CPS Central Administration Guide, Release 24.1.0

First Published: 2024-03-14

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

CONTENTS

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

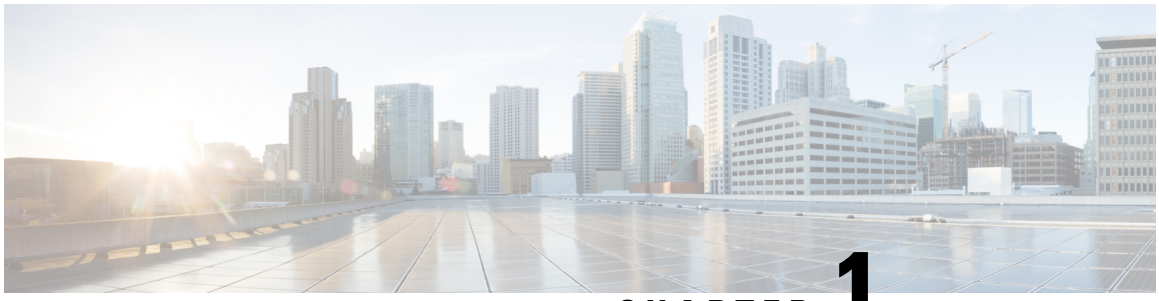
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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

About CPS Central

Central Overview

CPS Central is a consolidated GUI platform that enables users to perform Policy Builder (PB) configurations, manage custom reference table data, and launch the following CPS web-based applications and utilities:

- Policy Builder
- Custom Reference Data
- Operations
  - User Interfaces
  - API Information

Central Architecture

The CPS Central system is built using the following major frameworks:

1. Webpack
2. Babel
3. vue.js
4. Node Package Manager
5. Bootstrap

The following section describes the components of CPS Central:

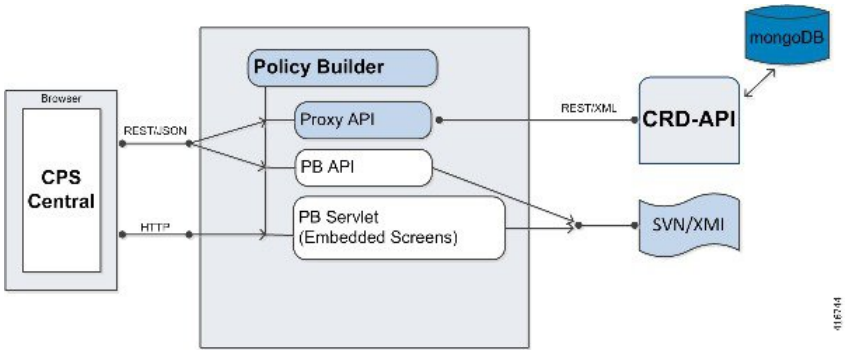
- PB API: Processes HTTP requests and contains the following two API sets :

- Utilizes the existing PB service API for user login authentication, multi-repositories, and publish operations.
- Serves as a proxy layer to interface with CRD-API and to support CRD data management.

While the PB API is composed of the two API sets described above, both are accessible from the CPS Central interface.

- PB Servlet: Supports PB embedded screens to provide the existing Policy Builder parity functions. Both PB basic and advanced operations are supported.
- Client GUI: CPS Central GUI where the major component is decomposed into various modules and sub-components to support CPS Central GUI.

Figure 1: Central Architecture



Central Users And Roles

CPS Central depends on the API layer to provide a user role for an operation.

The following types of users/roles are supported:

- Admin: User with create, read, update, and delete (CRUD) access to CPS Central.

  When user is authorized and granted with admin privileges, user belongs to qns group and **ADMIN** text is displayed in the top right corner of the screen.

- Read Only: Restricted to read access only.

  When user is authorized and granted with read only privileges, user belongs to qns-ro group and **READONLY** is displayed in the top right corner of the screen.

Access CPS Central

To access CPS Central, use the following URLs:

- For High Availability (HA) Deployments: https://<*lbvip01*>:443/central

Note Run the `about.sh` command from the Cluster Manager to display the actual addresses as configured in your deployment.

The default login credentials are described in the following table:

Table 1: Supported User Roles and Credentials

User	Username	Password
Admin	qns-svn	cisco123

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.

