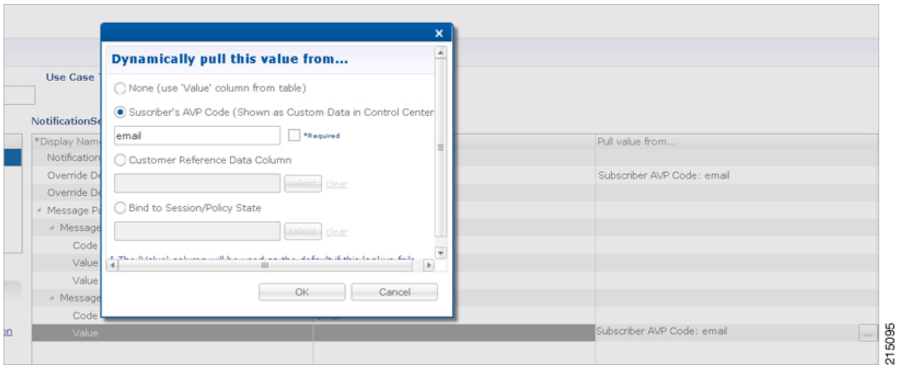
NotificationService Parameters

*Display Name	Value	Pull value from...
Notification To Send	Email 1	
Override Destination		Subscriber AVP Code: email
Override Destination Retriever		
Message Parameters (List)		
MessageParameter		
Code	timeStamp	
Value		
Value Retriever	Timestamp Retriever	
MessageParameter		
Code	email	
Value		Subscriber AVP Code: email

For the timestamp, use the Value Retriever.

For the email, select from the “Pull value from…” column.

Figure 177: Subscriber AVP code Email Values



Dynamically pull this value from...

○ None (use 'Value' column from table)

● Suscriber's AVP Code (Shown as Custom Data in Control Center

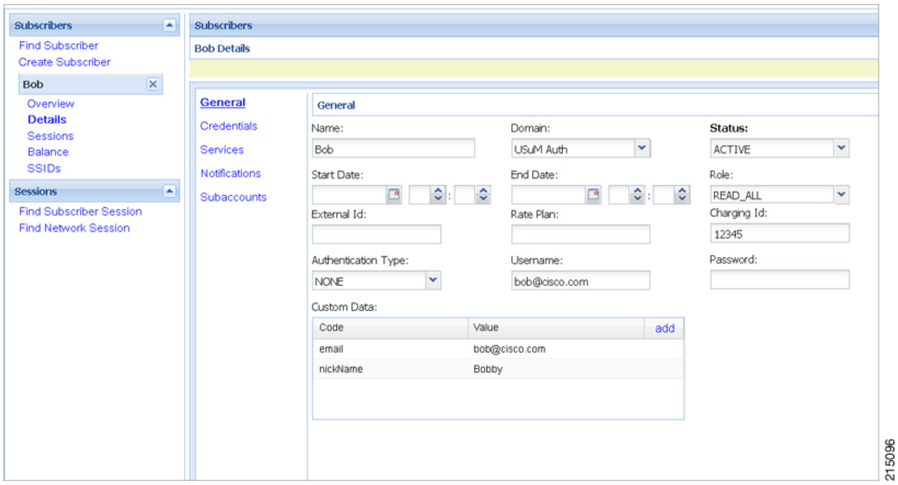
email □ *Required

○ Customer Reference Data Column

○ Bind to Session/Policy State

For reference, our subscriber has a Custom Data AVP set in the details of his subscriber record. This is where the value is being pulled from in Control Center.

Figure 178: Subscriber General Details



Name: Bob
Domain: USuM Auth
Status: ACTIVE
Start Date:
End Date:
Role: READ_ALL
External Id:
Rate Plan:
Charging Id: 12345
Authentication Type: NONE
Username: bob@cisco.com
Password:
Custom Data:

Code	Value
email	bob@cisco.com
nickName	Bobby

Logging

```
2015-05-01 14:34:46,345 [pool-2-thread-1] DEBUG c.b.n.impl.NotificationsManager.? - Email
encoding : UTF8
2015-05-01 14:34:46,345 [pool-2-thread-1] DEBUG c.b.n.impl.NotificationsManager.? - Email
Text body : Date/Time: 1430512486305
Dear bob@cisco.com, your new session has started
2015-05-01 14:34:46,345 [pool-2-thread-1] DEBUG c.b.n.impl.NotificationsManager.? - Email
HTML body : <br/><br/>
Date/Time: 1430512486305
<br/><br/>
<b>Dear bob@cisco.com, your new session has started.</b>
```

To use Email Notifications, we need to configure Service Options.

For more information on the configuration, refer to Service Option Configuration, on page 418.

Multiple Email Notification Configuration

Configure Notifications

This section describes how to configure CPS to send email notifications to multiple email servers.

When multiple email servers are configured, CPS utilizes a round-robin selection scheme to distribute the email notifications to subscribers. No weighting is used when selecting the email servers from the configured pool.

If CPS detects that the running status of an email server is DOWN, CPS will automatically skip this server and send the notifications to the next email server. If a message cannot be delivered by an email server, CPS will retry the same message to the next email server.

Note In a CPS High Availability deployment, where two Policy Director (load balancer) VMs (lb01 and lb02) are used, each Policy Director operates a separate notification service. As a result, email notifications are first balanced across each Policy Director, and then each Policy Director delivers the message to an email server in a round robin fashion. This can result in concurrent messages being delivered to the same email server.

The following SNMP Notifications (Alarms) are used to monitor these email server connections. Refer to *CPS SNMP and Alarms Guide*, Release 9.1.0 and prior releases or *CPS SNMP, Alarms and Clearing Procedures Guide*, Release 10.0.0 and later releases for more information.

- AllEmailNotificationServerDown
- AtLeastOneEmailNotificationServerUp
- EmailNotificationServerDown
- EmailNotificationServerUp

To generate the SNMP Notifications (alarms), you need to configure `-Dnotification.interface.monitor.emailserver=true` in `/etc/broadhop/qns.conf` file. After configuring the parameter, run the following commands:

```
/var/qps/install/current/scripts/build_all.sh
```

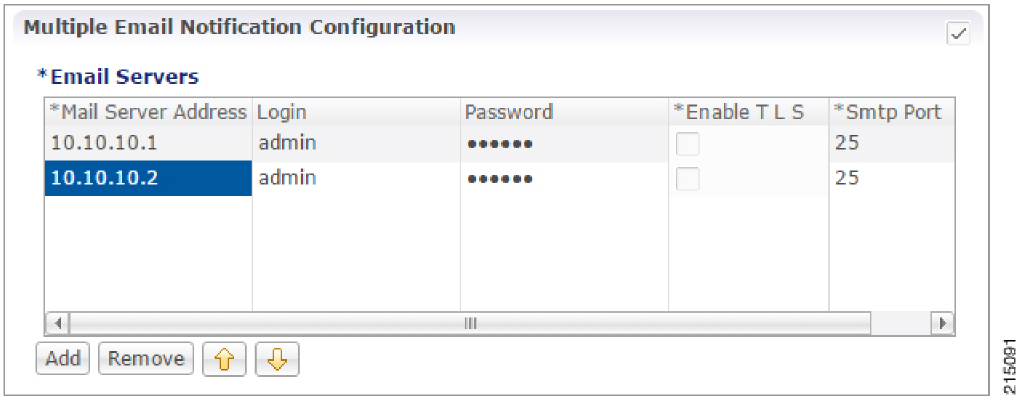
```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Note Before continuing with these steps to add a pool of email servers, first remove the Primary and Secondary servers configured under the Email Notification section of Policy Builder.

To configure a pool of email server connections that CPS uses to send email notifications to subscribers:

1. Login to Policy Builder.
2. Go to **Reference Data** > **Systems** > ***a system or a cluster*** > **Plugin Configurations** > **Notification Configuration**.
3. Click the check box next to **Multiple Email Notification Configuration**.
4. View the Notification Configuration screen that drops down.
5. Click **Add** to add an email server to the list.

Figure 179: Multiple Email Notification Configuration



Multiple Email Notification Configuration

*Email Servers

*Mail Server Address	Login	Password	*Enable T L S	*Smtp Port
10.10.10.1	admin	••••••	□	25
10.10.10.2	admin	••••••	□	25

Note Moving an entry up or down in the table reflects only the display order; it has no impact on the selection when processing email notifications.

The following parameters can be configured for each email server:

Table 165: Email Notification Configuration Parameters

Parameter	Description
Mail Server Address	IP address or host name of the mail server to which the notification emails will be sent. Only IMAP email is supported at this time.
Login/Password	Enter any login and password information needed.
Enable TLS	Enables transport layer security. This option is used for connecting to services other than basic IMAP services, such as Google's Gmail.
Smtp Port	Specifies the SMTP port. This option is used for connecting to services other than basic IMAP services, such as Google's Gmail.

6. Go to Configure Messages, to configure the message to be sent for the notification configuration.

SMS Notifications

Configure Notifications

CPS supports sending Short Message Service (SMS) notifications to one primary and one secondary SMSC server, or alternatively to a pool of SMSC servers.

See Multiple SMSC Server Configuration

The following section describes how to configure CPS to send SMS notifications to a primary SMSC server and a secondary SMSC server.

Step 1 Login to Policy Builder.

Step 2 Go to **Reference Data** > **Systems** > ***a system or a cluster*** > **Plugin Configurations** > **Notification Configuration** .

Step 3 Click the check box next to **SMS Notification Configuration**.

Step 4 View the Notification Configuration screen that drops down.

The following parameters can be configured under SMS Notification:

Table 166: SMS Notification Parameters

Parameter	Description
SMSC Host Address	The TCP/IP address or host name of the SMPP server, that is, the URL of the SMSC host that pushes the SMS message.
SMSC Port	The TCP/IP port on the SMPP server to which the gateway connects.
System ID	The user name for the gateway to use when connecting to the SMPP server
Password	The password for the gateway to use when connecting to the SMPP server.
System Type	An optional login parameter used only if required by the SMPP server. The SMPP system administrator provides this value, usually a short text string.
Registered Delivery	Optional field for some custom deployments.
DataCoding (Advanced Use Only)	Optional field for some custom deployments. Data Coding can be used instead of the Message Encoding and the other DCS fields on the Notification message definition screen, but should be used with care. **Note** If it is necessary to use a specific value in this field for data coding, then the message alphabet information should be included in the Data Coding value per the SMS specification as well as any other necessary data coding information. The result is a combination of the capabilities of the SMSC and is not totally controlled by CPS.
Priority Flag	Optional field for some custom deployments.
Binding Type	TX (transmit) or TRX (transceiver)

Parameter	Description
Enquire Link Time	Specifies the Enquire Link Timer value. The plug-in instance performs an Enquire Link operation to the SMSC to keep the connection alive. The time between inquiries is specified by this timer value. Default value is 5000 seconds.
Reconnect	If checked, CPS will check connection to the SMSC at the interval specified in the“Reconnect Smsc Time” field.
Reconnect Smsc Time	The interval to check the connection to the SMSC, and reconnect if lost. This will check the primary and secondary if the secondary properties are set.

Other then the parameters mentioned in Table 166: SMS Notification Parameters, on page 403, the user can configure the following parameters after selecting **Retry Configuration** check box.

The following parameters can be configured under Retry.

Table 167: Retry Parameters

Parameter	Description
No. Of Retries	Number of retries allowed to resubmit the message.
Retry Interval	Interval in which message are resubmitted until success.

Go to Configure Messages, to configure the SMS message to be sent for the notification configuration done above.

Configure Messages

To create the SMS to be sent by CPS, perform the following steps:

1. Select **Reference Data** > **Notifications** > **SMS Notifications**.
2. From right side, click **SMS Notification** under **Create Child** to open the pane.

   The following parameters can be configured under **SMS Notification**:

   Table 168: SMS Notification Parameters

Parameter	Description
Name	Name of the notification message. This name is used later in the policy definition to send the SMS.
Source Address	Source address of the SMS message.

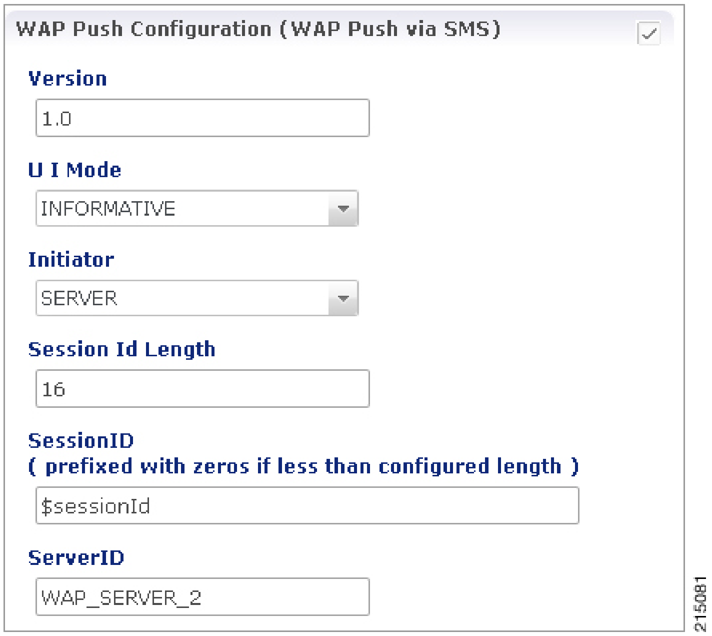
Parameter	Description
Callback Number	This is an optional field. This parameter is used to configure the callback number adhering to specification.The input format is a hexadecimal string. It will correspond to the exact hexadecimal sent in the stream. Currently, only a single callback number is supported. For more information, refer to SMS Notification Extension.
Address TON	Type of Number for the source. It defines the format of the phone numbers. Values: ABBREVIATED, ALPHANUMERIC, INTERNATIONAL, NATIONAL, NETWORK_SPECIFIC, SUBSCRIBER_NUMBER, UNKNOWN
Address NPI	Numbering Plan Indicator. It defines the format of the addresses. Values: DATA, ERMES, INTERNET, ISDN, LAND_MOBILE, NATIONAL, PRIVATE, TELEX, UNKNOWN, WAP
Message Class (DCS)	The message class per the SMPP specification. Valid values are CLASS0, CLASS1, CLASS2. Default value is CLASS1.
Message Encoding (DCS)	Defines the alphabet and byte encoding used for the message. Valid values are US-ASCII (7 bit), ISO-8859-1 (8 bit), and UTF-16 (UCS-2) which is 16 bit. Default value is US-ASCII.
Override Character Limit (Advanced)	Some SMSCs create multi-part messages for long SMS messages instead of having CPS create the multiple messages. This option provides such behavior by overriding the default single message size. This option is for advanced use only. The reason is that if space in the message submitted from CPS does not allow for header information, such as the User Data Header (UDH), then many SMSC are not accepted the messages at all.
Compressed (DCS)	Select this check box to set whether compression is used per the SMPP specification. Default is false.
Use Plugin Config Data Coding Instead (DCS	Select this check box when you want to use the value specified in Data Coding field in the Notifications Configuration screen instead of the Message Class, Message Encoding, Compressed, and Contain Message Class values on this screen.
Contain Message Class	Select this check box to set whether the contain message class options is used per the SMPP specification. Default is false.

Parameter	Description
Use Message Encoding with Plugin Config Data Coding	Select this check box when the “Use Plugin Config Data Coding Instead” check box above is checked. The check box "Use Plugin Config Data Coding Instead” must be true to use this value. This check box allows the Message Encoding value on this screen to define the byte conversion method that is used in conjunction with the Data Coding value in the Notifications Configuration screen. By default, the byte conversion method is US-ASCII regardless of the Plugin Configuration’s Data Coding value. Other UTF-16 conversions may use Big Endian, Little Endian or Byte Order Mark (BOM). This field is also important for ensuring the proper division of messages, particularly for non-English languages, for multi-part SMS message support.
Message	The text that the subscriber receives. SMS messages have character limits dependent on the selected DCS values. Text in excess of this limit triggers the submission of the multi-part messages to the SMSC.

WAP Settings

WAP push over SMS has been added to facilitate another way of initiation of notification from ANDSF server to the client (UE).

Figure 180: WAP Push Configuration



WAP Push Configuration (WAP Push via SMS) ☑

Version
1.0

U I Mode
INFORMATIVE

Initiator
SERVER

Session Id Length
16

SessionID
(prefixed with zeros if less than configured length)
$sessionId

ServerID
WAP_SERVER_2

The following parameters can be configured under **WAP Push Configuration**:

Table 169: WAP Push Configuration Parameters

Parameter	Description
Version	String, version of WAP message. This can be updated to reflect changes. For example, 1.0, 2.0, 2.1. No characters are allowed. Only numbers or '.' are allowed.
UI Mode	(User Interactive Mode): This field specifies the server recommendations whether the server wants the management session to be executed in background or show a notification to the user. Values: NOT_SPECIFIED, INFORMATIVE, BACKGROUND, USER_INTERACTION Default is NOT_SPECIFIED. • NOT_SPECIFIED: Specifies that the server doesn't have a recommendation to this element. • INFORMATIVE: Specifies that the server recommends the client to display an informative notification or maybe emitting a beep sound announcing the beginning of the provisioning session to the device user. • BACKGROUND: Specifies that the server recommends the management action SHOULD be done as a background event. • USER_INTERACTION: Specifies that the server recommends the client to prompt the device user for acceptance of the offered management session before the management session takes place.
Initiator	Specifies how the server has interpreted the initiation of the management action, either because the end user requested it or because the server has management actions to perform. Value from drop down is added to the WAP message and does not trigger any action on the CPS side. • Client: Specifies that the end user caused the device management session to start. • Server: Specifies that the server (operator, enterprise) caused the device management session to start.
Session Id Length	Integer - Up to 16
SessionID	Session Id is 16 bits which is 2 ASCII character according to the specification. However, there is no restriction on ANDSF session-id size, it can be of any length. In PB, session-id length is made configurable per notification template (Shown in snapshot above). When actual session id length is greater that the configured size then the notification would not be sent and an error would be logged. However, if session is less than the configured size, then zero would be prefixed in order to make sure that it satisfies session-id length configured in PB. It is assumed that the client would strip off the prefix and send the server initiated policy pull.

Parameter	Description
ServerID	String - Up to 255 Characters The field specifies the Server Identifier of the management server. For example, “Server_1”, “WAP_SERVER_2”

For more information on WAP fields, click WAP Fields.

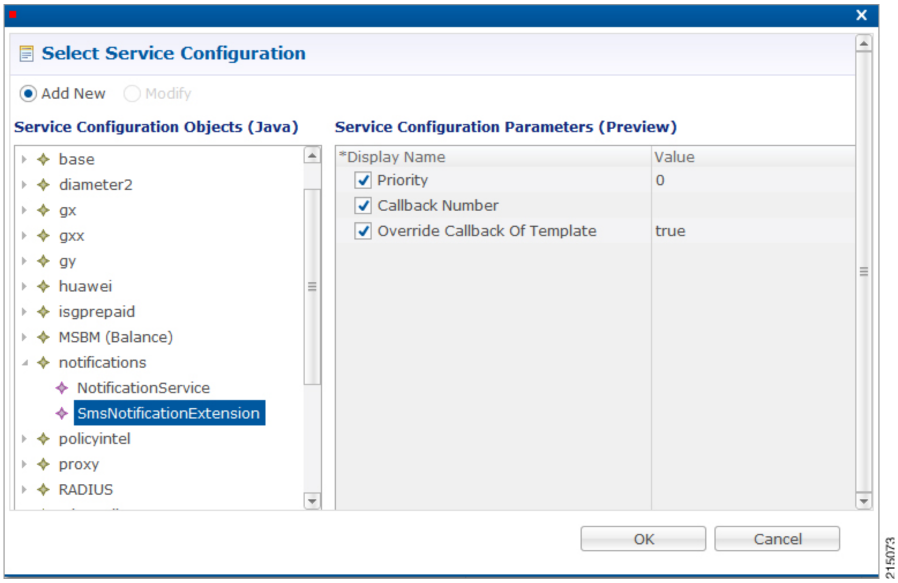
To use SMS Notifications, we need to configure **Service Options**.

For more information on the configuration, refer to Service Option Configuration, on page 418.

SMS Notification Extension

A new Service Configuration named as SmsNotificationExtension has been added. Note that since its an extension, it needs the base NotificationService also configured as a part of the main service for it to fetch the base template details. For example, an operator can specify their call-center number for subscribers to call back.

Figure 181: Select Service Configuration



Select Service Configuration

● Add New ○ Modify

*Display Name	Value
☑ Priority	0
☑ Callback Number	
☑ Override Callback Of Template	true

The following parameters are configured under **SmsNotificationExtension**:

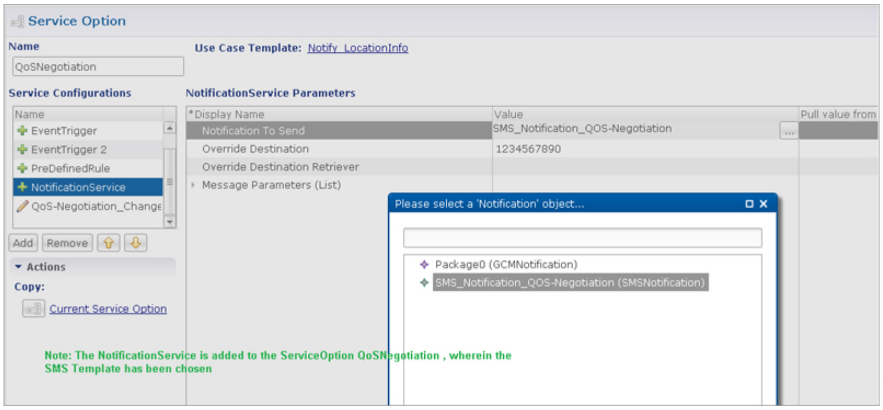
Table 170: SmsNotificationExtension Parameters

Parameter	Description
Priority	If there are multiple SMS Notification Extension configurations, this parameter will decide which Service configuration and corresponding parameter values to use. Higher the value, higher precedence it will have. For example, if there are two extension templates having priority as 1 and 2 each, the one with priority value 2 will be used. Default value is 0.

Parameter	Description
Callback Number	This is the service configuration level value for the callback number. This will satisfy the need of overriding the template value. **Note** Callback Number must be the exact hexadecimal string converted value of the call back number sent in the stream. Currently, only a single callback number is supported.
Override Callback Of Template	This parameter helps to decide whether to use the service configuration callback number to override the template or not. Default value is true.

Configure a service with the base Notification Service and select the SMS Notification Template.

Figure 182: Notification Object



Service Option

Name: QoSNegotiation

Use Case Template: Notify_LocationInfo

Service Configurations

Name
EventTrigger
EventTrigger 2
PreDefinedRule
NotificationService
QoS-Negotiation_Change

NotificationService Parameters

*Display Name	Value	Pull value from
Notification To Send	SMS_Notification_QOS-Negotiation	
Override Destination	1234567890	
Override Destination Retriever		
Message Parameters (List)		

Please select a 'Notification' object...

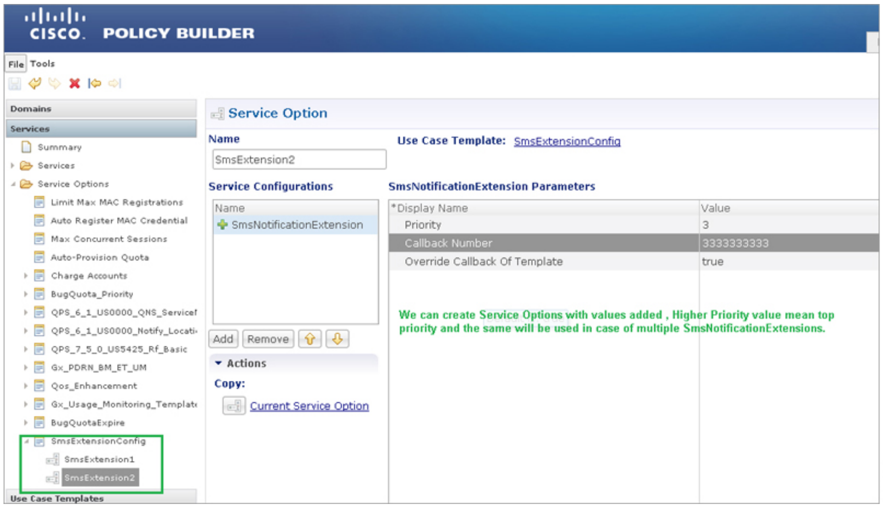
- Package0 (GCMNotification)
- SMS_Notification_QOS-Negotiation (SMSNotification)

Note: The NotificationService is added to the ServiceOption QoSNegotiation , wherein the SMS Template has been chosen

Create a Use Case Template using the new SMS Extension.

Add multiple extensions at service option level and configure the corresponding values.

Figure 183: SMS Extension Configuration



Service Option

Name: SmsExtension2

Use Case Template: SmsExtensionConfig

Service Configurations

Name
SmsNotificationExtension

SmsNotificationExtension Parameters

*Display Name	Value
Priority	3
Callback Number	3333333333
Override Callback Of Template	true

We can create Service Options with values added , Higher Priority value mean top priority and the same will be used in case of multiple SmsNotificationExtensions.

Configure a Service which has the NotificationService configured with corresponding SMS Template chosen and on top we can add the other SMSExtensions.

Multiple SMSC Server Configuration

Configure Notifications

This section describes how to configure CPS to send SMS notifications to multiple SMSC servers.

When multiple SMSC servers are configured, CPS utilizes a round-robin selection scheme to distribute the SMS notifications to subscribers. No weighting is used when selecting the SMSC servers from the configured pool.

If CPS detects that the running status of an SMSC server is DOWN, or if the SMSC server is marked disabled in the Policy Builder interface, CPS will automatically skip this server and send the messages to the next SMSC server. If a message cannot be sent to an SMSC server, CPS will retry to send it to the next SMSC server.

In the event that an SMSC server goes down, CPS can also be configured to reconnect to the server automatically. The frequency at which CPS will attempt to reconnect is also configurable.

Note In a CPS High Availability deployment, where two Policy Director (load balancer) VMs (lb01 and lb02) are used, each Policy Director operates a separate notification service. As a result, SMS notifications are first balanced across each Policy Director, and then each Policy Director delivers the message to an SMSC server in a round robin fashion. This can result in concurrent SMS messages being delivered to the same SMSC server.

The following SNMP Notifications (Alarms) have been introduced to monitor the SMSC server connections. Refer to *CPS SNMP and Alarms Guide*, Release 9.1.0 and prior releases or *CPS SNMP, Alarms and Clearing Procedures Guide*, Release 10.0.0 and later releases for more information.

- AllSMSCNotificationServerDown
- AtLeastOneSMSCNotificationServerUp
- SMSCNotificationServerDown
- SMSCNotificationServerUp

Note Before continuing with these steps to add a pool of SMSC servers, first remove the Primary and Secondary servers configured under the SMS Notification Configuration section of Policy Builder.

To configure CPS to send SMS notifications to a pool of SMSC servers:

1. Login to Policy Builder.
2. Go to **Reference Data** > **Systems** > ***a system or a cluster*** > **Plugin Configurations** > **Notification Configuration**.

3. Click the check box next to **Multiple SMSC Server Configuration**.
4. View the Notification Configuration screen that drops down.
5. Click **Add** to add an SMSC server to the list.

Note Moving an entry up or down in the table reflects only the display order; it has no impact on the selection when processing SMS notifications.

The following parameters can be configured for each SMSC server:

Table 171: SMSC Server Parameters

Parameter	Description
Admin Status	This field allows the operator to disable a specific SMSC server without removing the configuration entirely. If a server is disabled, CPS will not send any SMS notifications to it.
SMSC Host Address	The TCP/IP address or host name of the SMPP server, that is, the URL of the SMSC host that pushes the SMS message.
SMSC Port	The TCP/IP port on the SMPP server to which the gateway connects.
Binding Type	TX (transmit) or TRX (transceiver)
System ID	The user name to use when connecting to the SMSC server
Password	The password to use when connecting to the SMSC server.
Enquire Link Time	Specifies the time between Enquiry Link operations in seconds. CPS performs an Enquire Link operation to the SMSC server to keep the connection alive. Default: 5000 seconds.
System Type	An optional login parameter used only if required by the SMSC server. The SMSC system administrator provides this value, usually a short text string.
Registered Delivery	Optional field for some custom deployments.
DataCoding	Optional field for some custom deployments.
	Data Coding can be used instead of the Message Encoding and the other DCS fields on the Notification message definition screen, but should be used with care. **Note** If it is necessary to use a specific value in this field for data coding, then the message alphabet information should be included in the Data Coding value per the SMS specification as well as any other necessary data coding information. The result is a combination of the capabilities of the SMSC and is not totally controlled by CPS.

Parameter	Description
Priority Flag	Optional field for some custom deployments.
Reconnect SMSC SMS	If checked, CPS will attempt to reconnect to an SMSC server if the connection was lost or server was down.
Reconnect SMSC Timer (seconds)	The interval in which CPS will attempt to reconnect to the SMSC server. Default: 300 seconds

Refer to Configure Messages, to configure the SMS message to be sent for the notification configuration done above.

Real Time Notifications

Real time Notifications allows you to send SOAP/XML and REST/JSON messages to a defined server when policy thresholds are breached. The information related to real time notification is provided in the following feature files:

- For HA Setup:

  In `/etc/broadhop/pb/features`:

  - com.broadhop.client.feature.notifications

  In `/etc/broadhop/pcrf/features`:

  - com.broadhop.notifications.local.feature

  In `/etc/broadhop/iomanager/features`:

  - com.broadhop.notifications.realtime.service.feature
  - com.broadhop.notifications.service.feature

If the VMs are already deployed, after modifying the feature files, execute the following commands:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Configure Notifications

Note The number of real time notifications depends on the number of RAR generated by the Policy Server (QNS) VM. If you need to increase the number of realtime notification, Max Timer T P S (under **Cluster** in Policy Builder) value has to be tuned accordingly. For more information, contact your Cisco Account representative.

CPS doesn't support configurations to trigger multiple real time notifications for multiple threshold breaches occurring at the same time.

Step 1 Log in to Policy Builder.

Step 2 Go to **Reference Data** > **Systems** > ***a system or a cluster*** > **Plugin Configurations** > **Notification Configuration**.

Step 3 Click the check box next to **Realtime Notification Configuration**.

Step 4 View the Notification Configuration screen that drops down.

The following parameters can be configured under Realtime Notification Configuration.

Table 172: Realtime Notification Configuration Parameters

Parameter	Description
Failed Notifications Directory	File system path where failed notifications are stored. So when CPS is not able to send notification on both Server URL and Server Fallback URL then that notification is stored in this path. The path to the failed notifications directory needs to be created manually on Policy Directors (load balancers) (lb01 and lb02).
Max Storage allowed for failed Notifications (in MB)	Maximum size up to which CPS can store failed notifications in the failed notifications directory.

Go to Configure Messages, on page 413, to configure the realtime notification message to be sent for the notification configuration done above.

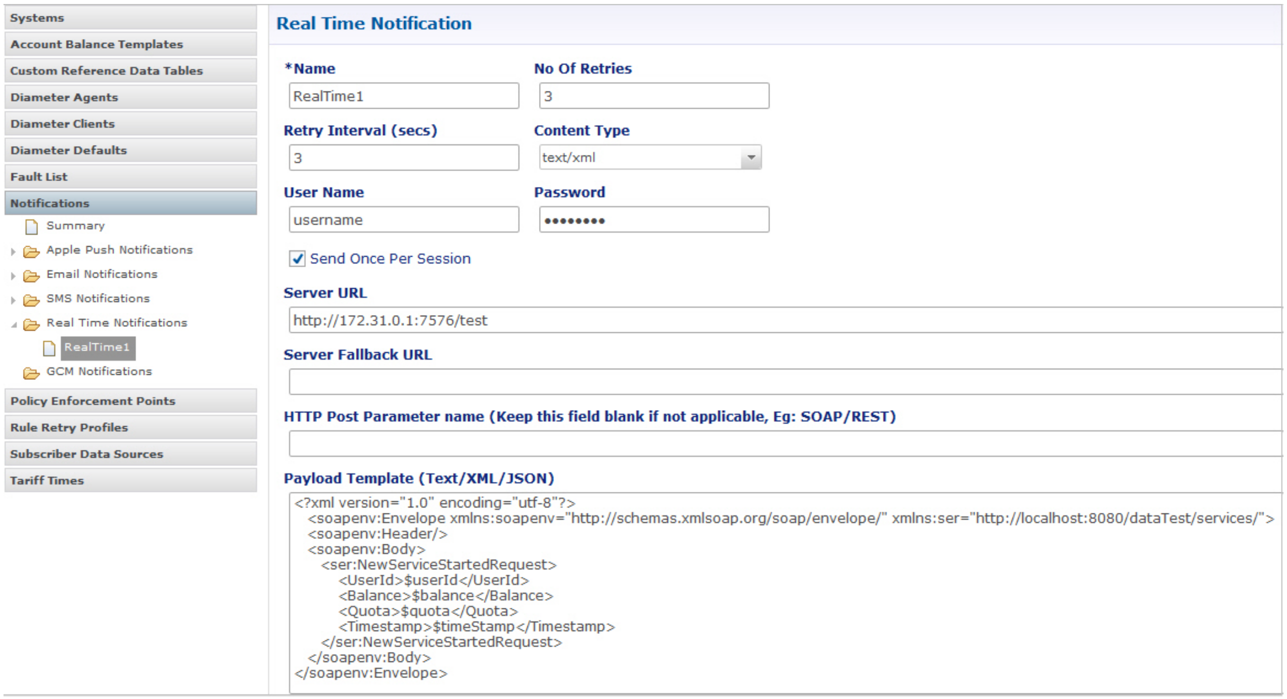
Configure Messages

To create the realtime notification to be sent by CPS, perform the following steps:

Step 1 Select **Reference Data** > **Notifications** > **Real Time Notifications**.

Step 2 On the right-hand-side panel, click **Real Time Notification** under **Create Child** to open the Notifications pane.

Figure 184: Real Time Notifications



Real Time Notification

*Name: RealTime1

No Of Retries: 3

Retry Interval (secs): 3

Content Type: text/xml

User Name: username

Password: ●●●●●●●●

☑ Send Once Per Session

Server URL: http://172.31.0.1:7576/test

Server Fallback URL:

HTTP Post Parameter name (Keep this field blank if not applicable, Eg: SOAP/REST):

Payload Template (Text/XML/JSON)