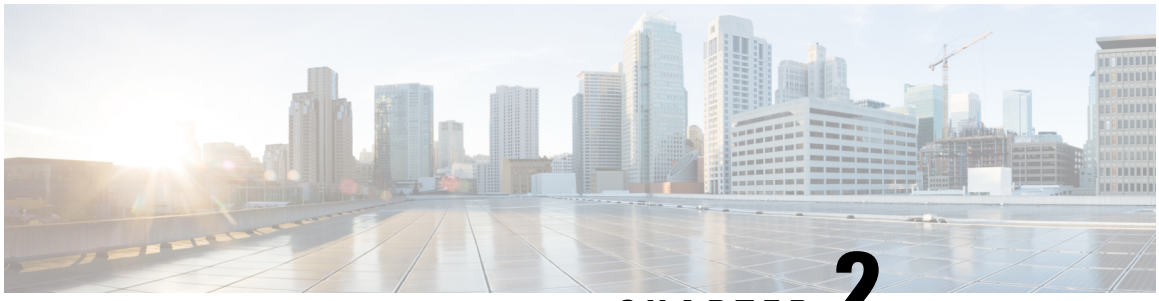
The hostname is displayed in the login panel only when the following argument is set to true:

```
-DshowSitenameLogin
```

Supported Browsers

CPS Central supports the most recent versions of the following browsers:

- Apple Safari
- Google Chrome
- Microsoft IE version 9 and above
- Mozilla Firefox



CHAPTER 2

Configuring CPS Central

Policy Builder Overview

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

Policy Builder interface supports both configuration of the overall CPS cluster of virtual machines (VMs) as well as the configuration of services and advanced policy rules.

Service Configuration

Service configuration objects are used to drive the system.

Services, Service Options and Use Case Templates enable you to configure these objects.

Services

A service is a code to label the service and a collection of Service Options which define the service.

Multiple services can be assigned to a single subscriber where the service options are combined between all the assigned services.

Create a New Service

Perform the following steps to create a new service:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Services**.

Step 4 Enter the values in each field as described in the following table:

Table 2: Service Parameters

Field	Description
Code	Value of the link between the Services assigned to a subscriber in Control Center and the Service in Policy Builder.
Name	Name displayed in Control Center.
Enabled	When enabled the service is not evaluated by the Policy Engine and is not displayed in Control Center. Default value is checked (true).
Suppress In Portal	When enabled this Service is not displayed in the Portal and is specific for SP Wi-Fi call flows. Default value is unchecked (false).
Balance Service	When enabled the Service runs through balance processing which results in one database read or write against the balance database. Performance improves (due to fewer database read or writes). For the services which do not rely on Balance or Quota, this value is unchecked. Default value is checked (true).
Add to Sub Accounts	When enabled this service is assigned to any subaccounts associated to the main subscriber. Default value is unchecked (false).
Service Options	
Name	Name of the Service Option
Use Case Template	Name of the Use Case Template
Add	Enables you to add another Service Option to a service.
Remove	Enables you to removes a Service Option from the Service.
Up or Down Arrow	Enables 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.

Step 5 Click **Save**.

Service Options

Service Options provides concrete values which can be reused for multiple services.

The configurable values in a Service Option are set up by the Use Case Template object. The Use Case Template can provide defaults to the Service Option or hide values in Service Configuration objects based on the necessity of certain use cases.

The following parameters can be configured under Service Option:

Table 3: Service Options Parameters

Parameter	Description
Name	Name of the service option which is referenced by the Service.
Use Case Template	Link to view the associated Use Case Template.
Service Configurations	List of the 'Service Configuration' objects that are to be set as part of the Service Option. 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: Adds a new Service Configuration that has been added to the Use Case Template. • Remove: Removes a new Service Configuration that has been added to the Use Case Template.
PreDefinedRule Parameters	
Add	Select to add 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	Select to remove 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	Display Name of the parameter. It can be updated by either the Service Option or the Use Case Template.
Value	Value of the parameter to be set.
Pull Value From...	Enables setting this value dynamically through AVP's, Custom Reference Data or the 'Policy State'.

Parameter	Description
Subscriber AVP Code	Enables 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	Enables pulling the value from the Custom Reference Data table's column specified.
Bind to Session/Policy State	Enables 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	Enables 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 are the building blocks of the Policy Builder service model architecture that include the following functionalities:

- Defines the Service Configuration objects to be set by a Service Option.
- Provides default values and/or hides values based on a use case.
- Enables service creation.

A copy of the Use Case Options is created while copying a Use Case Template.

The following parameters can be configured under Use Case Template:

Table 4: Use Case Template Parameters

Parameter	Description
Use Case Initiators	Group of conditions which indicate if the Service Configuration objects within a use case template are used. If no use case initiators are specified, the Service Configuration objects will always be added.