```
<?xml version="1.0" encoding="utf-8"?>
  <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ser="http://localhost:8080/dataTest/services/">
  <soapenv:Header/>
  <soapenv:Body>
    <ser:NewServiceStartedRequest>
      <UserId>$userId</UserId>
      <Balance>$balance</Balance>
      <Quota>$quota</Quota>
      <Timestamp>$timeStamp</Timestamp>
    </ser:NewServiceStartedRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

The following parameters can be configured under Real Time Notifications:

Table 173: Real Time Notifications Parameters

Parameter	Description
Name	Name of the real-time notification message.
No of Retries	When CPS sends real-time notification to the provided Server URL and if it is not reachable then this field specifies how many times CPS should send the notification. Same is true for Server Fallback URL. Default value is 3.
Retry Interval (secs)	The time to wait between retries configured in the **No of Retries** field. Default value is 3.
Content Type	The content type is set based on the type of the payload template (Text/XML/JSON). You can select the following: • text/xml • application/json • application/x-www-form-urlencoded The content type that you choose must match the template in the **Payload Template** field. The default value is text/xml.

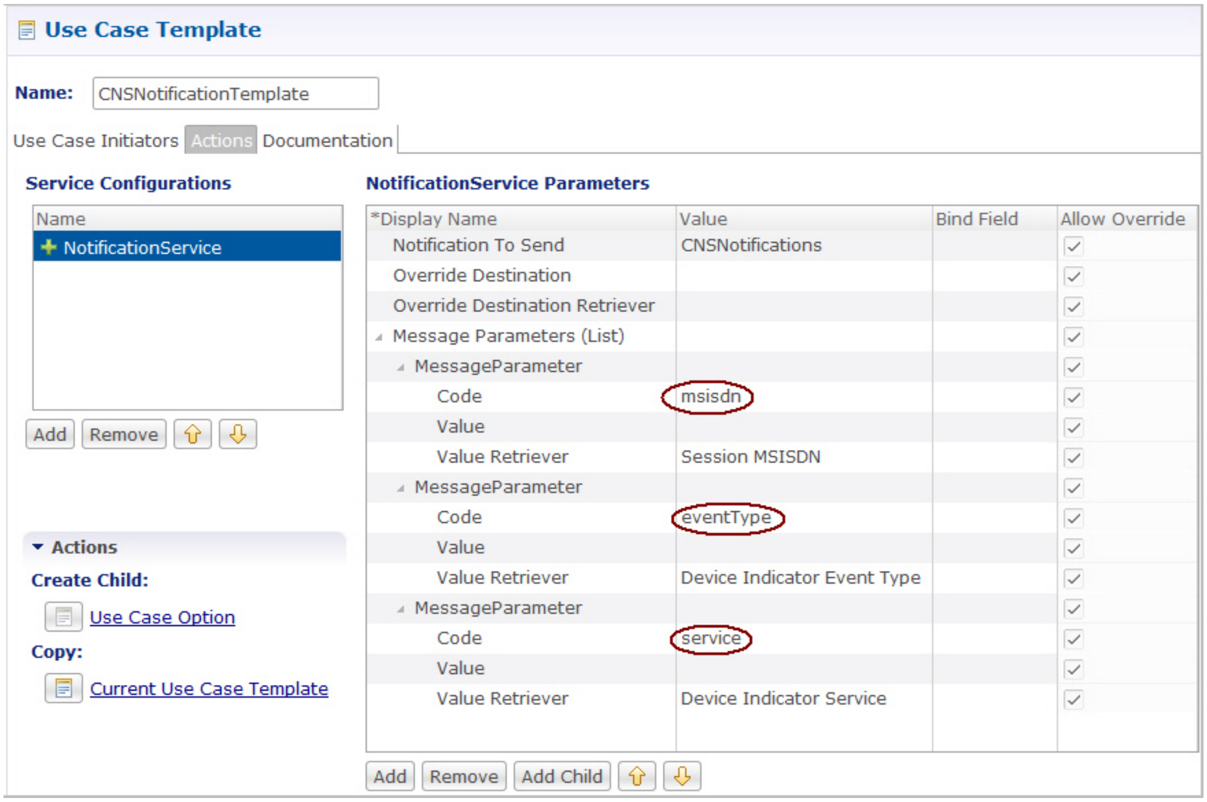
Parameter	Description
User Name	The user name for accessing the endpoint specified in the **Server URL** and **Server Fallback URL** fields. If no user name is required, leave this field blank.
Password	The password for accessing the endpoint specified in the **Server URL** and **Server Fallback URL** fields. If no password is required, leave this field blank.
Send Once Per Session	If checked, real-time notifications are generated for each session and not for all messages within that session. Default value is true.
Server URL	Primary URL where CPS sends real-time notifications.
Server Fallback URL	When the Primary URL is not reachable, CPS tries to send notification to this URL for the configured **No of Retries**. When the number of retries are exhausted, CPS tries to send notification to the Server Fallback URL.
HTTP Post Parameter name (Keep this field if not applicable, Eg: SOAP)	For SOAP this field is not applicable and hence should be blank. This field specifies the HTTP Post parameter name.
Payload Template (Text/XML/JSON)	This field contains the payload template, so real-time notifications are generated using the configured template. CPS provides values to the fields specified in the template from the ongoing session. For all fields that are specified in the template with values found, the real-time notification is generated. The names of the variables/placeholders defined here must match with the notification service parameter codes defined in service parameters of the corresponding use case template. You should also ensure that the correct value retriever is selected for each notification service parameter code in the use case template.

The following example shows a JSON payload template for reference only.

```
{
  "notifications": [
     {
        "ctn_id": "$msisdn",
        "eventType":"$eventType",
        "eventData":{
           "services":["$service"]
        }
     }
  ]
}
```

Configure the NotificationService parameters in a use case template that pertains to the JSON example above.

Figure 185: NotificationService Parameter Configuration for JSON Example



Name: CNSNotificationTemplate

Name
NotificationService

*Display Name	Value	Bind Field	Allow Override
Notification To Send	CNSNotifications		☑
Override Destination			☑
Override Destination Retriever			☑
Message Parameters (List)			☑
MessageParameter			☑
Code	msisdn		☑
Value			☑
Value Retriever	Session MSISDN		☑
MessageParameter			☑
Code	eventType		☑
Value			☑
Value Retriever	Device Indicator Event Type		☑
MessageParameter			☑
Code	service		☑
Value			☑
Value Retriever	Device Indicator Service		☑

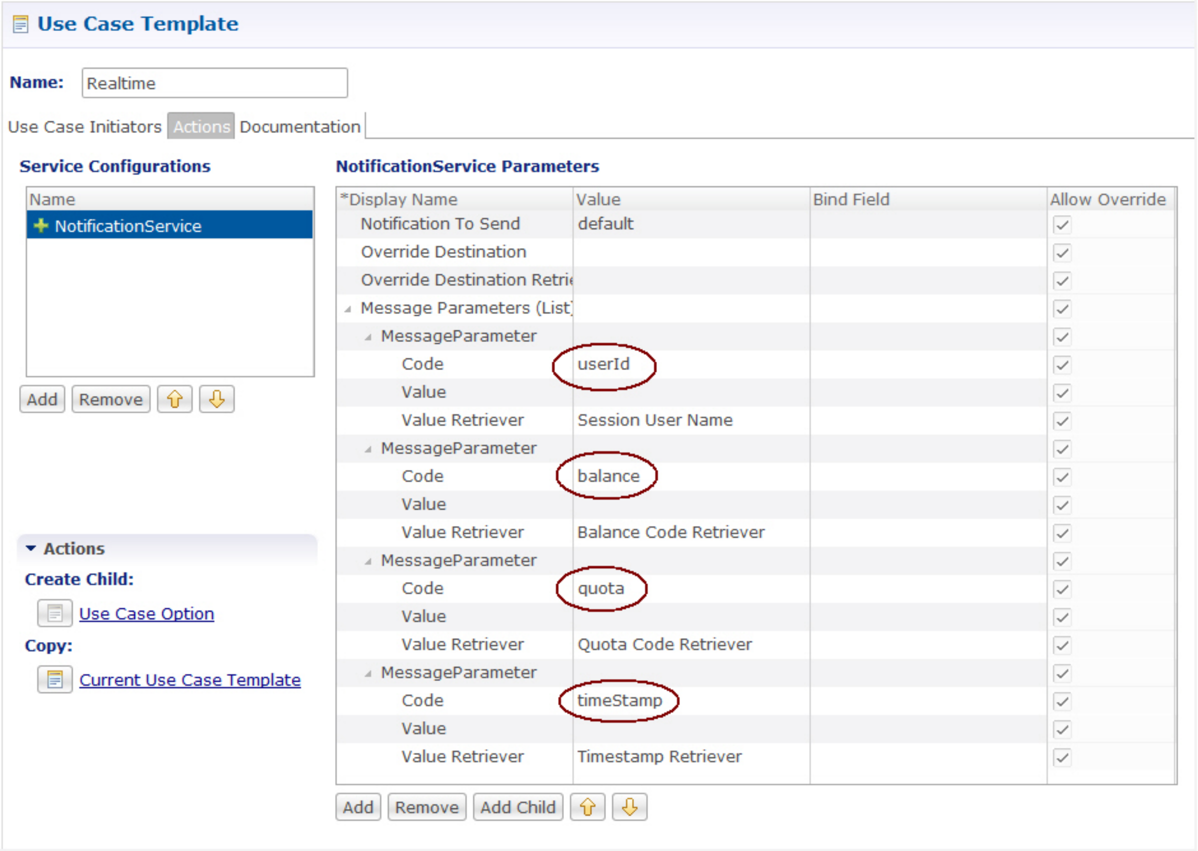
- The `$msisdn`, `$eventType`, and `$service` notifications in the JSON example are added as **Code** values under **Message Parameters**.
- These values are pulled using the **Value Retriever** for each message parameter. Use the select box provided in each **Value Retriever** field to select the retrievers.
  - For *Code* type eventType, the **Value Retriever** is Device Indicator Event Type which allows the retrieval of event type. This is currently hard-coded to QoS_Change.
  - For *Code* type service, the **Value Retriever** is Device Indicator Service which allows retrieval of service status (ON or OFF).
- For the **Notification To Send** parameter, select the Real Time Notification you want from the list.