Parameter	Description
Service Initiators (OR Together)	Service Initiators are groups of conditions. If the service initiators on a Use Case Template is 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 is true, as indicated by the caption “OR Together”. The Plus/X keys enables the user add or remove a service initiator. The Up/Down arrow enables the user to move the initiators up and down. This affects the order in which the service initiators are evaluated.
Name	Name of the initiator.
Actions	
Service Configurations	
Name	Name of the Use Case Template which can be modified.
Add	Enables you to add a Use Case Template.
Remove	Enables you to remove a Use Case Template.
Service Configuration Parameters	Enables you add the Service Configuration objects needed to configure a use case.
Display Name	Display Name
Value	Value of the parameter to be set.
Bind Field	This is an internal field that should be modified only when requested by the BU and may be removed in future releases.
Allow Override	Indicates whether an option will be displayed for configuration in the Service Option by default.
Create Child: Use Case Option	Enables you to create a child use case option of a use case template.
Copy: Current Use Case Template	Enables you to create a copy the current Use Case Template.
Documentation	Enables you to write notes about the implementation for reference.

For more information regarding Service Configuration Objects, refer to *CPS Mobile Configuration Guide*.

Managing Reference Data

Reference Data provides access to configure various aspects of the system in order to make the system ready for operation and to provide settings and parameters that are referenced by policy rules across various services.

System Configuration

You need to define a system as it represents the customer deployment. The system represents a set of PCRF clusters that share the same session database.

Each system contains one or more clusters that represent a single high availability site environment. A cluster is used to define configurations related to the blades and shares the same set of policy directors. In Policy Builder, the Environment specific data section displays a list of system configurations that enables you to perform create, read, update, and delete (CRUD) operations and to create clusters which can further overwrite and customize system configurations.

Configure System

Perform the following steps to configure a system:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **System (beta version)** under **Reference Data**.

Step 4 Click **New System**.

Step 5 Enter the values in each field as described in the following table:

Table 5: System Parameters

Field	Description
Name	Name of the CPS system.
Description	Description of the entire system.
Session Expiration (hours)	If no messages are received in x hours, the session is removed. Default value is 8.
Session Expiration (minutes)	If no messages are received in x minutes, the session is removed. Default value is 0.
Timeout For Unknown Session	Time in minutes that CPS takes to keep a session alive after the subscriber logs off. The other network entities involved in the session close the session. Default value is 0.
Timeout For Soft Delete	Time in seconds in which a soft delete session is maintained for a CPS session after the session ends. Default value is 30.

Field	Description
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. Keep the Enable Multi Primary Key unchecked. Default is unchecked.

Step 6 Click **Save**.

Add Clusters

Perform the following steps to add clusters:

Step 1 To add clusters, click **Add Clusters**.

Step 2 Enter the values in each field as described in the following table:

Table 6: Cluster Parameters

Field	Description
Name	Name of the cluster.
Description	Description of the cluster.
DB Write Concern	Determines the write behavior of sessionMgr and for the error exceptions raised. Default option is OneInstanceSafe.
Failover SLA (ms)	Used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.
Replication Wait Time (ms)	Specifies a time limit, in milliseconds. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern.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 exceeds the replication wait time limit. The time is in milliseconds.
Trace Database Size (MB)	Determines the size in MegaBytes of the policy_trace database capped collection. Default value is 512.
Min Key Cache Time (minutes)	The minimum amount of time in minutes to keep a secondary key for a session. Default value is 2000.
Max Timer TPS	Default value is 2000.

Field	Description
Re-evaluation diffusion buckets	The number of batches or buckets into which CPS will divide 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 TPS field. Default is 50 buckets.
Re-evaluation diffusion interval (ms)	Defines the delay before processing the next bucket. Enter the sum of all the delays between all the buckets. Assuming 50 re-evaluation buckets are configured (by default), the default interval of 20000 milliseconds will introduce a delay of 408 milliseconds before proceeding with the next bucket of transactions. bucket_size-1 / interval = delay between buckets 50-1 / 20000 = 408 Default is 20000 milliseconds
Broadcast Message Wait Timer (ms)	The amount of time in milliseconds for the Policy Engine to wait between sending each Broadcast Policy Message. Default value is 50.
Max Sessions Per Shard	This is the maximum number of shard per session.
Look Aside Key Prefixes	Added to improve Gx/Rx lookup and caching performance.
Key Prefix	To improve Gx/Rx lookup and caching performance, you can add the lookaside key prefixes.For more information, see *Cisco Policy Suite Mobile Configuration Guide*.
Admin Database Configurations	
Shard Configuration	
Primary IP Address	The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server.
Secondary 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 pair's architecture. This field is present but deprecated to maintain downward compatibility.
Port	Port number of the database for Session data. Default value is 27717.
Backup DB Configuration	
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 sec.

Field	Description
Rate Limit	Used to control the TPS (with how much TPS reconciliation should take place once primary balance db is up).
End Point Configurations	
Shard Configuration	
Primary IP Address	The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server.
Secondary 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 pair's architecture. This field is present but deprecated to maintain downward compatibility.
Port	Port number of the database for Session data. Default value is 27717.
Backup DB Configuration	
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 sec.
Rate Limit	Used to control the TPS (with how much TPS reconciliation should take place once primary balance db is up).
Trace Database Configurations	
Shard Configuration	
Primary IP Address	The IP address of the sessionmgr node that holds trace information which allows for debugging of specific sessions and subscribers based on unique primary keys.
Secondary 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 pair's architecture. This field is present but deprecated to maintain downward compatibility.
Port	Port number of the database for Session data. Default value is 27717.
Backup DB Configuration	
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 sec.
Rate Limit	Used to control the TPS (with how much TPS reconciliation should take place once primary balance db is up).

Field	Description
Data Center Parameter	Deprecated
Enable	
Parameter Name	
Parameter Value	
Common Time Changes	Deprecated
Time	
Distribution Period (seconds)	

Step 3 Click **Save**.

Step 4 Click **Done**.

For field descriptions of system configuration templates, refer to *Plug-in Configuration* in *CPS Mobile Configuration Guide*.

Diameter Configuration

This section includes the following topics:

- Diameter Clients
- Diameter Defaults
- Rule Retry Profiles

Diameter Clients

Diameter Clients enables you to create different clients based on the interface. The clients defined can be used to configure a policy so that different clients get different service configuration objects.

You need to create specific client that corresponds to your interface and if there is no specific client for your interface select the generic Diameter Clients. You can also use the diameter client to filter the service objects that are going to be used in a policy.

The interface specific diameter clients are built on top of the generic Diameter Clients. They add specific behavior and should always be used in the context of the specific interface.

CPS supports the following Diameter Clients:

- Diameter Client: The generic diameter client object should be used for any interface that does not have a matching specific diameter client.
- Gx Client: The specific diameter client object should be used only in relation with the Gx interface. It adds Gx specific features to the generic diameter client.

- Rx Client: The specific diameter client object should be used only in relation with the Rx interface. It adds Rx specific features to the generic diameter client.
- Gxx Client: The specific diameter client object should be used only in relation with the Gxx interface. It adds Gxx specific features to the generic diameter client.
- Gy Client: The specific diameter client object should be used only in relation with the Gy interface. It adds Gy specific features to the generic diameter client.

Create Diameter Clients

Perform the following steps to create diameter clients:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Diameter Clients** under **Reference Data**.

A Diameter Clients editor page is displayed with the following options:

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

Step 4 To create diameter clients, select **Diameter Client**.

Step 5 Enter the values in each field as described in the following table:

Table 7: Diameter Client Parameters

Field	Description
Name	The client name 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. The first choice for Realm Pattern value should always be the exact peer realm name.
Extract Avps	
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.

Step 6 Click **Save**.

Create Gx Clients

Perform the following steps to create Gx clients:

Step 1 To create Gx clients, select **Gx Client**.

Step 2 Enter the values in each field as described in the following table:

Table 8: Gx Client Parameters

Field	Description
Name	The client name 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. The first choice for Realm Pattern value should always be the exact peer realm name.
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 used for Rx dedicated bearers. • Derive Flow-Direction (default): Flow-Direction AVP is derived based on Flow-Description AVP value and Flow-Status AVP value. This option is used in case the PCEF advertised support for Rel10 feature under Supported-Features AVP. • 3GPP Gx Rel11 Compliant: Flow-Direction AVP is derived as per 3GPP TS 29.212 v11 • Exclude Flow-Direction: Flow-Direction AVP is not set.
Emergency Called Station Ids	List of APNs that are allowed to initiate IMS emergency calls. For more information, see *CPS Mobile Configuration Guide*.

Field	Description
Sending Delayed Message Wait Time Ms	This parameter specifies the amount of time the Gx RAR will be delayed after Gx CCA is sent when "Gx Triggered Session-Release-Cause in RAR" is enabled. In case of multiple Media-Component-Descriptions being received in an AAR message by CPS, where one of them is rejected after evaluating for Gx 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 Gx RAR is sent to AF based on Sending Delayed Message Wait Time configured. Default value is 500 milliseconds.
Control Session Lifecycle	Decides if all the other sessions bound to the current Gx session get terminated upon Gx session termination. Default value is checked.
Remove Realm In User ID Mapping	When enabled removes the realm from the NAI (if present) before attempting to load the session by username. Default value is not checked.
Exclude Sponsor Identity AVP	When enabled 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 not checked.
Load By Imsi	When enabled 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 not checked.
Load By Nai	When enabled 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 not checked.
Load By Msisdn	When enabled 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 not checked.
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.