The following example shows an XML payload template for reference only.

```
<?xml version="1.0" encoding="utf-8"?>
    <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://localhost:8080/dataTest/services/">
    <soapenv:Header/>
    <soapenv:Body>
        <ser:NewServiceStartedRequest>
           <UserId>$userId</UserId>
           <Balance>$balance</Balance>
           <Quota>$quota</Quota>
           <Timestamp>$timeStamp</Timestamp>
       </ser:NewServiceStartedRequest>
    </soapenv:Body>
</soapenv:Envelope>
```

Configure the NotificationService parameters in a use case template that pertains to the XML example above.

Figure 186: NotificationService Parameter Configuration for XML Example



Use Case Template

Name: Realtime

Use Case Initiators | Actions | Documentation

Service Configurations

Name
NotificationService

Actions

Create Child: Use Case Option

Copy: Current Use Case Template

NotificationService Parameters

*Display Name	Value	Bind Field	Allow Override
Notification To Send	default		✓
Override Destination			✓
Override Destination Retri			✓
Message Parameters (List)			✓
MessageParameter			✓
Code	userId		✓
Value			✓
Value Retriever	Session User Name		✓
MessageParameter			✓
Code	balance		✓
Value			✓
Value Retriever	Balance Code Retriever		✓
MessageParameter			✓
Code	quota		✓
Value			✓
Value Retriever	Quota Code Retriever		✓
MessageParameter			✓
Code	timeStamp		✓
Value			✓
Value Retriever	Timestamp Retriever		✓

- Adding substitute values into the message body.

  To substitute any value into your message, add the character '$' to the beginning of the variable name. For example, $userName.

  The XML Template example contains the `$userId`, `$balance`, `$quota`, and `$timeStamp` variables, which we will replace with values from the session and post to the Server URL defined in the Notifications Plugin.

- The Server URL is the destination of the message, and this is not set as an attribute of the subscriber like the other notifications.

- **Notification To Send:** Select the Real Time Notification you want from the list.

Message Parameters (using the example XML payload template):

- userId: This value is pulled using the Session User Name Retriever. Use the select box from the Value Retriever field.

- balance: This value is pulled using the Balance Code Retriever. Use the select box from the Value Retriever field.

- quota: This value is pulled using the Balance Code Retriever. Use the select box from the Value Retriever field.

- timestamp: This value is pulled using the Timestamp Retriever. Use the select box from the Value Retriever field.

For more information on service options, refer to Service Option Configuration, on page 418.

Service Option Configuration

This section provides an example Service Options configuration which can be used for SMS, EMAIL, Apple Push, and GMC notifications. The bodies of the messages are identical to make the service options parameters simpler to follow.

Adding substitute values into the message body

To substitute any value into your message, add the character '$' to the beginning of the variable name. For example, Ex. $userName.

This set of substitute variables are used as an example for SMS, EMAIL, Apple Push, and GCM.

- $timeStamp
- $userId
- $nickName

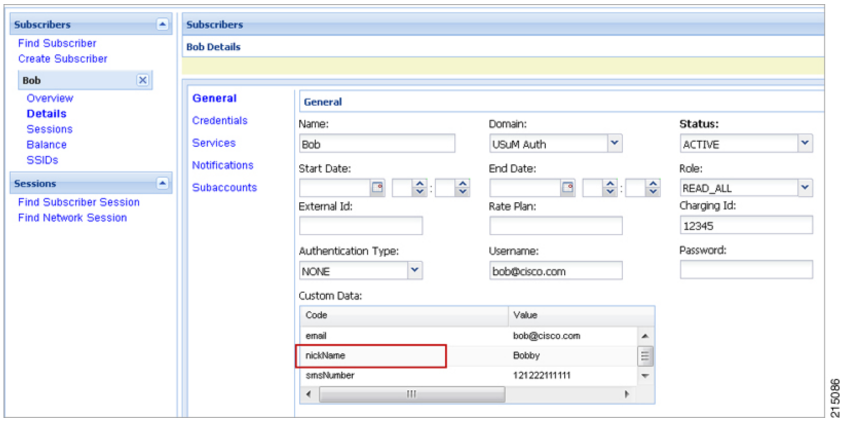
You assign the variables their value using the Notification Service Parameters.

There are four values provide for the example configuration:

- Notification To Send: Select the Notification you want from the list.
- Timestamp: This value is pulled using Timestamp Retriever. Use the select box from the Value Retriever field.
- userId: This value is pulled using Session User Name Retriever. Use the select box from the Value Retriever field.
- Nickname: We are filling this value using the Subscriber AVP Code action, pulling from the Custom Data attached to the subscriber. You can see these values in the Control Center.

  nickName example: Custom AVP in the Control Center

Figure 187: nickName Configuration



Name: Bob	Domain: USuM Auth	Status: ACTIVE
Start Date:	End Date:	Role: READ_ALL
External Id:	Rate Plan:	Charging Id: 12345
Authentication Type: NONE	Username: bob@cisco.com	Password:

Custom Data:

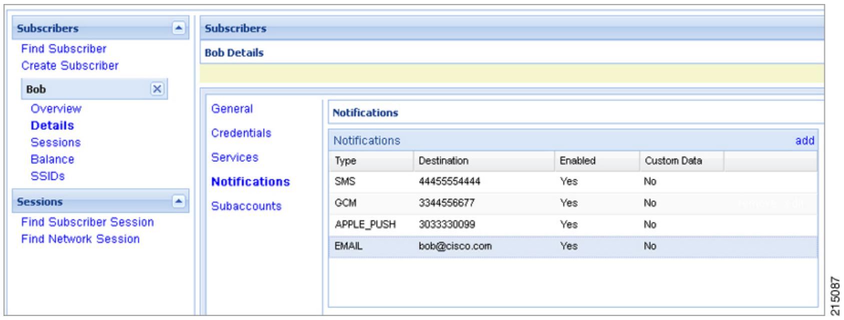
Code	Value
email	bob@cisco.com
nickName	Bobby
smsNumber	121222111111

Apple Push Notification Destination

By default, this notification will go the Destination set in the Notifications section under the subscriber details for the type of Notification being sent.

For example, an Apple Push message will go to Apple Push Destination, and SMS to SMS, and so on.

Figure 188: Notification Destinations



Type	Destination	Enabled	Custom Data
SMS	44455554444	Yes	No
GCM	3344556677	Yes	No
APPLE_PUSH	3033330099	Yes	No
EMAIL	bob@cisco.com	Yes	No

To override the destination set for the subscriber, you can use the **Override Destination** field in the Service Option.

NAP Notification

CPS is enhanced to support decoding of the URL sent from the LDAP/NAP server.

Create (Payload):

```
%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-
8%22+standalone%3D%22yes%22%3F%3E%3CCustomerTransactions%3E%3CCustomerTransaction%3E%3
CTransactionInfo%3E%3CRequestedAction%3Ecreate%3C%2FRequestedAction%3E%3CCustomerID%3E
200569444%3C%2FCustomerID%3E%3Cmsisdn%3E4047047821%3C%2Fmsisdn%3E%3CVersion%3E1.4%3C%2
FVersion%3E%3CTransactionID%3E5153654875871906187%3C%2FTransactionID%3E%3CVendorID%3E5
3%3C%2FVendorID%3E%3C%2FTransactionInfo%3E%3CAccountInfo%3E%3CCustomerID%3E200569444%3
C%2FCustomerID%3E%3Cmsisdn%3E4047047821%3C%2Fmsisdn%3E%3Cimsi%3E310260399339533%3C%2Fi
msi%3E%3Cban%3E932945358%3C%2Fban%3E%3CaccountType%3EI%3C%2FaccountType%3E%3CaccountSu
```

```
bType%3ER%3C%2FaccountSubType%3E%3CbillCyclePeriod%3E14%3C%2FbillCyclePeriod%3E%3CStat
usCode%3EA%3C%2FStatusCode%3E%3CCustomerType%3E1%3C%2FCustomerType%3E%3CPAHmsisdn%3E40
47047821%3C%2FPAHmsisdn%3E%3CLanguage%3Eeng%3C%2FLanguage%3E%3CPairingFlag%3E1%3C%2FPa
iringFlag%3E%3C%2FAccountInfo%3E%3CServiceInfo%3E%3CVendorID%3E53%3C%2FVendorID%3E%3CF
eatures%3E%3CFeature%3E%3CName%3EB52ROAM%3C%2FName%3E%3C%2FFeature%3E%3C%2FFeatures%3E
%3C%2FServiceInfo%3E%3C%2FCustomerTransaction%3E%3C%2FCustomerTransactions%3E
```

After URL Decoding:

```
<?xml+version="1.0"+encoding="UTF-
8"+standalone="yes"?><CustomerTransactions><CustomerTransaction><TransactionInfo><Requ
estedAction>create</RequestedAction><CustomerID>200569444</CustomerID><msisdn>40470478
21</msisdn><Version>1.4</Version><TransactionID>5153654875871906187</TransactionID><Ve
ndorID>53</VendorID></TransactionInfo><AccountInfo><CustomerID>200569444</CustomerID><
msisdn>4047047821</msisdn><imsi>310260399339533</imsi><ban>932945358</ban><accountType
>I</accountType><accountSubType>R</accountSubType><billCyclePeriod>14</billCyclePeriod
><StatusCode>A</StatusCode><CustomerType>1</CustomerType><PAHmsisdn>4047047821</PAHmsi
sdn><Language>eng</Language><PairingFlag>1</PairingFlag></AccountInfo><ServiceInfo><Ve
ndorID>53</VendorID><Features><Feature><Name>B52ROAM</Name></Feature></Features></Serv
iceInfo></CustomerTransaction></CustomerTransactions>
```

The schema for such NAP notifications is not defined in a XSD but is a free flowing XML as defined by NAP. CPS has adapted its parsing code to ensure the entire XML is received and processed although only IMSI, service level and prepaid flag are submitted to the policy engine as LDAP change event message from the servlet.

CHAPTER 12

Service Configuration Objects

diameter2 Configuration Objects

RequestReject

RequestReject service configuration can be used to send an error code to reject a session during initial attach or update when certain condition (such as, APN-RAT combination) is met.

Note The RequestReject service configuration functionality remains the same whether the policy configuration is CRD based or not.

For explanation purposes, CRD based functionality is described in this section.

This configuration has two attributes, ErrorCode and IsExperimentalErrorCode and values to these two attributes gets populated using result column of STG (output columns of CRD).

Note Error-Code is a Number type column and IsExpermentalErrorCode is a Boolean type column.

CRD table gets evaluated with retrievers/request bindings (such as, APN, RAT-TYPE, Cmd-Code, application-id, Request-Type) done at CRD level and gives ErrorCode and IsExperimentalErrorCode as derived output. Based on this ErrorCode, CPS sends the response message. If no Error-Code is derived, then CPS behaves normally.

CPS logs a counter for each request rejection. For this a new statistics, *<InterfaceName>_<RequestType>_policy_driven_rejection_<ResultCode>* has been added.

Table 174: RequestReject Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Error Code	Value of this field is pulled from the CRD output column which is of type **Number** (need to configure pull value from column to map to a result column of the CRD table), which represents the error code that needs to be sent in response. Default value of Error Code is 0. **Note** If application detects an error and decides to reject the request, the Error Code value configured in the service configuration object takes precedence over any other Result-Code that the application would have normally sent (for example, DIAMETER_UNKNOWN_SESSION_ID (5002), DIAMETER_PENDING_TRANSACTION (4144)).
Is Experimental Error Code	Value of this field is pulled from the CRD output column which is of type **Boolean** (need to configure pull value from column to map to a result column of the CRD table), which represents how CPS has to send the Error Code in response either through Result-Code AVP or 'Experimental-Result-Code' grouped AVP. Default value is false that means CPS sends an error code in response through Result-Code AVP.

ResetDiameterSession

ResetDiameterSession service configuration is used to release the primary Gx session of the subscriber when primary Gx session has released all the other secondary sessions gracefully.

Table 175: ResetDiameterSession Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Protocol	Currently, GX_TGPP is the only protocol supported. **Note** You can configure other interfaces but they are not supported by CPS.

Parameter	Description
Release Cause	Reason for aborting Gx session. Default value is UNSPECIFIED_REASON(0). The following release causes are supported: • Default: UNSPECIFIED_REASON(0) • UE_SUBSCRIPTION_REASON(1) • INSUFFICIENT_SERVER_RESOURCES(2) • IP_CAN_SESSION_TERMINATION(3) • UE_IP_ADDRESS_RELEASE(4)

Gx Service Configuration Objects

ActionBasedOnGxEventTrigger

The ActionBasedOnGxEventTrigger service configuration object allows CPS to make policy decisions based on the following event triggers received over Gx:

- OUT_OF_CREDIT
- REALLOCATION_OF_CREDIT
- CREDIT_MANAGEMENT_SESSION_FAILURE
- CISCO_EVENT_TRIGGER

Table 176: ActionBasedOnGxEventTrigger Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	

Parameter	Description
Event Trigger Stg	StgNameReferencePair: • Stg Name (Optional): This can be left blank • Stg Reference (Mandatory): This is the reference to the CRD table • List Of Input Column Avp Pairs (Mandatory): Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name: The name of the Diameter AVP that is used as input for CRD table evaluation. Supported values are Cisco-CC-Failure-Type, Charging-Rule-Name, and Rule-Failure-Code. • Column: The reference to the CRD column for the input AVP. • List Of Output Column Avp Pairs (Mandatory): Defines the mapping between the AVP Names and the output columns defined in the selected STG. These mappings indicate how the output columns' values are mapped to AVPs after the CRD is evaluated. • Avp Name: The name of the Diameter AVP to which the value of the output column is mapped. Supported values are Remove-Rx-Rule, Terminate-Session, and Reinitiate-Session. • Column: The reference to the CRD column for the output AVP.

ActionOnDefaultBearerQoSChange

Table 177: RxAppQoSInformation Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Collapse Dedicated Bearer	If this value is set to true, then on Default Bearer QoS uplift, a check is done to see if any of the existing dedicated bearers have the same QoS as the uplifted QoS (specifically same QCI and ARP). CPS then installs those rules and flows on the default bearer associated with existing dedicated bearer. This is due to the fact that PGW removes the dedicated bearer when QCI and ARP matches with the default bearer. With the removal of the dedicated bearer all the flows and rules associated with that bearers are removed.
Evaluate Static Rules	Reserved for future use.
Evaluate Qo S Group Rules	Reserved for future use.

ADTMAttributeStagePriority

ADTMAttributeStagePriority configuration object is used to provide stage and priority values for the Active Traffic Management (ADTM) attribute.

The following table describes the service configuration parameters:

Table 178: ADTMAttributeStagePriority Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.
Input Column Binding (List)	Input parameters in terms of CRD column name and mapped AVP Code. ColumnAndAvpPair • Avp Name: Supported custom input AVP names are: • Message: This represents the incoming or outgoing message type. Supported values are CCR-I, CCA-I, GX-RAR and RX-AAR. • APNString: This represents the existing active APNs for the subscriber. Various names are separated by colon in an alphabetical order. For example, Hotspot:IMS:SOS are in alphabetical order. • APNCount: APN count is the total count of existing active APNs for the subscriber. • Column: The key column in the STG that corresponds to the specified AVP.
Priority Level	CRD table output column having the priority value. Value can be any positive integer. 0 is an invalid value. The maximum value is based on the bit length configured under Attribute Encode Table in Policy Builder. Lesser the number higher the priority. There is no default value.
Stage	CRD table output column having Stage column value. These is the stage column valid value present in Stage table under Attribute Encoding Table in Policy Builder. Valid value is any string.

ADTMIMSServiceAction

ADTMIMSServiceAction configuration object is used to define IMS service action.

The following table describes the service configuration parameters:

Table 179: ADTMIMSServiceAction Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.
Input Column Binding (List)	Input parameters in terms of CRD column name and mapped AVP Code. ColumnAndAvpPair • Avp Name: Supported custom input AVP names are: • Stage: Stage value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the stage of the incoming call which leads to deletion or pause of the existing bearer. • Priority: Priority value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteLogicalApn: APN value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the APN priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteFrontEndId: Front End Id value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the front end ID of the incoming call which leads to deletion or pause of the existing bearer. • MPS-Identifier: MPS identifier of the existing Rx session. • Reservation-Priority: Reservation priority of the existing Rx session. • MCPTT-Identifier: MCPTT identifier of the existing Rx session. • Media-Type: Media Type of the existing Rx session. • Column: The key column in the STG that corresponds to the specified AVP.

Parameter	Description
Priority Level	CRD table output column having the priority value. Value can be any positive integer. 0 is an invalid value. The maximum value is based on the bit length configured under Attribute Encode Table in Policy Builder. Lesser the number higher the priority. There is no default value.
Action	CRD table output column for the action value. Valid values are DELETE and PAUSE. Configuring DELETE results in removal of the rules from gateway and termination on Rx. Currently, PAUSE is not supported for IMS service. There is no default value.

ADTMMogServiceAction

ADTMMogServiceAction configuration object is used to define MOG service action.

The following table describes the service configuration parameters:

Table 180: ADTMMogServiceAction Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.

Parameter	Description
Input Column Binding (List)	Input parameters in terms of CRD column name and mapped AVP Code. ColumnAndAvpPair • Avp Name: Supported input AVP names are: • Stage: Stage value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the stage of the incoming call which leads to deletion or pause of the existing bearer. • Priority: Priority value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteLogicalApn: APN value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the APN priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteFrontEndId: Front End Id value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the front end ID of the incoming call which leads to deletion or pause of the existing bearer. • Service-Info-Status: Service Info Status of the existing Rx session. • Sponsor-Identity: Sponsor Identity of the existing Rx session. • DPCC-Name: DPCC Name of the existing Rx session. • DPCC-Value: DPCC Value of the existing Rx session. • Intention: Intent of the existing Rx session. • Media-Type: Media Type of the existing Rx session. • Column: The key column in the STG that corresponds to the specified AVP.
Priority Level	CRD table output column having the priority value. Value can be any positive integer. 0 is an invalid value. The maximum value is based on the bit length configured under Attribute Encode Table in Policy Builder. Lesser the number higher the priority. There is no default value.

Parameter	Description
Action	CRD table output column for the action value. Valid values are DELETE and PAUSE. Configuring DELETE results in rule removal or QoS reversal and termination on Rx Configuring PAUSE results in rule removal or QoS reversal at gateway but no termination on Rx. The rules are re-installed or QoS is re-installed when the PAUSE condition is gone. There is no default value.

ADTMSDServiceAction

ADTMSDServiceAction configuration object is used to define TDF Sd service action.

The following table describes the service configuration parameters:

Table 181: ADTMSDServiceAction Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.

Parameter	Description
Input Column Binding (List)	Input parameters in terms of CRD column name and mapped AVP Code. ColumnAndAvpPair • Avp Name: Supported custom input AVP names are: • Stage: Stage value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the stage of the incoming call which leads to deletion or pause of the existing bearer. • Priority: Priority value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteLogicalApn: APN value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the APN priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteFrontEndId: Front End Id value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the front end ID of the incoming call which leads to deletion or pause of the existing bearer. • TDF-App-Id: TDF application identifier of the existing Sd detected application. • Sponsor-Id: Sponsor identity of the existing Sd detected application. • Column: The key column in the STG that corresponds to the specified AVP.
Priority Level	CRD table output column having the priority value. Value can be any positive integer. 0 is an invalid value. The maximum value is based on the bit length configured under Attribute Encode Table in Policy Builder. Lesser the number higher the priority. There is no default value.
Action	CRD table output column for the action value. Valid values are DELETE and PAUSE. When custom muting is enabled and PAUSE is configured, all the services are moved to default bearer and are custom muted. Configuring DELETE removes the services from the gateway. There is no default value.

ADTMSPRBearerAction

ADTMSPRBearerAction configuration object is used to define SPR Bearer service action.

The following table describes the service configuration parameters:

Table 182: ADTMSPRBearerAction Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.
Input Column Binding (List)	Input parameters in terms of CRD column name and mapped AVP Code. ColumnAndAvpPair • Avp Name: Supported input AVP names are: • Stage: Stage value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the stage of the incoming call which leads to deletion or pause of the existing bearer. • Priority: Priority value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteLogicalApn: APN value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the APN priority of the incoming call which leads to deletion or pause of the existing bearer. • RemoteFrontEndId: Front End Id value as received in Active Traffic Management (ADTM) Attribute notification from UDC FE. This is the front end ID of the incoming call which leads to deletion or pause of the existing bearer. • Attribute-Name: Name of the existing subscriber attribute. • Attribute-Value: Value of the same existing subscriber attribute. • Column: The key column in the STG that corresponds to the specified AVP.
Priority Level	CRD table output column having the priority value. Value can be any positive integer. 0 is an invalid value. The maximum value is based on the bit length configured under Attribute Encode Table in Policy Builder. Lesser the number higher the priority. There is no default value.

Parameter	Description
Action	CRD table output column for the action value. Valid values are DELETE and PAUSE. When DELETE is configured, SPR attributes does not participate in the policy evaluation. When PAUSE is configured, SPR attribute does not participate in policy evaluation until PAUSE condition is valid. There is no default value.

ApnMapping

The ApnMapping service configuration object pushes the configured Target APN in a CCA-I message by matching the incoming APN in a CCR-I message with the configured source APN.

Table 183: ApnMapping Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Source APN	The APN that will be mapped to the target APN.
Target APN	The APN that will be the used instead of the source APN.

BandwidthMonitor

The BandwidthMonitor service configuration object grants PCEF a specified amount/dosage and records the timestamp when it was granted.

Table 184: BandwidthMonitor Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Name	Any name can be specified.
Reporting Timeout	The number of minutes used to set the Revalidation-Time AVP so that the subscriber has a chance to get unthrottled before the allocated dosage is used.

Parameter	Description
Monitoring Key	BaseUsageMonitoringKey For detailed descriptions of these parameters, see Common Parameter Descriptions, on page 508. • Encoding Format • Monitoring Key • Dosage • Monitoring Level • Enabled
Bandwidth Threshold (List)	BandwidthThresthold • Lower Value – The minimum bandwidth value (in kbps) that you can specify for the corresponding Label. This value should be an integer. When the computed bandwidth used is greater than this value, the corresponding Label is set to the subscriber for the particular application identified by the Name option. • Label – The name of the label, which depends upon user requirements.

BearerControlMode

The BearerControlMode service configuration object sets the Bearer Control Mode to the specified value. If you do not specify a value, the value is derived. This value overwrites any previously specified value.

Table 185: BearerControlMode Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Mode Type	The type of mode that is being set explicitly.

CcGroup

The CcGroup service configuration object is used with entitlement to specify which credit-control-group the session should be associated with.

Note This configuration object requires custom properties be enabled in the qns.conf file.

Table 186: CcGroup Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Name	The name of the CC-Group value to be assigned to the user's session.

ChargingInformation

The ChargingInformation service configuration object sets the session charging information to the specified value.

Table 187: ChargingInformation Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Online	
Offline	
Primary O C S	The primary Online Charging System to be used.
Secondary O C S	The secondary Online Charging System to be used.
Primary O F C S	The primary Offline Charging System to be used.
Secondary O F C S	The secondary Offline Charging System to be used.

CiscoContentFilteringPolicy

The goal of Content Filtering is to provide support for content filtering within the network by use of Policy IDs. Policy identifiers (Policy IDs) are rules that are configured on the ASR 5000 platform and invoked by the CPS. Policy IDs are used to implement the required Content Filtering policies defined for the subscriber. The Policy IDs are selected at the ASR 5000 by provisioning their values through the Gx interface by the PCRF.

When a user initiates a session, the ASR5K communicates with the CPS to initialize the defined policies. CPS provides the Policy ID to the ASR5K to provide the necessary Content Filtering services for the user.

The primary purpose of this feature is for CPS to provide Policy IDs configured in the subscriber's service to the PCEF (ASR5K).

Table 188: CiscoContentFilteringPolicy Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Cisco Content Filtering Policy	The name of the policy being applied by this configuration.

CiscoEventTriggerType

The CiscoEventTriggerType service configuration object allows CPS to arm Cisco Custom event to get notified whenever a Gy failure occurs at PCEF. For arming event, 5 is sent and for disarming, 0 is sent.

- 0 - NO_CISCO_EVENT_TRIGGERS
- 5 - CREDIT_CONTROL_FAILURE

Table 189: CiscoEventTriggerType Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Event Trigger	

CiscoOverrideControl

CPS supports Override-Control specific AVPs in CCA-i and CCA-u responses to the PCEF on the Gx Interface and Gx RAR message. These AVPs are used to override charging parameters for predefined and static rules on the PCEF.

Table 190: CiscoOverrideControl Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Override Rule (List)	Specifies the name of the rule (predefined or static) for which override values are sent.
Override Charging Action Exclude Rule (List)	Exclude Rule – Defines the rule name where the override will not be applied. • Rule Name – the name of the rule to be excluded.

Parameter	Description
Override Service Identifier	Used to override the value of Service Identifier configured in the charging action.
Override Rating Group	Defines the value of the rating group configured for a static/predefined rule.
Override Reporting Level	Used to override the value of reporting level configured in the charging action.
Override Online	See Common Parameter Descriptions, on page 508.
Override Offline	
Override Metering Method	Used to override the value of Metering Method configured in the charging action.
Override QoS	Used to Override QoS-Information for a predefined rule or charging action.
Override-Max-Requested-Bandwidth-UL	Defines the maximum bit rate allowed for the uplink direction.
Override-Max-Requested-Bandwidth-DL	Defines the maximum bit rate allowed for the downlink direction.
Override-Guaranteed-Bitrate-UL	Defines the guaranteed bit rate allowed for Uplink direction. This AVP should be included only for rules on dedicated bearers.
Override-Guaranteed-Bitrate-DL	Defines the guaranteed bit rate allowed for downlink direction. This AVP should be included only for rules on dedicated bearers.
Override-Allocation-Retention-Priority	Used to override the pre-configured value of ARP.
Override Merge Wildcard	Used to merge override control charging/policy parameters between override control with specific charging action and wildcard override control.

CiscoQosGroupRule

The CiscoQosGroupRule service configuration object defines QoS Group Rules (and their sub-rules), on which CRD Driven rules depend.

Table 191: CiscoQosGroupRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	

Parameter	Description
Qos Group Rule Name	The name of the QoS group rule to which the policy is being applied.
Flow Status	See Common Parameter Descriptions, on page 508.
Encoding Format	
Monitoring Key	
Redirect Server	RedirectServer • Address Type • Server Type
Cisco Qos Information	CiscoQoSInformation For detailed information about these parameters, see Common Parameter Descriptions, on page 508. • Qci • Max Req Bandwidth U L • Max Req Bandwidth D L • Guaranteed Bit Rate U L • Guaranteed Bit Rate D L • APN Agg Max Bit Rate U L • APN Agg Max Bit Rate D L • Arp

CSGReporting

The CSG-Information-Reporting AVP is sent from the PCRF to the PCEF to request the PCEF to report the user CSG information change to the OFCS.

Table 192: CSGReporting Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
CSG-Information-Reporting AVP value	AVP values are 0, 1, or 2. 0 = CHANGE_CSG_CELL 1 = CHANGE_CSG_SUBSCRIBED_HYBRID_CELL 2 = CHANGE_CSG_UNSUBSCRIBED_HYBRID_CELL

DefaultBearerQoS

The DefaultBearerQoS service configuration object configures the QoS attributes for the default bearer.

Table 193: DefaultBearerQoS Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508
Diameter Client	
Qci	
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guarnateed Bit Rate D L	
Apn Agg Max Bit Rate U L	
Apn Agg Max Bit Rate D L	
Arp	
ConditionalApnAggregateMaxBitrate	Stores values corresponding to the Conditional-APN-Agg-Max-Bitrate grouped AVP.

DefaultBearerQoSActions

The DefaultBearerQoSActions service configuration object sets the values for the various DBQ Attributes based on Policy or the configured DBQ object. There are three types of DefaultBearerQoSActions:

- Mirror: The value requested is granted.
- Enforce: (Default) The default bearer qos value is granted.
- Bound: A min between the two is granted.

Table 194: DefaultBearerQoSActions Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508
Diameter Client	
Qci	
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guarnateed Bit Rate D L	
Apn Agg Max Bit Rate U L	
Apn Agg Max Bit Rate D L	
Arp	

DefaultBearerQciArpOverride

The DefaultBearerQciArpOverride service configuration object is used to override the calculated default bearer Qci and ARP attributes.

Table 195: DefaultBearerQciArpOverride Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508
Diameter Client	
Qci	
Allocation Retention Priority	
Priority Level	Priority Level AVP value.
Preemption Capability	Pre-emption Capability AVP value.
Preemption Vulnerability	Pre-emption Vulnerability AVP value.

DelayBearerCreation

The DelayBearerCreation service configuration object is used to decide whether to delay the bearer creation or not. Delay value can be configured in the service (or) can be pulled from CRD. Using this configuration CPS holds the CCA-I and Gx-RAR messages for the configured delay time. This service configuration gets added to policy state based on specific use case initiators.

Table 196: DelayBearerCreation Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508
Diameter Client	
Default Bearer Delay In Milliseconds	Based on this value CPS initiates delay timer for holding the CCA-I message. Default value is zero which indicates that there is no delay.
Dedicated Bearer Delay In Milliseconds	Based on this value CPS initiates delay timer for holding the Gx-RAR message. Default value is zero which indicates that there is no delay.

DetectedAppDefaultBearerQos

The DetectedAppDefaultBearerQos service configuration object is used to apply the Default Bearer QoS based on the TDF-Application-Identifier received in Sd CCR-U and Gx CCR-U. This can be used for both Gx and Sd detected applications.

Table 197: DetectedAppDefaultBearerQos Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Name of the CRD table used in the service configuration.
Apply Prev Applied T D F Id Qos	By default, the value is set to false that indicates CPS considers QoS derived from Rx and default bearer QoS service for missing QoS attributes. If set to true, CPS considers QoS derived from previously applied TDF ID QoS for missing QoS attributes.
Input Column Binding (List)	Input parameters in terms of CRD column name and mapped AVP Code. Supported AVP code is TDF-Application-Identifier.
Output Column Binding (List)	Output parameters in terms of CRD column name and mapped AVP Code. Supported AVP codes are: QoS-Class-Identifier, Priority-Level, Preemption Capability, Preemption Vulnerability, APN-Aggregate-Max-Bitrate-UL, APN-Aggregate-Max-Bitrate-DL, Max-Requested-Bandwidth-UL, Max-Requested-Bandwidth-DL, Guaranteed-Bitrate-UL, and Guaranteed-Bitrate-DL.

DetectedAppPriorityDeafaultBearerQoS

The DetectedAppPriorityDeafaultBearerQoS to populate 'Priority' and 'CC-Time' by taking TDF-Application-Identifier as input. This can be used for both Gx and Sd detected applications.

Table 198: DetectedAppPriorityDeafaultBearerQoS Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Default T D F App Id Priority	When default value for the TDF Id is not configured, CPS considers this by default value is -1, which takes high precedence and if multiple TDF-APP-Id`s does not have priority then both will have same priority then CPS may not process in order so behavior would vary every time CPS evaluate this table.
Default C C Time In Seconds	Default CC-Time when not received in Sd_CCR-U.
Stg Name	Name of the CRD table used in this service configuration.
List Of Input Column Avp Pairs (List)	Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name - The name of the AVP that is used as input for CRD table evaluation. Supported value is TDF-Application-Identifier. • Column - The reference to the CRD column for the input AVP.
TDF App Id priority Column	Priority Configured for TDF-Application-Identifier.
C C Time Output Column	CC-Time Configured for the TDF-Application-Identifier.

Note

- TDF Application Identifier must be unique.
- Priority must be mandatory and it should be unique.

DynamicTrafficSteering

The DynamicTrafficSteering service configuration object is not used.

EMPS

The EMPS (Enhanced Multimedia Priority System) service configuration object defines the MPS EPS Priority MPS Priority Level and IMS Signaling Priority level. This is required for Always on MPS.

Table 199: EMPS Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Mps Eps Priority Enabled	When selected, invokes the Priority EPS Service. • 1: Enable • 0: Disable
Mps Priority Level	Indicates the priority level (Integer range 1-15).
Ims Signaling Priority	IMS signaling priority level (Integer range 1-15).

EventTrigger

The EventTrigger service configuration object specifies the event to be sent.

Table 200: EventTrigger Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Event Trigger	

EventTrigger 48

The PresenceReportingAreaConfiguration service configuration object indicates the maximum number of PRA identifiers supported.

Table 201: EventTrigger 48 Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Event Trigger	Indicates value of the event trigger.

GxDynamicRuleReference

The GxDynamicRuleReference configuration object is used only when the ADC (Application Detection & Control) Feature is enabled at PCEF and new dynamic rules need to be installed over the Gx interface based on Application Detection on the Gx interface by the PCEF.

Table 202: GxDynamicRuleReference Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
STG Table	The name of the Search Table group table that is being referenced.
List Of Input Column Avp Paris (List)	See Common Parameter Descriptions, on page 508.
List Of Output Column Avp Paris (List)	
Retry Pcc Rules On Failure	Can be set to true or false. Default: false

IntermediateRulesParamOnFailure

The IntermediateRulesParamOnFailure service configuration is used to send Flow-Status, Rating-Group, Service-Id when Retry Profile is configured with interval.

The following table describes the service configuration parameters:

Table 203: IntermediateRulesParamOnFailure Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD table. This is a mandatory parameter.
List of Input Column Avp Pairs (List)	Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name – The name of the AVP that is used as input for CRD table evaluation. Supported values are Charging-Rule-Name, Rule-Failure-Code, Cisco-CC-Failure-Type, TDF-Application-Identifier, Application-Service-Provider-Identity, DPCC-Name, DPCC-Value, AF-Application-Identifier, and Sponsor-Identity. • Column – The reference to the CRD column for the input AVP.

Parameter	Description
List of Output Column Avp Pairs (List)	List of Output AVPs for the CRD. • Avp Name – The name of the AVP that is used as input for CRD table evaluation. Supported values are Service-Identifier, Rating-Group, Flow-Status, Online, Offline, Metering-Method, Reporting-Level, Precedence, Redirect-Support, Redirect-Address-Type and Redirect-Server-Address. • Column – The reference to the CRD column for the output AVP.

MaxQos

The MaxQoS service configuration object authorizes the requested QoS against the maximum-allowed QoS.

Table 204: MaxQoS Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Qci	
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guaranteed Bit Rate D L	
Apn Agg Max Bit Rate U L	
Apn Agg Max Bit Rate D L	
Arp	

ModifyChargingRules

Table 205: ModifyChargingRules Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD tables that define the Qos Action.

Parameter	Description
List Of Input Column Avp Pairs (List)	Defines the mapping between the 'AVP Names' and the key 'Columns' defined in the selected STG. These AVPs will be the inputs while evaluating the CRD table in STG. ColumnAndAvpPair: • Avp Name – The name of the diameter AVP (received in Media Component Description AVP of the AAR message) that will be used as input for CRD table evaluation. Supported list of AVPs are: QoS-Class-Identifier, TDF-Application-Identifier, Sponsor-Identity, Application-Service-Provider-Identity, Priority-Level, Pre-emption-Capability, Pre-emption-Vulnerability. DPCC_NAME - Used to derive the Dynamic PCC rule from CRD tables. DPCC_VALUE - Used to derive the Dynamic PCC rule from CRD tables. • Column – References the key column defined in the selected STG.

Parameter	Description
List of Output Column Avp Pairs (List)	Defines the mapping between the 'AVP Names' and the output columns defined in the selected STG. These mappings indicate how the output column values are mapped to AVPs after the CRD is evaluated. ColumnAndAvpPair: • Avp Name – The name of the diameter AVP (attribute from Qos-Information) to which the value of the output column should be mapped while setting the Qos-Information for the dedicated bearer on Gx. Supported values are: • Rating-Group • Reporting-Level • Service-Identifier • Online • Offline • Flow-Status • Metering-Method • Precedence • Allow-Usage-Monitoring (Map to corresponding crd column which is of type boolean). **Note** CPS sends Monitoring key for pre-configured rules only when ‘CC-Total-Octets’ is sent in Rx-AAR request (granted service units) and Allow-Usage-Monitoring is configured as true. The values for 'AVP name' must be exactly the same as those used while defining the input columns. • Column – References the output column defined in the selected STG.

OverrideQoS

Override QoS service configuration is used to allow configuring override for Gx default bearer QoS APN AMBR UL/DL values.

CPS first evaluates the derived QoS values for default bearer. CPS then evaluates the table provided in Override QoS service configuration by using the key values and determine the result APN AMBR UL/DL values. If the "Condition to Override" is "LT", then CPS limits the derived QoS values with these override values. If the "Condition to Override" is "GT", then CPS selects the maximum UL/DL among the derived and override values.

Table 206: OverrideQoS Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Reference	This is the reference to the STG that contains the QoS reference and the QoS parameter values (QCI, APN-MBR-UL, and so on).
List Of Input Column Avp Pairs (List)	Defines the list to specify the mapping for input (key) columns for determining their values for querying the STG. • ColumnAndAvpPair • Avp Name: Specify the AVP name whose value is used to map to the corresponding key Column for querying the STG. • Column: The key column in the STG that corresponds to the specified AVP.
Apn Agg Max Bit Rate U L	Reference to the STG output column that gives the "APN-Aggregate-Max-Bitrate-UL" value for limiting QoS. This value and the corresponding value derived after QoS actions are compared to determine the final value for APN-Aggregate-Max-Bitrate-UL.
Apn Agg Max Bit Rate D L	Reference to the STG output column that gives the "APN-Aggregate-Max-Bitrate-DL" value for limiting QoS. This value and the corresponding value derived after QoS actions are compared to determine the final value for APN-Aggregate-Max-Bitrate-DL.
Condition to Override	The condition to compare the values. Only two values are supported "LT" and "GT". If LT is selected, CPS picks the lowest QoS parameter value from the two QoS references. If GT is selected, CPS picks the highest QoS parameter value from the two QoS references. Possible Values: • LT: Less than (Default) • GT: Greater than

PreConfiguredRule

The PreConfiguredRule service configuration object configures a dynamic rule; these values are then used in the charging rule definition.

Table 207: PreConfigurationRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rule Group	
Rule Name	
Enable Resource Allocation Notification	
Dual Stack Session	
Framed I P Type	
ToD Schedule	
Scheduled Hour	
Retry Profile	
Online	
Offline	
Flow Status	
Rating Group	
Service Identifier	The identity of the service or service component that the service data flow in a PCC rule relates to.

Parameter	Description
Reporting Level	The Reporting-Level AVP is of type Enumerated and it defines on what level the PCEF reports the usage for the related PCC rule. There are three types of reporting levels: • SERVICE_IDENTIFIER_LEVEL (0): Usage will be reported on service id and rating group combination level and is applicable when the Service-Identifier and Rating-Group have been provisioned within the Charging-Rule-Definition AVP, and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. • RATING_GROUP_LEVEL (1): Usage will be reported on rating group level and is applicable when the Rating-Group has been provisioned within the Charging-Rule-Definition AVP, and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging. • SPONSORED_CONNECTIVITY_LEVEL (2):Usage will be reported on sponsor identity and rating group combination level and is applicable when the Sponsor-IdentityAVP Application-Service-Provider-Identity AVP and Rating-Group AVP have been provisioned within the Charging-Rule-Definition AVP. Applicable for offline charging.
Precedence	Determines the order in which the service data flow templates are applied at service data flow detection at the PCEF. A PCC rule with the Precedence AVP having a lower value will be applied before a PCC rule with the Precedence AVP having a higher value.
Metering Method	The Metering-Method AVP (AVP code 1007) is of type Enumerated and it defines what parameters will be metered for offline charging. The PCEF may use the AVP for online charging in case of decentralized unit determination. There are three types of metering method: • DURATION (0): The duration of the service data flow will be metered. • VOLUME (1): The volume of the service data flow traffic will be metered. • DURATION_VOLUME (2): The duration and the volume of the service data flow traffic will be metered.
Monitoring Key	See Common Parameter Descriptions, on page 508.
Flow Information (List)	FlowInformation • Flow Description • Tos Traffic Class • Flow Direction

Parameter	Description
QoS Information	QoSInformation For detailed information about these parameters, see Common Parameter Descriptions, on page 508. • Qci • Max Req Bandwidth U L • Max Req Bandwidth D L • Guaranteed Bit Rate U L • Guaranteed Bit Rate D L • Apn Agg Max Bit Rate U L • Apn Agg Max Bit Rate D L • Arp
Redirect Information	RedirectInformation For detailed information about these parameters, see Common Parameter Descriptions, on page 508. • Redirect Support • Redirect Address Type • Redirect Server Address
Mirror Default Bearer QCI/ARP	When set to true, CPS mirrors the QCI and ARP from the command level to the rule level, and enforces the rule level MBR values from the Policy Builder configuration for the rule level. Default: false.
Provision Default Bearer QoS	See Common Parameter Descriptions, on page 508.
Tdf Application Identifier	
Mute Notification	
Use in Rule Status Condition	Controls whether or not the PCC rule reported status AVPs are created. Default: true
Use in Rule Install Condition	Controls whether or not the PCC rule installed AVPs are created. Default: false
Encoding Format	When set to true, indicates monitoring key is encoded. When set to false, indicates no encoding is required. By default, CPS does not do any encoding for monitoring key. Default: false

PreDefinedRule

The PreDefinedRule service configuration object creates static rules that will be mapped to the charging rules that will be installed.

Table 208: PreDefinedRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rule Group	
Rule Name	
Enable Resource Allocation Notification	
Dual Stack Session	
Framed I P Type	
ToD Schedule	
Scheduled Hour	
Retry Profile	

PreDefinedRuleBase

The PreDefinedRuleBase service configuration object creates static rules that will be mapped to the charging rule base name.

Table 209: PreDefinedRuleBase Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rule Group	
Rule Name	
Enable Resource Allocation Notification	
Dual Stack Session	
Framed I P Type	
ToD Schedule	
Scheduled Hour	
Retry Profile	

PresenceReportingAreaConfiguration

The PresenceReportingAreaConfiguration service configuration configures the PRA identifiers supported.

Table 210: PresenceReportingAreaConfiguration Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Sd Auto Subscribe	When this flag is "false", the PCRF forwards PRA status when available to TDF, if TDF has subscribed with Event Trigger CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48). When this flag is "true" and the PRA status is available it is forwarded to TDF without waiting for the Event Trigger 48 subscription from TDF.
Presence Reporting Area Identifier List	This list contains the PRA identifier names which PCRF needs, to subscribe to PCEF with Event Trigger CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT.

Note Add Event Trigger CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) in the service configurations for the PRA identifiers to be subscribed towards PCEF.

ReleaseBearerDelayMessage

The ReleaseBearerDelayMessage service configuration object is used to release CCA-I /Gx-RAR messages which is held based on delay bearer creation configuration. For more information on Delay Bearer Creation service configuration object, refer to DelayBearerCreation, on page 439.

Table 211: ReleaseBearerDelayMessage Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508
Diameter Client	

ReprovisionObjects

The ReprovisionObjects service configuration object forces the Policy Charging Control (PCC) rules to be reprovisioned when the flag is set to true.

Table 212: ReprovisionObjects Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
PCC Rules	Can be set to true or false. When set to true, the PCC rules will be reprovisioned. Default: false
Default Bearer QoS	Can be set to true or false. When set to true, the Default Bearer QoS will be reprovisioned. Default: false
Override Control	Can be set to true or false. When set to true, the AVP Override Control is repovisioned during handoff. Default: false

RevalidationTime

The RevalidationTime service configuration object populates the revalidation time AVP at the message level; the PCEF will come back to the PCRF when that timestamp is hit.

Note The Revalidation Time and the Health Check Time Interval (**Diameter Configuration** > **PolicyDRA Health Check** > **Binding Db** should not be configured with the same value.

Table 213: RevalidationTime Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Absolute Time Flag	This flag can be set to true or false. true – The next revalidation time is set using the absolute values specified for the following three revalidation attributes (Hour Minute, and Sec). false – The next revalidation time is derived by adding the values specified for the following three revalidation attributes to the system time.
Revalidation Time in Hour	The hour the revalidation will occur. Specify this value using 24-hour format.
Revalidation Time in Minute	The minutes setting in the revalidation timestamp.
Revalidation Time in Sec	The seconds setting in the revalidation timestamp.

SupressRxMessage

The SupressRxMessage service configuration object is used to suppress the Rx ASR message. CPS evaluates the STG configured in this service and derives the information whether to suppress Rx ASR or not.

Table 214: SupressRxMessage Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.
Input Column Binding (List)	ColumnAndAvpPair • Avp Name: The name of the Diameter AVP that is used as input for CRD table evaluation. • Column: The key column in the STG that corresponds to the specified AVP.

Parameter	Description
Is Message Suppressed Output Column	References to the output column defined in the CRD.

TableDrivenChargingRule

The TableDrivenChargingRule service configuration object represents a charging rule in stored CRD format; there can be multiple charging rules.

Table 215: TableDrivenChargingRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Logical Grouping	No longer used.
Search Table	The name of the table from which to perform a lookup.
Search Group	A constant value that CPS uses to search within the Search Table Group indicated by “Search Table” element.
Search Column	Must be bound to the key column of the STG. The data contained in the STG column is of type Text.
Best Match Excludes Star Match	By default, the parameter is set to true. When set to true, the best match result records with exact match and if the exact match records are not found then it return records with star and pattern match. When set to false, then the result includes exact match as well as star and pattern match.
Rule Name Source	A key column that must be bound to the Rule Name column within the STG. The data in the STG column is of type Text.
Flow Status Source	Must be bound to the Flow Status column in the Search Table Groups (STG). The data contained in the STG column is of type Text.
Monitoring Key Source	Must be bound to the Monitoring Key column in the STG. The data contained in the STG column is of type Text.

Parameter	Description
Redirect Address Table	The name of the Redirect Address Table. This table contains redirected attributes, such as these (described in the following four rows): • Redirect Enabled Source • Redirect Address Type Source • Redirect Address Source • Redirect Support Source
Redirect Enabled Source	Must be bound to the Redirect Enabled column in the STG. The data contained in the STG column is of type True/False.
Redirect Address Type Source	Must be bound to the Redirect Address Type column in the STG. The data contained in the STG column is of type Text.
Redirect Address Source	Must be bound to the Redirect Address column in the STG. The data contained in the STG column is of type Text.
Redirect Support Source	Must be bound to the Redirect Support column in the STG.
Online Source	Must be bound to the Online column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Offline Source	Must be bound to the Offline column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Rating Group Source	Must be bound to the Rating Group column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Service Id Source	Must be bound to the Service ID column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Reporting Level Source	Must be bound to the Reporting Level column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Precedence Source	Must be bound to the Precedence column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Metering Method Source	Must be bound to the Metering Method column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.

Parameter	Description
Flow Information Source	Must be bound to the Flow Information column in the STG. The data contained in the STG column is of type Text. **Note** A particular format should be used when adding Flow Information Source parameter so that CPS can perform proper Flow Information grouped AVP mapping. A wrongly formatted Flow Information Source can result in missing AVPs under Gx Flow Information AVP. Here is the format: **`<Flow-Description>;<Flow-Direction>;<Decimal value of first octet of ToS-Class-AVP>;<Decimal value of second octet of ToS-Class-AVP>`**
Use Override Server Address	Must be bound to the Override Server Address column in the STG. The data contained in the STG column is of type True/False. If set to true, the address is taken from the service option. If set to false, the redirect server address will not be overridden.
Override Server Address	Must be bound to the corresponding column within the STG.
Qci Source	Must be bound to the QCI column in the STG. The data contained in the STG column is of Type Number. For more information, see Common Parameter Descriptions, on page 508.
Max Req Bandwidth U L Source	Must be bound to the Max Req Bandwidth UL column in the STG. The data contained in the STG column is of Type Number. For more information about Max Req Bandwidth U L, see Common Parameter Descriptions, on page 508.
Max Req Bandwidth D L Source	Must be bound to the Max Req Bandwidth DL column in the STG. The data contained in the STG column is of Type Number. For more information about Max Req Bandwidth D L Source, see Common Parameter Descriptions, on page 508.
Guaranteed Bit Rate U L Source	Must be bound to the Guaranteed Bit Rate UL column in the STG. The data contained in the STG column is of Type Number. For more information about Guaranteed Bit Rate U L see Common Parameter Descriptions, on page 508.
Guaranteed Bit Rate D L Source	Must be bound to the Guaranteed Bit Rate DL column in the STG. The data contained in the STG column is of Type Number. For more information about Guaranteed Bit Rate D L, see Common Parameter Descriptions, on page 508.
ARP Priority Level Source	Must be bound to the ARP Priority Level column in the STG. The data contained in the STG column is of Type Number. For more information about Priority Levels, see Common Parameter Descriptions, on page 508.

Parameter	Description
ARP Preemption Capability Source	Must be bound to the ARP Preemption Capability column in the STG. The data contained in the STG column is of Type Number. For more information about Preemption Capability, see Common Parameter Descriptions, on page 508.
ARP Preemption Vulnerability Source	Must be bound to the ARP Preemption Vulnerability column in the STG. The data contained in the STG column is of Type Number. For more information about Preemption Vulnerability, see Common Parameter Descriptions, on page 508.
Apn Agg Max Bit Rate U L	See Common Parameter Descriptions, on page 508.
Apn Agg Max Bit Rate D L	
Rule Retry Profile Name	Must be bound to the Rule Retry Profile column in the STG. The data contained in the STG column is of type Text.
Mirror Default Bearer QCI/ARP	When set to true, CPS mirrors the QCI and ARP from the command level to the rule level, and enforces the rule level MBR values from the Policy Builder configuration for the rule level. Default: false.
Provision Default Bearer QoS	See Common Parameter Descriptions, on page 508.
Tdf Application Identifier Source	References the application detection filter (for example, its value may represent an application such as a list of URLs, etc.) to which the PCC rule for application detection and control in the PCEF applies. Tdf Application Identifier Source must be bound to the appropriate column in the STG, and Type should be Text. For more information about Tdf Application Identifier, see Common Parameter Descriptions, on page 508.
Mute Notification Source	Must be bound to the Mute Notification column in the STG. The data contained in the STG column is of Type Number or Decimal. For more information about Mute Notification, see Common Parameter Descriptions, on page 508.
Enable Resource Allocation Notification Source	Must be bound to the Enable Resource Allocation Notification column in the STG. The data contained in the STG column is of Type Number. The possible values are mentioned in 3GPP specification 29.212.
Input List (List)	InputColumnObject: • Crd Column – Is bound to the appropriate key column in the STG for those AVPs that are inputs to this table. • Referenced Output Column – Reserved for future use. • Column Value – The value of the AVP that is bound to the Crd Column and has a single value. • Referenced MultiValue AVP Name – The name of the attribute that is bound to the Crd Column and has multiple values.

Parameter	Description
Use in Rule Status Condition	Controls whether or not the PCC rule reported status AVPs are created. By default, this parameter is set to true.
Use in Rule Install Condition	Controls whether or not the PCC rule installed AVPs are created. By default, this parameter is set to false.
Encoding Format Source	The parameter is used to pull the value from a CRD column of type Boolean. When set to true, CRD value indicates monitoring key is encoded. When set to false, CRD value indicates no encoding is required. By default, CPS does not do any encoding for monitoring key. Default: false

TableDrivenChargingRuleRefresh

The TableDrivenChargingRuleRefresh service configuration object forces a rule revalidation based on the rule reporting status.

Table 216: TableDrivenChargingRuleRefresh Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table	The name of the table from which to perform a lookup.
Input Rule Name Column	The input column for the Search Table Group (STG), which contains the rule name.
Input Rule Status Column	The input column for the STG, which contains the rule status against which new rules are to be added.
Output Rule Group Column	The output column for the STG, which contains the rule group used as a group to search the TableDrivenChargingRule.
Output Search Table	If there are multiple TableDrivenChargingRules mapped with multiple Search Tables, and if we want to use only one table to be looked at for new rules installation on rule failure, we can give the table as Output Search Table so that only one TableDrivenChargingRule object, which has the 'Search Table' matching the 'Output Search Table' in TableDrivenChargingRuleRefresh, is evaluated for refresh rules.

TableDrivenCiscoQosGroupRules

The TableDrivenChargingRuleRefresh service configuration option forces a rule revalidation based on the rule reporting status.

Table 217: TableDrivenCiscoQosGroupRules Service Configuration Parameters

Parameter	Discription
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Logical Grouping	No longer used.
Search Table	The name of the table from which to perform a lookup.
Search Group	A constant value that CPS uses to search within the STG indicated by “Search Table” element.
Search Column	Must be bound to the key column of the STG. The data contained in the STG column is of type Text.
Best Match Excludes Star Match	By default, the parameter is set to true. When set to true, the best match result records with exact match and if the exact match records are not found then it return records with star and pattern match. When set to false, then the result includes exact match as well as star and pattern match.
Rule Name Source	A key column that must be bound to the Rule Name column within the STG. The data contained in the STG column is of type Text.
Monitoring Key Source	Must be bound to the Monitoring Key column within the STG. The data contained in the STG column is of type Text.
Encoding Format Source	Must be bound to the Encoding format column within the STG. The data contained in the STG column is of type True/False.
Redirect Address Table	The name of the Redirect Address Table. This table contains redirected attributes, such as these (described below): • Redirect Enabled Source • Redirect Address Type Source • Redirect Address Source
Redirect Enabled Source	Must be bound to the Redirect Enabled column within the STG. The data contained in the STG column is of type True/False.
Redirect Address Type Source	Must be bound to the Redirect Address Type column within the STG. The data contained in the STG column is of type Text.
Redirect Address Source	Must be bound to the Redirect Address column within the STG. The data contained in the STG column is of type Text.

Parameter	Discription
Use Override Server Address	Must be bound to the Override Server Address column within the STG. The data contained in the STG column is of type True/False. If set to true, the address is taken from the service option. If set to false, the redirect server address will not be overridden.
Override Server Address	Must be bound to the corresponding column within the STG.

TableDrivenPredefinedChargingRule

The TableDrivenPredefinedChargingRule service configuration object represents a charging rule in stored CRD format; there can be multiple charging rules.

Table 218: TableDrivenPredefinedChargingRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Logical Grouping	No longer used.
Search Table	The name of the table from which to perform a lookup.
Search Group	A constant value that CPS uses to search within the Search Table Group indicated by “Search Table” element.
Search Column	Must be bound to the key column of the STG. The data contained in the STG column is of type Text.
Best Match Excludes Star Match	By default, the parameter is set to true. When set to true, the best match result records with exact match and if the exact match records are not found then it return records with star and pattern match. When set to false, then the result includes exact match as well as star and pattern match.
Rule Name Source	A key column that must be bound to the Rule Name column within the STG. The data in the STG column is of type Text.

Parameter	Description
Input List (list)	InputColumnObject: • Crd Column – Is bound to the appropriate key column in the STG for those AVPs that are inputs to this table. • Referenced Output Column – Reserved for future use. • Column Value – The value of the AVP that is bound to the Crd Column and has a single value. • Referenced MultiValue AVP Name – The name of the attribute that is bound to the Crd Column and has multiple values.
Use In Rule Status Condition	Controls whether or not the PCC rule reported status AVPs are created. By default, this parameter is set to false.
Use In Rule Install Condition	Controls whether or not the PCC rule installed AVPs are created. By default, this parameter is set to false.

TableDrivenRuleNameSupport

The TableDrivenRuleNameSupport service configuration object allows CPS to perform a UNION operation on two sets of rule lists. This operation uses the rules that are common to both lists obtained from two different Search Table Groups (STGs).

Table 219: TableDrivenRuleNameSupport Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Logical Grouping	No longer used.
Search Table	The name of the table from which to perform a lookup.
Search Group	A constant value that CPS uses to search within the STG indicated by “Search Table” element.
Search Column	Must be bound to the key column of the STG. The data contained in the STG column is of type Text.
Best Match Excludes Star Match	By default, the parameter is set to true. When set to true, the best match result records with exact match and if the exact match records are not found then it return records with star and pattern match. When set to false, then the result includes exact match as well as star and pattern match.

Parameter	Description
Rule Name Source	A key column that must be bound to the Rule Name column within the STG. The data contained in the STG column is of type Text.

TDFServerInformation

The TDFServerInformation service configuration object is used to configure TDF-Server-Information based on Gx APN, GX-MCCMNC and LDAP attribute SUB_TYPE. Based on the service configuration, CRD look up is done to obtain the TDF-Server-Information and TSR would be initiated towards Sd interface.

Table 220: TDFServerInformation Service Configuration Parameters

Parameter	Description
Priority	The priority of the message for processing. The higher the number, the higher the priority. Default: 0 For more information, see Common Parameter Descriptions, on page 508.
Diameter Client	The client configuration is used to apply different policies based on PCEF type. This is optional parameter. For more information, see Common Parameter Descriptions, on page 508.
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.
List Of Input Column Avp Pairs (List)	Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. ColumnAndAvpPair • Avp Name: The name of the Diameter AVP that is used as input for CRD table evaluation. • Column: The key column in the STG that corresponds to the specified AVP.
List Of Output Column Avp Pairs (List)	Defines the mapping between the AVP Names and the output columns defined in the STG selected. These mapping indicate how the output column's values are mapped to AVPs after the CRD is evaluated. ColumnAndAvpPair • Avp Name: The name of the Diameter AVP to which the value of the output column is mapped. • Column: The reference to the CRD column for the output AVP.

UsageMonitoringKey

The UsageMonitoringKey service configuration object allows scheduled monitoring in the Monitoring Schedule (List) parameter.

Table 221: UsageMonitoringKey Service Configuration Parameters

Parameter	Description
Priority	Not Supported
Diameter Client	See Common Parameter Descriptions, on page 508.
Encoding Format	
Monitoring Key	
Dosage	
Monitoring Level	
Enabled	Can be set to true or false. • True – Monitoring information will flow to PCEF. • False – Monitoring information will not flow to PCEF.
Balance Code	See Common Parameter Descriptions, on page 508.
Validity Period Minutes	The number of minutes that the balance code representing the quota is valid. The default value is 60 minutes. This parameter is deprecated.
Reporting Threshold	Not used.
Dosage Override (List)	Default dosage override based on remaining balance on the selected account. • Remaining Balance Below Megabytes • Dosage Override Megabytes
Monitoring Schedule (List)	UsageMonitoringSchedule: • Start Time – Enter the time in 24-hour format (00:00 to 23:59). • End Time – Enter the time in 24-hour format (00:00 to 23:59). • Balance Code – See Common Parameter Descriptions, on page 508. • Dosage – See Common Parameter Descriptions, on page 508. • Rate – Enter the numeric value which to charge usage.
Target Balance Code	Indicates a text input for the balance code name to be mapped to the specific target balance.

UsageMonitoringKeyDual

The UsageMonitoringKeyDual service configuration object allows time usage monitoring (The UsageMonitoringKey is supported for Volume Usage monitoring). This service configuration object provides a way to configure usage monitoring for both time and volume (independently as well as together under single monitoring key). To monitor usage under one key for Volume and Time, both the balance codes need to be provided in the Service Configuration. For independent monitoring, only the relevant type of fields can be set. For example, for only Volume monitoring, fields related to time monitoring can be left blank/null and vice versa. Multiple instances of UsageMonitoringKeyDual can also be included in the service configuration each corresponding to a unique monitoring key.

Table 222: UsageMonitoringKeyDual Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Encoding Format	
Monitoring Key	
Dosage	
Monitoring Level	
Enabled	Can be set to true or false. • True – Monitoring information will flow to PCEF. • False – Monitoring information will not flow to PCEF.
Validity Period Minutes	The number of minutes that the balance code representing the quota is valid. The default value is 60 minutes. This parameter is deprecated.
Volume > UsageMonitoringBucket > Balance Code	This value indicates the Volume type balance with which the key is associated.
Time > UsageMonitoringBucket > Balance Code	This value indicates the Time type balance with which the key is associated.
Target Balance Code	Indicates a text input for the balance code name to be mapped to the specific target balance.
Inactivity Detection Time	The time interval in seconds after which the time measurement shall stop for the Monitoring Key, if no packets are received belonging to the corresponding Monitoring Key. Corresponds to Quota-Consumption-Time AVP

Gy Service Configuration Objects

This section describes the parameters for the following Gy Service Configuration Objects:

ExternalRatingGroup

The ExternalRatingGroup service configuration object is used to identify if a rating group status is indicated by an external component. If the status is invalid, the final unit actions are applied as specified in this object.

The rating group for this object is list of values identifying all external rating groups.

Table 223: ExternalRatingGroup Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rating Group	Corresponds to a value configured on the ASR5000 that represents which data should be monitored.
Ocs State	Indicates the status of the external rating group as notified by the external component. The possible values are VALID/INVALID. Default: VALID
Final Unit Action	Can be set to one of the following options: • TERMINATE – Send a CCR-u with the final usage for the rating group. • NONE – No action taken. • RESTRICT_ACCESS – Send a Restriction Filter Rule and Filter ID. • REDIRECT – Send a Redirect Address of Redirect Address Type. Default: TERMINATE
Redirect Address Type	See Common Parameter Descriptions, on page 508.
Redirect Address	
Filter ID	When the Final Unit Action is RESTRICT_ACCESS, the access device must restrict the user access to the IP packet filters identified by Filter-id AVP.
Restriction Filter Rule	When the Final Unit Action is RESTRICT_ACCESS, the access device must restrict the user access to the IP packet filters defined in the Restriction-Filter-Rule AVP.

GySessionWallet

Please configure the GySessionWallet service configuration object only with the help of Cisco Advanced Services or the Cisco Technical Assistance Center (TAC).

RatingGroup

CPS uses the RatingGroup Service Configuration Object to hold the configuration parameters for Gy towards OCS. The RatingGroup object can be added to a service upon a CCR-i request from the PCEF with a Gx rule or QoS. This object is used if the RatingGroupServiceID object is not used.

Table 224: RatingGroup Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rating Group	Corresponds to a value that represents which data should be monitored.
Rg Type	Rating Group Type. The value can be set to either Volume or Time.
Dosage	See Common Parameter Descriptions, on page 508.
Balance Code	
Final Unit Action	Can be set to one of the following options: • TERMINATE – Send a CCR-u with the final usage for the rating group. • NONE – No action taken. • RESTRICT_ACCESS – Send a Restriction Filter Rule and Filter ID. • REDIRECT – Send a Redirect Address of Redirect Address Type. Default: TERMINATE
Redirect Address Type	See Common Parameter Descriptions, on page 508.
Redirect Address	
Restriction Filter Rule	When the Final Unit Action is RESTRICT_ACCESS, the access device must restrict the user access to the IP packet filters defined in the Restriction-Filter-Rule AVP.
Filter ID	When the Final Unit Action is RESTRICT_ACCESS, the access device must restrict the user access to the IP packet filters identified by Filter-id AVP.
Tariff Change Time	Outside the scope of this document. Default: 0

Parameter	Description
Tariff Switch Model	Outside the scope of this document. Default: SINGLE_COUPON
Validity Time	Sets a session timer for the Gy quota grant; even if quota is not exhausted, the PCEF must check back in at the end of the validity time (in seconds). Default: 3600
Volume Quota Threshold	PCEF will check back in with OCS when the Volume Quota Threshold has been reached. The value must be set to less than the overall Dosage (in bytes). Default: 0
Time Quota Threshold	PCEF will check back in with OCS when the Time Quota Threshold has been reached. The value must be set to less than the overall Dosage (in seconds). Default: 0
Quota Holding Time	The amount of time the quota should be available on the PCEF without activity from the user (in seconds). Default: 0
Quota Consumption Time	Idle traffic threshold time (in seconds); only used with time quota rating groups. Default: 0
Use Shared Bucket	Used in a shared quota use case in which the same account balance and rating group can be used within a shared group of users. Default: false

RatingGroupServiceId

The RatingGroupServiceId service configuration object identifies a set of services that are identified by Service-Identifier and subject to the same cost and rating type. The service identifier is provisioned along with the rating group this object is used.

Table 225: RatingGroupServiceId Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rating Group	Corresponds to a value configured on the ASR5000 that represents which data should be monitored.
Service Identifier	Identifies a set of services subject to the same cost and rating type.
Rg Type	Rating Group Type. The value can be either Volume or Time.

Parameter	Description
Dosage	See Common Parameter Descriptions, on page 508.
Balance Code	
Final Unit Action	Can be set to one of the following options: • TERMINATE – Send a CCR-u with the final usage for the rating group. • NONE – No action taken. • RESTRICT_ACCESS – Send a Restriction Filter Rule and Filter ID. • REDIRECT – Send a Redirect Address of Redirect Address Type. Default: TERMINATE
Redirect Address Type	See Common Parameter Descriptions, on page 508.
Redirect Address	
Restriction Filter Rule	When the Final Unit Action is RESTRICT_ACCESS, the access device must restrict the user access to the IP packet filters defined in the Restriction-Filter-Rule AVP.
Filter ID	When the Final Unit Action is RESTRICT_ACCESS, the access device must restrict the user access to the IP packet filters identified by Filter-id AVP.
Tariff Change Time	Outside the scope of this document. Default: 0
Tariff Switch Model	Outside the scope of this document. Default: SINGLE_COUPON
Validity Time	Sets a session timer for the Gy quota grant; even if quota is not exhausted, the PCEF must check back in at the end of the validity time (in seconds).
Volume Quota Threshold	PCEF will check back in with OCS when the Volume Quota Threshold has been reached; value must be set as less than the overall Dosage (in bytes).
Time Quota Threshold	The threshold value in seconds and can be provisioned by OCS when granted service units include cc-time. The PCEF shall seek re-authorization from OCS for the quota when the quota contents fall below the supplied threshold.
Quota Holding Time	The amount of time the quota should be available on the PCEF without activity from the user (in seconds).
Quota Consumption Time	Idle traffic threshold time (in seconds); only used with time quota rating groups.
Rate1	When tariff time is provisioned by OCS, PCEF reports usage before and after tariff change time when reporting after tariff change time. Rate 1 indicates at what rate usage before tariff change time is charged.

Parameter	Description
Rate2	When tariff time is provisioned by OCS, PCEF reports usage before and after tariff change time when reporting after tariff change time. Rate2 indicates at what rate usage after tariff change time is charged.
Use Shared Bucket	Used in a shared quota use case in which the same account balance and rating group can be used within a shared group of users. Default: false

LDAP Service Configuration Objects

LdapAddProfile

Attention In CPS 13.1.0 and higher releases, LdapAddProfile service configuration has been deprecated. Instead of using LdapAddProfile, you can use *LdapAddEntries*.

LdapAddProfile service configuration can be used to define an LDAP profile (list of attributes) that can be written to an external LDAP server.

Table 226: LdapAddProfile Service Configuration Parameters

Parameter	Description
Ldap Server Set	The parameter is used to define the target server set to which the add request is sent.
Dn	This is the LDAP Distinguished Name for the new entry that is added via the add request.
Dn Replacement Rules (List)	This parameter is used to specify the replacement rules (one for each Dn parameter) that helps to resolve the parameters provided as part of Dn. ReplacementMapping: • Replacement String: This is used to specify the variable (one for each parameter) used in the DN. • Replacement Source: This is a policy-state retriever that can be used to retrieve the required value for replacement.

Parameter	Description
Ldap Add Attribute (List)	This parameter is used to specify the list of attributes (name/value pairs) that are to be included in the new profile added using add request. LdapSynchAttribute: • Type: This is the LDAP attribute name. • Value: This is the LDAP attribute value which can be dynamically set by using the **Pull value from...** field to get its value from CRD output, subscriber AVP, and so on.
Controls (List)	This parameter is used to specify the LDAP controls that needs to be send in the LDAP modifyRequest. Control is a way to specify extension information to the LDAP server. Control: A control is a way to specify extension information. Controls which are sent as part of a request apply only to that request and are not saved. • Control Type: This field MUST be a UTF-8 encoded dotted-decimal representation of an OBJECT IDENTIFIER which uniquely identifies the control. This prevents conflicts between control names. • Criticality: Currently, not supported. • Control Value: Currently, not supported. These above mentioned configuration fields are added as per the LDAP controls defined in RFC-2251.

LdapAddEntries

LdapAddEntries service configuration allows you to define multiple LDAP entries (DNs) to add on external server in specified order (sequential in synchronous mode).

Table 227: LdapAddEntries Service Configuration Parameters

Parameter	Description
Ldap Server Set	The parameter is used to define the target server set to which the add request is sent.
Entries (List)	Multiple attributes can be defined to be added under each LDAP entry (which are added under the specified DN). If an entry already exists or add operation for an entry returns an error, CPS continues sequentially adding other entries in the list as long as the connection is usable. LdapEntries: For more information, refer to Table 228: LdapEntries, on page 472.

Table 228: LdapEntries

Parameter	Description
Dn	This is the LDAP Distinguished Name for the new entry that is added via the add request.
Dn Replacement Rules (List)	This parameter is used to specify the replacement rules (one for each Dn parameter) that helps to resolve the parameters provided as part of Dn. ReplacementMapping: • Replacement String: This is used to specify the variable (one for each parameter) used in the DN. • Replacement Source: This is a policy-state retriever that can be used to retrieve the required value for replacement.
Modify If Exists	If the "Modify If Exists" flag is set to true for the entry that already exists, CPS attempts a LDAP modify operation with "change type: replace" for each included attribute for which the "Add Only" flag is false ("Add Only" = true attributes are not included in the modify operation). This modify operation is executed in parallel to the other add operations (for other DNs).
Ldap Attributes (List)	This parameter is used to specify the list of attributes (name/value pairs) that are to be included in the new profile added using add request. LdapSynchAttribute: • Type: This is the LDAP attribute name. • Value: This is the LDAP attribute value which can be dynamically set by using the **Pull value from...** field to get its value from CRD output, subscriber AVP, and so on. • Add Only: The default value is false. • Statistic Name: If Statistic Name parameter is configured with a value, then a counter is created with this name to track the success or failure of LDAP operations for this attribute. If the value is not provided, counters are not generated for the attribute.

Parameter	Description
Controls (List)	This parameter is used to specify the LDAP controls that needs to be send in the LDAP modifyRequest. Control is a way to specify extension information to the LDAP server. Control: A control is a way to specify extension information. Controls which are sent as part of a request apply only to that request and are not saved. • Control Type: This field MUST be a UTF-8 encoded dotted-decimal representation of an OBJECT IDENTIFIER which uniquely identifies the control. This prevents conflicts between control names. • Criticality: Currently, not supported. • Control Value: Currently, not supported. These above mentioned configuration fields are added as per the LDAP controls defined in RFC-2251.

Note If both LdapAddEntries and LdapSynchProfile are found in policy, CPS consolidates the LDAP add (from LdapAddEntries) and LDAP modify (from LdapSynchProfile) operations into a single LDAP add operation if any of the LDAP DNs provided under LdapAddEntries matches the DN provided under LdapSynchProfile. If a match is found, all attributes under LdapSynchProfile are copied into the LDAP add operation (and the "Modify If Exists" flag is overridden to "true" for that DN entry). If a DN match is not found, both operations execute separately in parallel.

LdapSynchProfile

LdapSyncProfile service configuration can be used to define a LDAP profile (list of attributes) that is updated on the external LDAP server. CPS calculates the values and tracks the LDAP attributes (included in the profile) for any changes through the lifetime of the session. If changes are detected, the server is updated with the new version of the profile.

Table 229: LdapSynchProfile Service Configuration Parameters

Parameter	Description
Ldap Server Set	A reference to the LdapServerSet configured in the reference-data. It links to the LDAP Plugin Configuration to identify the LDAP server configuration parameters.
Dn	This is the Distinguished Name for identifying the subscriber to be updated on the LDAP directory.

Parameter	Description
Dn Replacement Rules (List)	This gives the option to dynamically replace the variables (identified with $) defined in DN. ReplacementMapping: • Replacement String: This is used to specify the variable used in the DN. • Replacement Source: This is a policy-state retriever that can be used to retrieve the required value for replacement.
Modified Date Attribute Name	Specifies the LDAP attribute name for storing the date when the LDAPModify request is triggered.
Ldap Synch Attribute (List)	Specifies the list of attributes that should be updated on the LDAP server through the modify request. LdapSynchAttribute: • Type: This is the LDAP attribute name. • Value: This is the LDAP attribute value which can be dynamically set by using the **Pull value from...** field to get its value from CRD output, subscriber AVP, and so on. • Add Only: The default value is false. • Statistic Name: If Statistic Name parameter is configured with a value, then a counter is created with this name to track the success or failure of LDAP operations for this attribute. If the value is not provided, counters are not generated for the attribute.
Controls (List)	Specifies the LDAP controls that needs to be send in the LDAP modifyRequest. Control is a way to specify extension information to the LDAP server. Control: A control is a way to specify extension information. Controls which are sent as part of a request apply only to that request and are not saved. • Control Type: This field MUST be a UTF-8 encoded dotted-decimal representation of an OBJECT IDENTIFIER which uniquely identifies the control. This prevents conflicts between control names. • Criticality: Currently, not supported. • Control Value: Currently, not supported. These above mentioned configuration fields are added as per the LDAP controls defined in RFC-2251.

Rx Service Configuration Objects

This section describes the parameters for the following Rx Service Configuration Objects:

ActionBasedOnSyPolicyCounters

ActionBasedOnSyPolicyCounters Service Configuration is used to pull CRD data from the STG.

The input parameters are: The Sy Policy Counter Identifier and Status in the format Identifier:Status. For multiple Policy Counters, each set of identifiers and counters are separated with semi-colons, for example: Identifier1:Status1;Identifier2:Status

When CPS receives Rx AAR or Sy SLA/SNR messages, CPS performs a one-time query on the CRD Table with the Sy Policy Counter Status as the input Key. Based on the output parameters, CPS sets SyCounterActions Object in Policy State with output parameters to handle in triggerAdditionalMessages method.

The output parameters are:

- Specific Action : The Specific Action to be sent in Rx-RAR
- Restricted-Media Type : The media types mapped. For multiple media types, each type is separated by a comma.
- Rx-Action : Action to be taken on Rx. Possible values are Continue (no action), Reject, and Terminate.
- Sy-Action : Possible values are Continue (no action), Terminate.
- Gx-Action : Rule-Group name in TableDrivenChardingRule STG which has Gx Rules for Flow-Status, Service-Id, Rating-Group , offline/online Metering method
- Sponsored-Identity : Sponsor Identity of session. For multiple Sponsor Identities, each is separated by a comma.
- Application-Service-Provider-Identity : Application-Service-Provider-Identity of session. For multiple Application-Service-Provider-Identity, each is separated by a comma.

The following table describes the service configuration parameters:

Table 230: ActionBasedOnSyPolicyCounters Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	Should not be configured.
Policy Counter Name (List)	Enter the Policy Counter Names in the order in which the CRD Input Column ‘Policy-Counter-Status’ is configured. Expected format is PolicyCounterIdentifier1:PolicyCounterStatus1; PolicyCounterIdentifier2:PolicyCounterStatus2
Stg Name	References the Search table group containing the CRD table.
List of Input Column Avp Pairs (List)	Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name – The Avp name. Only supported value is Policy-Counter-Status. • Column – The reference to the CRD column for the input AVP.

Parameter	Description
List of Output Column Avp Pairs (List)	List of Output AVPs for the CRD. • Avp Name: The Avp name. Only values supported are ‘Rx-Action, ‘Gx-Action’, ‘Sy-Action’ , ‘Application-Service-Provider-Identity’, ‘Sponsor-Identity’, ‘Specific-Action’ and ‘Restricted-Media-Type’. • Column: The reference to the CRD column for the output AVP.

Important You must configure a table search initiator to the Search Table Group mapped in ActionBasedOnSyPolicyCounters with the condition "a customer reference data AVP exists" , which ensures that the table is not evaluated every time on any event by the policy engine. In the Table Search Initiator, enter a name for the initiator and add code as "CRD-CODE" and set the value to True.

ModifyRxDynamicRule

Rx Dynamic Rules can be modified by configuring ModifyRxDynamicRule service configuration and the modification can be based on Default Bearer QoS, Media-Type, AF-Application-identifier, Sponsor-Id and Application-Service-Provider-Identity.

The following table describes the service configuration parameters:

Table 231: ModifyRxDynamicRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD table.

Parameter	Description
List of Input Column Avp Pairs (List)	Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name – The name of the AVP that is used as input for CRD table evaluation. Supported values are QoS-Class-Identifier, Priority-Level, Pre-emption-Capability, Pre-emption-Vulnerability, Media-Type, AF-Application-Identifier, Sponsor-Identity, Application-Service-Provider-Identity, Flow-Status, Flow-Usage, and MCPTT-Identifier. DPCC_NAME - Used to derive the Dynamic PCC rule from CRD tables. DPCC_VALUE - Used to derive the Dynamic PCC rule from CRD tables. **Note** All input values should be configured as **Key** in Policy Builder. For custom fields, runtime binding should be set to **None**. • Column – The reference to the CRD column for the input AVP.
List of Output Column Avp Pairs (List)	List of Output AVPs for the CRD. • Avp Name – The name of the AVP that is used as input for CRD table evaluation. Supported values are QoS-Class-Identifier, Qci, Priority-Level, Priority Level, Pre-emption-Capability, Preemption Capability, Pre-emption-Vulnerability, Preemption Vulnerability, Guaranteed-Bitrate-UL, Guaranteed Bit Rate U L, Guaranteed-Bitrate-DL, Guaranteed Bit Rate D L, Max-Requested-Bandwidth-UL, Max Req Bandwidth U L, Max-Requested-Bandwidth-DL, and Max Req Bandwidth D L. • Column – The reference to the CRD column for the output AVP.
Ignore Existing Rule	This flag is used to ignore modification of existing Rx dedicated bearer which needs to be true to avoid existing rule modification on default bearer boost.
Disable Make N Break Rule on Qos Change	When set to true, modified QCI/ARP are sent under same rule instead of generating new rule. When set to false, make and break functionality for Rx Dynamic Rule works. A new rule gets generated when QCI/ARP gets changed for current rule. Default: false
Retain Modification On Boost Termination	When set to true, existing dedicated bearer is not modified and boost/throttle is terminated. Default: false Type: Boolean

Important The AVP Names Qci, Priority Level, Preemption Capability, Preemption Vulnerability, Guaranteed Bit Rate U L, Guaranteed Bit Rate D L, Max Req Bandwidth U L, and Max Req Bandwidth D L support QoS Action Mirror, Enforce or Bound.

For more details on QoS Action, refer to Programmatic CRD (QoS Action), on page 341.

RxAppQoSInformation

The RxAppQoSInformation service configuration option defines the QoS to be used for Rx dedicated bearer based on the application ID and media type.

Table 232: RxAppQoSInformation Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Qci	
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guaranteed Bit Rate D L	
Arp	
Af Application Id	The AF-Application-Id for which the QoS values should be applied.
Media Type	The Media-Type for which the QoS values should be applied. (Use an Integer value as per 3GPP specifications).

For more information, refer to RxAppQosInformation Service Configuration, on page 330.

RxAuthorizationSTGConfiguration

RxAuthorizationSTGConfiguration service configuration can be used to evaluate Rx Authorization table and obtain the output values configured. The RxAuthorizationSTGConfiguration supports chained evaluation of STGs which means multiple Search Table Groups can be configured hierarchically in the RxAuthorizationSTGConfiguration and outputs of one table can be used as input keys for another table. The Rx Authorization table from which Bearer Authorization and Error Cause output values are received needs to be configured as the last table in the list of chained STGs configured under RxAuthorizationSTGConfiguration.

Note

- Rx Authorization in AAR messages is supported for only new bearers, and not modification of existing bearers.
- Rx_RAR on failure of Rx Authorization is sent only if Specific-Action= INDICATION_OF_FAILED_RESOURCES_ALLOCATION is armed in AAR message.

The following table describes the service configuration parameters:

Table 233: RxAuthorizationSTGConfiguration Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	

Parameter	Description
Stg Details (List)	StgNameReferencePair: • Stg Name (Optional): References the Search table group containing the CRD table. STG names configured have to be unique. • Stg Reference (Mandatory): This is the reference to the CRD table • List Of Input Column Avp Pairs (Mandatory): Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name: Incase the Input AVP is a standard AVP, then the AVP Name can be configured to the name of the diameter AVP (received in Media Component Description AVP of the AAR message) which is to be used as input for CRD table evaluation. (For example, AF-Application-Identifier, Media-Type and so on). **Note** AVPs present at Media-Sub-Component level are not supported. In case of chained evaluation of STGs, the AVP Name must be exactly the same as the Output AVP which it is being mapped to. • Column: The reference to the CRD column for the input AVP. • List Of Output Column Avp Pairs (Mandatory): Defines the mapping between the AVP Names and the output columns defined in the selected STG. These mappings indicate how the output columns' values are mapped to AVPs after the CRD is evaluated. • Avp Name: The name of the AVP to which the value of the output column is mapped. The final STG from which you want to derive the output must have its output columns named Bearer-Authorization and Error-Message. The intermediate STGs used for chained evaluation can have any AVPs standard/non-standard. Supported values for Bearer-Authorization are Accept/Reject. In case the output column is not a standard AVP, then you can use any AVP Name (for example, Bearer-Throttling). But if this output column is chained into another STG's input column (for example, STG B's input column), then the AVP name for STG B's input column should also be Bearer-Throttling. • Column: The reference to the CRD column for the output AVP.

RxChargingParameterSTGConfiguration

The RxChargingParameterSTGConfiguration service configuration object sets the charging parameters for dedicated bearers created for IMS session (non-sponsored data case).

Table 234: RxChargingParametersSTGConfiguration Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Chargingparameterstg Name	References the Search table group containing the CRD tables that define the Qos Action.
List Of Input Column Avp Pairs (List)	See Common Parameter Descriptions, on page 508. The following is the list of supported AVP Names under Input Column: • AF-Application-Identifier • Media-Type • Flow-Status • Reservation-Priority • Flow-Number • Flow-Usage • AF-Signalling-Protocol • DPCC_NAME - Used to derive the Dynamic PCC rule from CRD tables. • DPCC_VALUE - Used to derive the Dynamic PCC rule from CRD tables.
List Of Output Column Avp Pairs (List)	See Common Parameter Descriptions, on page 508. The following is the list of supported AVP Names under Output Column: • Metering-Method • Offline • Online • Rating-Group • Service-Identifier • Reporting-Level • Precedence

RxDelayedMCDProcessing

RxDelayedMCDProcessing service configuration is used to delay the processing of media reported in AAR until it receives response for Gx RAR triggered based on Event-Triggers enabled based on RxTableDrivenEventTriggers, on page 493.

The following table describes the service configuration parameters:

Table 235: RxDelayedMCDProcessing Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	

Restrictions

RxDelayedMCDProcessing service configuration also requires defining the RxTableDrivenEventTriggers to determine the Event-Triggers to be sent on the dummy Gx RAR message.

When CPS evaluates the RxDelayedMCDProcessing and determines that a dummy Gx RAR is required to be triggered then CPS skips the Rx Authorization processing. No need to add specific condition on RxAuthorizationSTGConfiguration template to disable it when dummy RAR needs to be triggered.

A policy with policy-action "Create Sy Service Session" is required to be configured for selectively triggering Sy SLR only after dummy RAR response is received. But if the CPS service does not have "Balance Service" check-box enabled and selective Sy needs to be triggered after dummy RAR response is received then "Calculate service configuration - on demand" policy-action is required to be added before the policy-action for triggering the "Create Sy Service Session".

RxDRMPSTGConfiguration

The RxDRMPSTGConfiguration service configuration object sets the priority of the Gx-RAR diameter message using the DRMP AVP in the circumstance of high priority traffic (for example, Multimedia Priority Service (MPS)) from the Rx interface. The DRMP AVP value is derived based on the Reservation-Priority AVP and MPS-Identifier AVP. Both, Reservation-Priority AVP and MPS-Identifier AVP, must present in the AAR message.

Note Reservation-Priority AVP present at the message level in the AAR is only used. Reservation-Priority AVP present at Media-Component-Description level is not used.

Table 236: RxDRMPSTGConfiguration Service Configuration Parameters

Parameter	Description
D R M P Reservation Priority Table	The name of the STG that is referenced.
Drmp Output Column	The output column of the STG, whose value on evaluation of the table, sets the DRMP AVP to set the priority of the Gx-RAR diameter message.

Parameter	Description
List Of Input Column Avp Pairs (List)	Defines the mapping between the AVP names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in the STG. • Avp Name – The name of the AVP that is used as input for the CRD table evaluation. The following is the list of supported AVP names under Input Column: • Reservation-Priority • MPS-Identifier • Column – The key column in the STG that corresponds to the specified AVP.

RxGuaranteedBitRateOverride

The RxGuaranteedBitRateOverride service configuration object overrides the GBR, and sets it from the MBR value.

Table 237: RxGuaranteedBitRateOverride Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Set Guaranteed Bit Rate from Max Requested	This configuration is applicable when CPS is not able to derive guaranteed bit rate values based on the QoS derivation algorithm defined in 3GPP 29.213 specification. So if GBR is not derived and this service option is configured, then CPS copies the values derived for Max Requested Bitrates into Guranteed Bitrates (applicable for both UL and DL). Default: true
Set Guaranteed Bit Rate from Max Requested (Qos-Action)	Set this flag to true for copying the Max-Requested-Bitrate values into Guaranteed-Bitrate after QoS-Actions (RxSTGConfiguration) are applied. The bit rate values are copied only if the new QCI is < 5 and the Qos-Action on Guaranteed Bitrates (UL/DL) is Mirror. Default: false

For more information, refer to RxGaranteedBitRateOverride Service Configuration, on page 330.

RxQoSInformation

The RxQoSInformation service configuration option sets QoS values for Rx dedicated bearer.

Table 238: RxQoSInformation Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Qci	
Max Req Bandwidth U L	
Max Req Bandwidth D L	
Guaranteed Bit Rate U L	
Guaranteed Bit Rate D L	
Arp	

For more information, refer to RxQoSInformation Service Configuration, on page 329.

RxSponsoredDataChargingParameterSTGConfiguration

The RxSponsoredDataChargingParameterSTGConfiguration service configuration object configures the CRD details for setting charging parameters for dedicated bearers that are created for sponsored data.

Table 239: RxSponsoredDataChargingParameterSTGConfiguration Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Sponsored Datachargingparameterstg Name	References the Search table group containing the CRD tables that define the Qos Action.
List Of Input Column Avp Pairs (List)	See Common Parameter Descriptions, on page 508. DPCC_NAME - Used to derive the Dynamic PCC rule from CRD tables. DPCC_VALUE - Used to derive the Dynamic PCC rule from CRD tables.
List Of Output Column Avp Pairs (List)	See Common Parameter Descriptions, on page 508.

RxSTGConfiguration

The following parameters can be configured under RxSTGConfiguration service configuration:

Table 240: RxSTGConfiguration Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD tables that define the Qos Action for Rx specific dynamic rules (dedicated bearer).
List Of Input Column Avp Pairs (List)	Define the mapping between the 'AVP Names' and the key 'Columns' defined in the selected STG. These AVPs will be the inputs while evaluating the CRD table in STG. ColumnAndAvpPair: • Avp Name – The name of the Diameter AVP (received in Media Component Description AVP of the AAR message) that are used as input for CRD table evaluation. For example: Flow-Number, Media-Component-Number, MCPTT-Identifier, and so on. DPCC_NAME - Used to derive the Dynamic PCC rule from CRD tables. DPCC_VALUE - Used to derive the Dynamic PCC rule from CRD tables. • Column – References the key column defined in the selected STG.

Parameter	Description
List of Output Column Avp Pairs (List)	Define the mapping between the AVP Names and the output columns defined in the STG selected. These mapping indicate how the output column's values are mapped to AVPs after the CRD is evaluated. ColumnAndAvpPair: • Avp Name – Name of the diameter AVP (attribute from Qos-Information) to which the value of the output column should be mapped to while setting the Qos-Information for the dedicated bearer on Gx. (for example,“Qos-Class-Identifier”) Similarly for Qos-Actions on the attribute the AVP Name specifies the qos-action for a specific Qos-Information attribute (for example, “Qci”). To support WPS Handling with Dynamic ARP, output AVPs that allow the dynamic value expression and their ranges to be defined are defined in Table 241: WPS Handling with Dynamic ARP - Output AVPs, on page 487. • Column – References the key column defined in the selected STG. For more information on output column AVP pairs, refer to RxSTGConfiguration Service Configuration, on page 342.
Input Codec Data	See Table 242: Input Codec Data Parameters, on page 488.
Arp Precedence	Determines which RxSTGConfiguration to use for the new ARP eMPS feature.
Qos Precedence	Determines which RxSTGConfiguration to use for QCI lookup.
Disable Qos Change	When set to true, CPS disables modification of Dedicated bearer QoS. Default: false

Table 241: WPS Handling with Dynamic ARP - Output AVPs

Output AVP	Description
Dynamic-QoS-ARP-Priority-Level	(Mandatory if WPS Handling with Dynamic ARP is enabled): This AVP can be bound to the new dynamic expression Priority-Level (PL) column. If value is null/not configured, then the Dynamic QoS ARP feature is disabled. If the value is configured, it overrides the integer PL value (if configured). The dynamic PL expression is either expected to match the Java regular expression (^[dD](\\ s*([+- /*]) \ \ s*([0 - 9]+))?$) or or must be an offset value (of syntax: [+-][0 - 9]+). In case the value is provided in the offset form, the "D" is implicit. Thus "+8" corresponds to "D+8" in expression form, "-5" corresponds to "D-5" and similarly, "0" corresponds to "D".
Dynamic-QoS-ARP-Priority-Level- Default	(Optional) In case the default bearer does not have a Priority-Level, this value is used as dedicated bearer PL. If the value is null/not configured, the default value (15) is used.
Dynamic-QoS-ARP-Priority-Level-Min	(Optional) This output AVP provides upper/lower bound for the calculated PL value using the dynamic expression provided under Dynamic-QoS-ARP-Priority-Level. If the value is null/ not configured, the default value (1) is used.
Dynamic-QoS-ARP-Priority-Level-Max	(Optional) The upper end of the valid PL range. If the value is null/not configured, the default value (15) is used.
Dynamic-QoS-Update-On-Change	(Optional) This AVP controls whether the Rx rules must be updated on change in the dynamic PL value (for example, due to change in default bearer PL value). If the value is null/not configured, the Rx rules are not updated with new dynamic PL value once installed.
Dynamic-QOS-ARP-Preemption-Capability	(Optional): This AVP can be bound to the new dynamic Pre-Emption Capability (PC) column. If value is null/not configured, then the Dynamic QoS ARP PC handling is disabled. If the value is configured "D", it overrides the PC value of the dedicated bearer with the Default Bearer PC.

Output AVP	Description
Dynamic-QOS-ARP-Preemption-Vulnerability	(Optional): This AVP can be bound to the new dynamic Pre-Emption Vulnerability (PV) column. If value is null/not configured, then the Dynamic QoS ARP PV handling is disabled. If the value is configured “D”, it overrides the PV value of the dedicated bearer with the Default Bearer PV.

Note

- Using the offset form may have minor performance gains as compared to full expression.
- Range limits are not applied for default dynamic values.
- Dynamic expression has an implicit “Enforce” QoS action. The Action column value is ignored.
- If the dynamic expression configured for Priority-Level is invalid, CPS ignores the expression and does not include the ARP parameters (since PL is set as null) in the rule install. This is true even if absolute PL value is configured (absolute value is ignored).

Table 242: Input Codec Data Parameters

Parameter	Description
Prefer Answer	Supported values are: • true – CPS uses the first Codec-Data AVP with "answer" on the second line, or the first Codec-Data AVP with "offer" if there is no Codec-Data AVP with "answer". • false – CPS uses the first Codec-Data AVP with "offer" or "answer" on the second line if AAR request has multiple 'Codec-Data' AVPs.

Parameter	Description
Input Columns Media Format	InputCodecMediaFormatColumns • Column Encoding Name – Column from a Search Table Group and a corresponding Custom Reference Data Table for QoS information. The encoding name extracted from the a:rtpmap line is used to match the column in the Search Table Group and the corresponding Custom Reference Data Table. • Column Clock Rate – Column from a Search Table Group and a corresponding Custom Reference Data Table for QoS information. The clock rate extracted from the a:rtpmap line is used to match the column in the Search Table Group and the corresponding Custom Reference Data Table. • Column Encoding Parameters – Column from a Search Table Group and a corresponding Custom Reference Data Table for QoS information. The encoding parameters extracted from the a:rtpmap line is used to match the column in the Search Table Group and the corresponding Custom Reference Data Table. • List of Input Column Parameter Pairs • Parameter – Media Specific Parameter name in the a:fmtp line to extract the value from. For example, mode-set, octet-align. • Default – Optional default parameter value. If Codec-Data AVP does not include the SDP parameter, the default value is used. • Column – Column from a Search Table Group and a corresponding Custom Reference Data Table for QoS information. The parameter value extracted from the standalone line or the default value is used to match the column in the Search Table Group and the corresponding Custom Reference Data Table.
List of Input Columns Sdp Pairs	InputCodecParameterColumnPair • Parameter – SDP parameter name in the standalone line to extract the value from. For example, "a=ptime". • Default – Optional default parameter value. If Codec-Data AVP does not include the SDP parameter, the default value is used. • Column – Column from a Search Table Group and a corresponding Custom Reference Data Table for QoS information. The parameter value extracted from the standalone line or the default value is used to match the column in the Search Table Group and the corresponding Custom Reference Data Table.

Parameter	Description
Media Comp Rtpmap Payload Type Index	Indicates which RTP map line to be used for codec matching. For example, index 2 indicates that the second rtp-map/fmtp line in codec AVP is used for configuration matching. To disable this parameter, the value must be less than 1. **Restriction** If Media Component Description AVP comes with multiple codec-data AVP (offer and answer), then in order to select the codec-data with answer, "prefer_answer" configuration has to be enabled under service option. If the configuration is not enabled, first codec-data is used for configuration matching, which means offer is expected to be first codec-data.

Note

- CPS supports default values for media specific parameters in `a=fmtp` line and SDP standalone lines.
- CPS supports SDP standalone lines in the form of **`<char>=<name>:<value>`**.

For more information, see Basic Options, on page 163.

RxSTGDefaultBearerConfiguration

RxSTGDefaultBearerConfiguration service configuration is used for CRD evaluation of default bearer QoS on receiving Rx AAR with Dynamic-PCC-Requested-QoS AVP. The same service configuration can also be used to support modification of default bearer based on MPS-Identifier, MCPTT-Identifier, and Reservation-Priority received in AAR from P-CSCF.

The following parameters can be configured under RxSTGDefaultBearerConfiguration service configuration for both use cases:

Table 243: RxSTGDefaultBearerConfiguration Service Configuration Parameters (Use Case - Rx AAR having Dynamic-PCC-Requested-QoS AVP)

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD tables that define the Qos Action for Rx specific dynamic rules (dedicated bearer).

Parameter	Description
List Of Input Column Avp Pairs (List)	Defines the mapping between the 'AVP Names' and the key 'Columns' defined in the selected STG. These AVPs are the inputs while evaluating the CRD table in STG. ColumnAndAvpPair: • Avp Name – The name of the Diameter AVP (received in Media Component Description AVP of the AAR message) that is used as input for CRD table evaluation. Supported input AVPs are: • AF-Application-Identifier • Flow-Number • Flow-Usage • Intention • QoS-Class-Identifier • Priority-Level • Pre-emption-Capability • Pre-emption-Vulnerability • DPCC_NAME • DPCC_VALUE • Application-Service-Provider-Identity • Media-Type • Sponsor-Identity • Service-Info-Status The value of AVP names must be exact same as per specifications while defining input columns. • Column – References the key column defined in the selected STG.

Parameter	Description
List of Output Column Avp Pairs (List)	ColumnAndAvpPair: • Avp Name – The name of the diameter AVP (attribute from Qos-Information) to which the value of the output column should be mapped while setting the Qos-Information for the dedicated bearer on Gx. Supported list of output AVPs are: QoS-Class-Identifier, APN-Aggregate-Max-Bitrate-DL, APN-Aggregate-Max-Bitrate-UL, Max-Requested-Bandwidth-DL, Max-Requested-Bandwidth-UL, Guaranteed-Bitrate-DL, Guaranteed-Bitrate-UL, Priority-Level, Pre-emption-Capability, and Pre-emption-Vulnerability Similarly, for Qos-Actions on the attribute, the AVP Name specifies the qos-action for a specific Qos-Information attribute; supported corresponding action AVPs are: Qci, Apn Agg Max Bit Rate U L, Apn Agg Max Bit Rate D L, Priority Level, Preemption Capability, and Preemption Vulnerability Actions for Max-Requested-Bandwidth and Guaranteed-Bitrate AVPs is always be enforced. If value is present and is not null in CRD then that value is enforced otherwise CPS takes no action and does not change the Max-Requested-Bandwidth and Guaranteed-Bitrate. • Column – References the output column defined in the selected STG.

Table 244: RxSTGDefaultBearerConfiguration Service Configuration Parameters (Use Case - Getting MPS Identifier and Reservation Priority AVP in AAR for Emergency Services)

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD tables that define the Qos Action for Rx specific dynamic rules (dedicated bearer).

Parameter	Description
List Of Input Column Avp Pairs (List)	Defines the mapping between the 'AVP Names' and the key 'Columns' defined in the selected STG. These AVPs are the inputs while evaluating the CRD table in STG. ColumnAndAvpPair: • Avp Name – The name of the Diameter AVP (received in AAR message) that is used as input for CRD table evaluation. Supported input AVPs are: • Reservation-Priority • MPS_Identifier • MCPTT-Identifier The value of AVP names must be exact same as per specifications while defining input columns. • Column – References the key column defined in the selected STG.
List of Output Column Avp Pairs (List)	ColumnAndAvpPair: • Avp Name – The name of the diameter AVP (attribute from Qos-Information) to which the value of the output column should be mapped while setting the Qos-Information for the dedicated bearer on Gx. Supported list of output AVPs are: • QoS-Class-Identifier • Priority-Level • Pre-emption-Capability • Pre-emption-Vulnerability Actions for QoS-Class-Identifier, Priority-Level, Pre-emption-Vulnerability, and Pre-emption-Capability AVPs is always enforced. If value is present and is not null in CRD then that value is enforced otherwise CPS takes no action and does not change the QoS-Class-Identifier, Priority-Level, Pre-emption-Vulnerability, and Pre-emption-Capability. • Column – References the output column defined in the selected STG.

RxTableDrivenEventTriggers

RxTableDrivenEventTriggers service configuration is used to derive a list of event-triggers that CPS should subscribe based on table evaluation. The input columns to this table are the Media-Component-Description AVP values or any other input parameters (derived from gx-session) and the output columns give the list of applicable event-triggers. Based on the selection logic user can configure any AVP received at MCD level to the input columns. In the CRD table, output columns can give an event-trigger number. So, there can be multiple output columns depending upon the number of event-triggers that are to be supported. You need to configure all these output columns that derive the event-trigger number in the service configuration.

This service configuration is also used for configuring the STG used to specify the event-triggers to be sent in dummy GxRAR. In this case, the same service option needs to be linked to two separate CRD tables (Rx-Table or dummy RAR Event-Trigger table). So, these service-options are created by modifying the RxTableDrivenEventTriggers Use Case Template with Use Case Initiator conditions that checks for triggering dummy RAR. This avoids enabling both the service option at the same time.

The following table describes the service configuration parameters:

Table 245: RxTableDrivenEventTriggers Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	References the Search table group containing the CRD tables that define the Qos Action for Rx specific dynamic rules (dedicated bearer).
List Of Input Column Avp Pairs (List)	Defines the mapping between the 'AVP Names' and the key 'Columns' defined in the selected STG. These AVPs are the inputs while evaluating the CRD table in STG. ColumnAndAvpPair: • Avp Name – The name of the diameter AVP that is used as input for CRD table evaluation. • Column – References the key column defined in the selected STG.
List of Output Column Avp Pairs (List)	ColumnAndAvpPair: • Avp Name – The name of the diameter AVP to which the value of the output column should be mapped. The output AVP name mapping indicates how the output column's values are mapped to AVPs after the CRD is evaluated. • Column – References the output column defined in the selected STG.

Restrictions

When using RxTableDrivenEventTriggers for both Rx-Table event-triggers and dummy RAR event-triggers, the template must be configured with modify conditions to have two service options that can be linked to the two STG tables. The condition to modify the template for dummy RAR event-triggers must be set as per the requirement to trigger the dummy Gx RAR message.

If dummy RAR Event-Trigger table indicates no new Event-Triggers are required then the actual RAR with bearer installation will not have the correct subscription based on the Rx Table (since the Rx table event-triggers will not get evaluated). Therefore, a limitation would be that whatever entries having event-trigger subscription in Rx-Table for specific media-type that media-type will also have corresponding event-triggers enabled for dummy RAR event-trigger table also.

EvaluateRxDedicatedBearer

The EvaluateRxDedicatedBearer service configuration object evaluates the Rx dedicated bearer depending on the trigger for the policy evaluation.

Table 246: EvaluateRxDedicatedBearer Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	
List Of Input Column Avp Pairs (List)	
List Of Output Column Avp Pairs	

EvaluateRxDedicatedBearerCreate

The EvaluateRxDedicatedBearerCreate service configuration object evaluates media sub-components from AAR's Initial request and uses it to determine if dedicated bearer needs to be created based on CRD lookup.

Table 247: EvaluateRxDedicatedBearer Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Stg Name	
List Of Input Column Avp Pairs (List)	
List Of Output Column Avp Pairs	

ThrottleRxBasedOnBearer

The ThrottleRxBasedOnBearer service configuration object enables you to throttle default bearer.

Table 248: ThrottleRxBasedOnBearer Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Qci	
Allocation Retention Priority	
Max Required Bandwidth U L	
Max Required Bandwidth D L	

ThrottleRxBasedOnMediaType

The ThrottleRxBasedOnMediaType service configuration object enables you to throttle Rx calls based on media type.

Table 249: ThrottleRxBasedOnMediaType Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Q O S Allocation Parameters (List)	List of parameters that can be configured to enable you to throttle Rx calls with the media type as follows: • Media Type - Type of Media. • Bandwidth Allocation For Media Type - Allocated bandwidth for the selected media type. • Percentage Allocation For R T P - Corresponding percentage of the bandwidth that needs to alloctaed for RTP. • Percentage Allocation For R T C P - Corresponding percentage of the bandwidth that needs to alloctaed for RTPC.

RxClient Service Configuration Objects

BindingDbHealthCheck

The BindingDbHealthCheck service configuration object is used to configure PCRF to initiate a message that results in sending dummy AAR to PolicyDRA to check if binding is available at PolicyDRA and allowing the PCRF to take corrective action based on the response.

Table 250: BindingDbHealthCheck Service Configuration Parameters

Parameter	Description
Enable Health Check	This field is used to enable the feature for a particular APN. This field can be read from a CRD table which has mapping to an APN name.
Destination Realm	This field notifies the destination realm of the Policy DRA or Rx peer.

Note The dummy AAR sent by PCRF for PolicyDRA binding database health check is routed back to PCRF. This dummy AAR has to be ignored/rejected. To identify the dummy (health-check) AAR the diameter session ID is appended with **BindingDbCheck** keyword. When PCRF receives an AAR with session ID ending with **BindingDbCheck** keyword, it needs to be replied by using RequestReject configuration that must be enabled using the condition that makes use of session ID having **BindingDbCheck** keyword. For configuration, refer to RequestReject , on page 421.

Note To improve the performance when PolicyDRA Health Check is enabled, you must configure ‘RxClientSessionKey’ key as the Lookaside Key Prefix so that memcache is used and full database scan is avoided. This is highly recommended for higher capacity systems.

Sd Service Configuration Objects

This section describes the parameters for the following Sd Service Configuration Objects:

ADCPreconfiguredRule

The ADCPreconfiguredRule service configuration object configures a dynamic application detection rule.

Table 251: ADCPreconfiguredRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rule Group	Not used
Rule Name	Not used
Adc Rule Name	The name of the ADC rule.
Tdf Application Identifier	See Common Parameter Descriptions, on page 508.
Flow Status	
Mute Notification	
Monitoring Key	
QoS Information	QoSInformation For detailed information about the following parameters, see Common Parameter Descriptions, on page 508. • Max Req Bandwidth U L • Max Req Bandwidth D L • Guaranteed Bit Rate U L • Guaranteed Bit Rate D L • Apn Agg Max Bit Rate U L • Apn Agg Max Bit Rate U L • Arp
Redirect Information	RedirectInformation For detailed information about the following parameters, see Common Parameter Descriptions, on page 508. • Redirect Address Type • Redirect Support • Redirect Server Address

ADCPredefinedRule

The ADCPredefinedRule object configures a static ADC rule.

Table 252: ADCPredefinedRule Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rule Group	
Rule Name	

ADCPredefinedRuleBase

The ADCPredefinedRuleBase object configures a predefined group of ADC rules. The group can contain predefined, pre-configured, dynamic, and predefined rule base rules.

Table 253: ADCPredefinedRuleBase Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Rule Group	
Rule Name	

EventTrigger

The EventTrigger service configuration object specifies the event to be sent.

Table 254: EventTrigger Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Event Trigger	

SdDynamicRuleReference

The SdDynamicRuleReference service configuration object is used to define the CRD table and column details for determining the rule-name and charging-parameters for the Sd Sponsored Data Dynamic PCC Rule.

Table 255: SdDynamicRuleReference Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
STG Table	The name of the Search Table group table that is being referenced.
List Of Input Column Avp Pairs (List)	See Common Parameter Descriptions, on page 508.
List Of Output Column Avp Pairs (List)	
Retry Pcc Rules On Failure	Can be set to true or false. Default: false

SdDefaultBearerQosADCRuleConfiguration

The SdDefaultBearerQosADCRuleConfiguration service configuration object is used to derive ADC rules.

The following Query Table Input/Output can be used:

- Inputs:
  - LDAP Attributes
  - Sy-Counter-Id and Sy-Counter-Status
  - Gx-Attributes: APN, Roaming-Status (RMS Table) and so on
- Output: ADC-Rule-Name, TDF-Application-Identifier, Event-Trigger

Table 256: SdDefaultBearerQosADCRuleConfiguration Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	

Parameter	Description
Crd Tables (List)	QueryTable Each Query Table represents a Customer Reference Data table. The application references the Input List and selects parameters and values along with it to query the table. Provide the input and output parameters according to your requirements. • **Table name** – Click the **...** button, and select a table name from the list. • Input List (List) – Click the arrow to expand the contents. InputColumnObject – Click the arrow to expand the contents. • **Crd Column** – Click the **...** button, and select a CRD column from the list. • **Referenced Output Column** – Click the **...** button, and select an output column from the list. • **Column Value** – Enter the column value. • **Referenced MultiValue AVP Name** – Enter the referenced multi-value AVP name. • Output List (List) – Gives the application relevant hints on how to use the query results. OutputColumnObject • **Crd Column** – Click the **...** button, and select a CRD column from the list. • **Target Avp Name** – Enter the target AVP name. • **Query Order** – Enter a numeric value. (The default is 0.) QPS determines the Query Table that needs to be queried based on the Query Order. The Query Order is based on the ascending order of precedence, that is, 0 > 1 > 2 > 3 and so on. **Restriction** All inputs to CRD table must be through retrievers only.
Realm	See Common Parameter Descriptions, on page 508. This value provides the information on the TDF node to which the Sd Diameter Interface connects.

SdToggleMonitoringKey

The SdToggleMonitoringKey service configuration object defines the monitoring-key to be used for the Sponsored Data Dynamic PCC Rule.

Table 257: SdToggleMonitoringKey Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Monitoring Key	

Service Configuration Objects

This section describes the parameters for the following Service Configuration Objects:

ServiceNotification

ServiceNotificationservice configuration under the"service" section needs to be configured for the subscriber service to trigger notifications.

Table 258: ServiceNotification Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Enable Rx Service	If this is set to false, no device indicator notification will be sent for Rx event. Possible values are true or false.
Enable Sd Service	If this is set to false, no device indicator notification will be sent for Sd event. Possible values are true or false.
Enable Sy Service	If this is set to false, no device indicator notification will be sent for Sy event. Possible values are true or false.
Enable Dscp Service	If this is set to false, no device indicator notification is sent for DSCP event. Default: false
Rx Service Crd Column	Resultcolumn of the CRD table. Value in this column specifies whether to send device notification or not for Rx event. To send device notification the value in the column should be"ON". Value other than "ON" will result in no device notification.

Parameter	Description
Sy Service Crd Column	Result column of the CRD table. Value in this column specifies whether to send device notification or not for Sy event. To send device notification the value in the column should be "ON". Value other than "ON" will result in no device notification.
Sd Service Crd Column	Result column of the CRD table. Value in this column specifies whether to send device notification or not for Sd event. To send device notification the value in the column should be "ON". Value other than "ON" will result in no device notification.
Dscp Service Crd Column	Result column of the CRD table. Value in this column specifies whether to send device notification or not for Dscp event. To send device notification the value in the column should be "ON". Value other than "ON", results in no device notification.
Sy Service STG	ServiceSTGConfiguration: STG Configuration for Sy Event. • Search Table Group: CRD table to decide whether to send device notification for the Sy event. • List of Input Column Avp pair (List): This is the list of column and AVP pair and is used as input to the CRD table. ColumnAndAvpPair: In the column and AVP pair, column is the column in the CRD table and AVP name is AVP received in SNR on Sy. While searching the table the values of the AVPs are populated for the corresponding table column. AVP name can have Policy-Counter-Identifier or Policy-Counter-Status as values.
Sd Service STG	ServiceSTGConfiguration: STG Configuration for Sd Event. • Search Table Group: CRD table to decide whether to send device notification for the Sd event. • List of Input Column Avp pair (List): This is the list of column and AVP pair and is used as input to the CRD table. ColumnAndAvpPair: In the column and AVP pair, column is the column in the CRD table and AVP name is AVP received in CCR-U on Sd. While searching the table the values of the AVPs are populated for the corresponding table column. AVP name can have TDF-Application-Identifier or Sponsor-Identity as values.
Initial Off On C C R I	Default: true
Initial Off On Sy S L A	Default: false

Parameter	Description
Dscp Service STG	ServiceSTGConfiguration: STG Configuration for DSCP Event. • Search Table Group: CRD table to decide whether to send device notification for the DSCP event. • List of Input Column Avp pair (List): This is the list of column and AVP pair and is used as input to the CRD table.

Sy Service Configuration Objects

This section describes the parameters for the following Sy Service Configuration Object:

SpendingLimitReport

The SpendingLimitReport service configuration object is used for the 3GPP Sy interface. The Sy reference point is located between the Policy and Charging Rules Function (PCRF) and the Online Charging System (OCS). The Sy reference point enables transfer of policy counter status information relating to subscriber spending from OCS to PCRF and supports the following functions:

- Request of policy counter status reporting from PCRF to OCS, and subscribe to or unsubscribe from spending limit reports (notifications of policy counter status changes).
- Notification of spending limit reports from OCS to PCRF.
- Cancellation of spending limit reporting from PCRF to OCS.

Table 259: SpendingLimitReport Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	

Parameter	Description
Subscriber Id (List)	Identifier – The user identity, which is mapped to the Subscription-Id AVP. Based on your requirements, you can configure one or more identifiers. Possible values for identifiers include: • Session MSISDN – The MSISDN value of the subscriber. • Session IMSI – The IMSI value of the subscriber. Skip Subscriber Id in SLR Initial – Flag to skip configured Subscriber id in SLR initial. When set to true, skips configured subscriber id in SLR initial. When set to false, subscriber id is sent in SLR initial. Default value is false. Skip Subscriber Id in SLR Intermediate – Flag to skip configured subscriber id in SLR intermediate. When set to true, skips configured subscriber id in SLR intermediate. When set to false, subscriber id is sent in SLR intermediate. Default value is false.
Asynchronous	This parameter can be set to true or false. True – Use asynchronous mode for Sy interface (PCRF will not wait for SLA response from OCS before sending the message on another interface like Gx.) False – Use synchronous mode for Sy interface (PCRF waits for the SLA response from the OCS or SLA timeout before sending the message on another interface like Gx.) Asynchronous mode is preferred.
Retry Time Seconds	Not used.
Realm	The Sy peer realm (OCS) where the message needs to be sent from PCRF.
Identifier (List)	Identifier Name – The subscribed Sy Policy Counter Identifier list, which maps to the Policy-Counter-Identifier AVP. PCRF uses this list to send the Policy-Counter-Identifiers to the OCS in the SLR message. If this list is blank, the PCRF requests subscription to all available policy counters.
Defaults On Failure (List)	DefaultSpendingLimitReport – The default list of Policy Counter Identifiers that are subscribed to in case of failures. This parameter is optional. • Failure Reason – One of the failure codes from the drop-down list for which the default identifier and it's status is given below. • Identifier – The policy counter identifier name. • Status – The policy counter identifier status.

Parameter	Description
Subscriber Id In S T R	This parameter can be set to true or false. It specifies whether to send subscriber-id AVP in the STR message. This is a custom feature, and is not as per 3GPP standards. Default: false
Subscriber Id In S N A	This parameter can be set to true or false. It specifies whether to send subscriber-id AVP in the SNA message. This is a custom feature, and is not as per 3GPP standards. Default: false
Force Create Session	This parameter can be set to true or false. When set to true, it initiates a new Sy session (if one does not already exist) irrespective of the policy event or the re-initiation count/time. Default: false
Resend Counter In SLR Inter Mediate	When this flag is set to true, CPS sends counter in SLR intermediate. Default value is false.
Receive Unknown Counter	When this flag is set to true, CPS honors the unknown counters received in SNR message. Default value is false.
Update Next Evaltime of session On Expiry	When this flag is set to true, CPS keeps sending check-alive SLR based on stale session configuration and does not extend time of check-alive SLR if SNR is received.

SyAction

The Sy Action service configuration object is used to send the SLR-U during policy counter-conflicts.

Table 260: SyAction Service Configuration Parameters

Parameter	Description
Priority	The priority of the message for processing. The higher the number, the higher the priority. Default for most settings: 0
Diameter Client	The client configuration is used to apply different policies based on OCS type. To filter a service based on the Diameter client, specify which Diameter client you want the service to be applied to. Diameter clients are configured in **Policies** > **Diameter Clients**. This parameter is optional.

Parameter	Description
Send SLR-Intermediate	When this parameter is set to true, CPS sends an SLR-U with a list of currently subscribed policy counter-identifiers. Default value is false.
SLR-Intermediate Max Retry	Number of retry attempts allowed on a non-successful SLR-Intermediate request. Default value is 1.

TableDrivenActionOverSy

TableDrivenActionOverSy service configuration is used to evaluate and retrieve action to be taken over Sy interface on receiving messages. On each policy evaluation (including Gx CCR-U), if TableDrivenActionOverSy is found in policy, CPS evaluates the referenced table and determine the Action to be executed on the Sy interface. If the Action value is **Update**, CPS then initiates a sync SLR-Inter message (provided Sy session exists). When the SLR-Inter response is received (Result Code 7000 if there is timeout), CPS reevaluates the TableDrivenActionOverSy configuration and determines the next Action. If that Action is **Reinitiate**, CPS terminates the existing session and initiates a new one (by sending an SLR-Initial).

When CPS terminates the existing session, if the **Standard Sy** flag is false, the STR message is not sent out and instead the session is cleaned up immediately. If the Standard Sy flag is true, then a sync Sy STR is sent out. On receiving response (can be success or failure or timeout), CPS cleans up the session.

Note To allow TableDrivenActionOverSy to be evaluated properly for timeouts, the Policy Director (LB) node must send back the 7000 response before the Sync action (for sending SLR-Inter message) times out. Also, CPS by default, retries the timed out request once directly from the Policy Director (LB) node.

Table 261: TableDrivenActionOverSy Service Configuration Parameters

Parameter	Description
Priority	See Common Parameter Descriptions, on page 508.
Diameter Client	
Search Table Group	Search Table Group table that is being referenced. The STG (and the contained CRDs) can also contain key columns that do not directly refer to Diameter AVPs in the trigger message. For example, Outputs of other tables. These columns must be bound correctly.
Input Column Binding (List)	ColumnAndAvpPair • Avp Name: The name of the Diameter AVP that is used as input for CRD table evaluation. • Column: The key column in the STG that corresponds to the specified AVP.

Parameter	Description
Output Column Binding (List)	ColumnAndAvpPair • Avp Name: The name of the Diameter AVP to which the value of the output column is mapped. • Column: The reference to the CRD column for the output AVP. **Note** The list of Output column to AVP bindings currently supports only one column/AVP binding for fixed AVP code **Action-Over-Sy**.

Note TableDrivenActionOverSy service configuration only accepts trigger Diameter message AVPs for Input column binding. Thus, the AVP Code has to exactly match to what is received in the message. In addition to message AVPs, the following AVP codes can be used as input AVP codes:

- Command-Code: To use command code of trigger message as Input key.
- Application-Id: The Diameter Application Identifier for the trigger message

UDC Client Service Configuration Objects

ADTMAttribue

The ADTMAttribue service configuration object is used to specify the attribute name which should be a LDAP attribute.

The following table describes the service configuration parameters:

Table 262: ADTMAttribue Service Configuration Parameters

Parameter	Description
Attribute Name	This parameter is used by CPS to inform UDC about the attribute update.
Logical Apn	Specifies the different Logical APN values for the encoded LDAP Attribute value.

For more information, refer to *ADTMAttribute Service Configuration Object* section in *CPS UDC Guide*.

Common Parameter Descriptions

These parameters are common between many service configuration objects. They are listed in alphabetical order.

Table 263: Common Service Configuration Object Parameters

Parameter	Description
Apn Agg Max Bit Rate DL	Defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN.
Apn Agg Max Bit Rate UL	Defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN.
Arp	AllocationRetentionPriority • Priority Level – Priority-Level AVP value. • Preemption Capability – Preemption-Capability AVP value • Preemption Vulnerability – Preemption-Vulnerability AVP value.
Balance Code	Indicates with which balance the quota is associated. You can subscribe to multiple balances, but the monitoring key is associated with one balance.
Diameter Client	The client configuration is used to apply different policies based on PCEF type. To filter a service based on the Diameter client, specify which Diameter client you want the service to be applied to. Diameter clients are configured in the **Reference Data** > **Diameter Clients** > **Diameter Clients** section of the interface. This parameter is optional.
Dosage	How much quota to initially give the client (in bytes). Default: 0
Dual Stack Session	Can be set to enabled or disabled. Default: disabled
Enable Resource Allocation Notification	Can be set to enabled or disabled. Default: disabled
Encoding Format	Can be set to true or false. If the Monitoring Key parameter is numeric, set this parameter to true. Default: false
Event Trigger	Used primarily to notify the starting and stopping of applications or to report usage. It is not used to rerequest rules.
Flow Status	Defines whether the service data flow is enabled or disabled.

Parameter	Description
Framed I P Type	Can be set to one of the following options: • ANY_ONE • BOTH • IPv4_ADDRESS • IPv6_ADDRESS Default: ANY_ONE
Guaranteed Bit Rate DL	Defines the guaranteed bit rate allowed for the downlink direction.
Guaranteed Bit Rate UL	Defines the guaranteed bit rate allowed for the uplink direction.
List of Input Column Avp Pairs (List)	Defines the mapping between the AVP Names and the key columns defined in the selected STG. These AVPs are used as inputs while evaluating the CRD table in STG. • Avp Name – The name of the Diameter AVP that is used as input for CRD table evaluation. For example: Flow-Number, Media-Component-Number, and so on. • Column – The key column in STG that corresponds to the specified AVP.
List Of Output Column Avp Pairs (List)	Defines the mapping between the AVP Names and the output columns defined in the selected STG. These mappings indicate how the output columns' values are mapped to AVPs after the CRD is evaluated. • Avp Name – The name of the Diameter AVP to which the value of the output column is mapped while setting the charging parameters on the dynamic rule (for the Dedicated Bearer). For example: Rating-Group Service-Identifier. • Column – The output column defined in the selected STG.
Max Req Bandwidth DL	Defines the maximum bit rate allowed for the downlink direction.
Max Req Bandwidth UL	Defines the maximum bit rate allowed for the uplink direction.
Monitoring Key	Identifies a usage monitoring control instance. You can specify any value.
Monitoring Level	Can be set to one of the following values: • SESSION_LEVEL (0) • PCC_RULE_LEVEL (1) • ADC_RULE_LEVEL (2)
Mute Notification	Indicates whether notifications for application starts and stops are muted for ADC Rule by the TDF.

Parameter	Description
New String Value	The new string value that is used to overwrite the “String Value” if the value of “String Value” field matches exactly with the value of “String Value To Override”.
Online	Defines whether the online charging interface from the PCEF for the associated PCC rule is enabled. The default charging method provided by the CPS takes precedence over any preconfigured default charging method at the PCEF. • Enable: Indicates that the online charging interface for the associated PCC rule is enabled. • Disable: Indicates that the online charging interface for the associated PCC rule is disabled.
Offline	Defines whether the offline charging interface from the PCEF for the associated PCC rule is enabled. The default charging method provided by the CPS takes precedence over any preconfigured default charging method at the PCEF. • Enable: Indicates that the offline charging interface for the associated PCC rule is enabled. • Disable: Indicates that the offline charging interface for the associated PCC rule is disabled.
Precedence	Defines the second level priority when the highest priority matches among the multiple generic service configurations.
Preemption Capability	When provided within the QoS-Information AVP, the AVP defines whether a service data flow can get resources that were already assigned to another service data flow that has a lower priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the Default Bearer can get resources that were already assigned to another bearer with a lower priority level. • 0: Indicates that the service data flow or bearer is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. • 1: Indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.

Parameter	Description
Preemption Vulnerability	When provided within the QoS-Information AVP, the AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow that has a higher priority level. If it is provided within the Default-EPS-Bearer-QoS AVP, the AVP defines whether the Default Bearer can lose the resources assigned to it in order to admit a pre-emption capable bearer with a higher priority level. • 0: Indicates that the resources assigned to the service data flow or bearer can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied. • 1: Indicates that the resources assigned to the service data flow or bearer cannot be pre-empted and allocated to a service data flow or bearer with a higher priority level.
Priority	The priority of the message for processing. The higher the number, the higher the priority. Default for most settings: 0
Priority Levels	Used to decide whether a bearer establishment or modification request can be accepted, or rejected due to resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest level of priority. • Values: 1 to 8 – Assigned for services that are authorized to receive prioritized treatment within an operator domain. • Values: 9 to 15 – Assigned to resources that are authorized by the Home network and thus applicable when a UE is roaming.
Provision Default Bearer QoS	Must be bound to the appropriate column in the STG. The data contained in the STG column is of type True/False. If the value is True, the Default Bearer QoS information from the session is applied to the rule, while QoS information derived from the prior parameters in this STG is ignored.

Parameter	Description
Qci	The Quality of Service (QoS) Class Identifier. The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction. The QCI values 0, 10 to 255 are divided for usage as follows: • 0: Reserved • 10-127: Reserved • 128-254: Operator specific • 255: Reserved
Rating Group	The charging key for the PCC rule used for rating purposes.
Realm	The destination realm where the message is sent from PCRF.
Redirect Address	Indicates the target for redirected application traffic.
Redirect Address Type	Defines the address type of the address given in the Redirect-Server-Address AVP. Default: IPV4_ADDRESS
Redirect Server Address	Indicates the target for redirected application traffic.
Redirect Support	This value indicates that Redirection is enabled for a detected application's traffic.
Retry Profile	Indicates the Rule Retry Profile to be used. When CPS receives a Charging-Rule-Report indicating failure to install or to activate one or more rules, it evaluates the failed rules and takes further action.
Rule Group	Used to classify rules at PCRF to change set of predefined rules based on policy. This parameter is optional.
Rule Name	A partial name configured in Policy Builder (as derived using AF-Application-Identifier and Media-Type values from the Custom dynamic rule name table in Gx Client). Default: AF

Parameter	Description
Scheduled Hour	Can be set to one of the following values: **Default:** Turns off the Hour Boundary RAR enhancement feature for look-ahead rules installation at hour boundary. This causes rules to be installed at hour boundary as applicable. **CurrentHour:** Rule activation time will be current time, deactivation time will be the next hour. **NextHour:** Rule activation time will be the next hour, and deactivation time will be next-next hour.
Search Column	Must be bound to the Key column in the STG. The data contained in the STG column is of type Text.
Search Group	A constant value that CPS uses to search within the Search Table Group indicated by the Search Table parameter.
Search Table	The name of the table from which to perform a lookup.
String Value to Override	Indicates whether overriding is required. For virtual services, if the value of “String Value” field matches exactly with the value of “String Value To Override”, then the value of “String Value” is over written with the “New String Value".
Tdf Application Identifier	References the application detection filter (for example, its value may represent an application such as a list of URLs) to which the PCC rule for application detection and control in the PCEF applies.
ToD Schedule	Identifies the schedule for rule activation and deactivation.