Field	Description
Load By Framed Ip	When enabled attempts to load the session by IP v4 address (Framed-IP-Address AVP value). Default value is not checked.
Load By Ip V6 Prefix	When enabled attempts to load the session by IP v6 address (Framed-IPv6-Prefix AVP value). Default value is not checked.
Session Chained	When enabled it does not attempt to terminate the Gx session by sending a Gx RAR to PCEF. Default value is not checked.
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	When enabled attempts to load the session by IMSI and APN. To effectively use this option Load By Imsi option needs to be enabled.
Re-install Rule on Monitoring Key Change	When enabled attempts to re-install a charging rule in case the only AVP value that changed for a PreConfiguredRule is the monitoring key value. Default value is not checked.
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	Enables CPS to validate missing AVP and send DIAMETER_MISSING_AVP (5005) result in the answer message. If this attribute is unchecked, then CPS will not perform the missing AVP validation. Default value is checked.

Field	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. When enabled 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. When disabled 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. Default value is unchecked.
Selective Muting	When enabled CPS selectively mutes the flow corresponding to a TDF-Application-Identifier on dedicated bearer after it receives the first Application_Start event trigger on the dedicated bearer. For default bearer, CPS selectively mutes the flow corresponding to a TDF-Application-Identifier after it receives the Application_Start event trigger on default bearer and maximum limit is reached on dedicated bearer. **Note** Limit on dedicated bearer is based on a combination of QCI and ARP limit. This value is configurable in Policy Builder. After CPS receives Application_Stop event trigger for a specific TDF-Application-Identifier (with TDF-App-Instance-ID=0), CPS removes that rule from dedicated bearer and installs the rule on the default bearer and unmutes all the rules related to that TDF-Application-Identifier on default bearer.
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.

Field	Description
Gx triggered Session-Release-Cause in RAR	When 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. When 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.
Cisco Pending Transaction Retry	Select to enable Cisco Pending Transaction Retry.
Sponsored Profile	Allows for customization of the monitoring key name. This option is used only in case the PCEF advertises support for SponsoredConnectivity feature under Supported-Features AVP.
Rx Based QoS Upgrade Of Default Bearer	Select to enable Rx based QoS upgrade
Count of Flow Descriptions in one Charging	Select to enable Count of Flow Descriptions in one Charging Rule.
Max number of Flow Descriptions on a bearer	Defines the maximum number of flows that can be installed on a default bearer per QCI. 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 does not install any rules for those flows. Default value is 64.
Charging Rule Retry	Select to enable Charging Rule Retry Configuration.
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.
Pending Transaction Retry	
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.

Field	Description
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	
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.
Custom Dynamic Rule Name	
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).
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.

For more information, see *CPS Mobile Configuration Guide*.

Step 3 Click **Save**.

Create Rx Clients

Perform the following steps to create Rx clients:

Step 1 To create Rx clients, select **Rx Client**.

Step 2 Enter the values in each field as described in the following table:

Table 9: Rx Client Parameters

Field	Description
Name	The client name 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. The first choice for Realm Pattern value should always be the exact peer realm name.
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.
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	Defines the timer by which the STA will be held back. Once the timer expires even if the CCR-U is not received, STA will be sent to the AF and the rxSession will be removed. Default value is 4000 milliseconds.
CCR-U Wait Time (in seconds)	After expiry of the CCR-U Wait Time (in seconds), CPS sends the Rx RAR message.
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.
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. Default value is unchecked.

Field	Description
Validate Flow-Description AVP Value	When checked, 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 the check box is unchecked, CPS does not validate the Flow-Description AVP value and forwards it to PCEF as part of generated rules. Default value is unchecked.
29.213 standard QoS for preliminary service	When selected, CPS supports the QoS handling for Preliminary Service Status. So, on receiving Service-Info-Status AVP as preliminary service information from AF, CPS will generate 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. Default value is unchecked.
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 starts two Rx charging rules, 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 will increment 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 existing Rx session. Default value 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. Default value is unchecked (false).

Field	Description
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. Default value is unchecked.
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 an Rx AAA response message 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 Rx AAA message, 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 will not report this information until it is received in a CCR message from PCEF.
Precedence Avp Lower And Upper	
Precedence Start Value	The precedence value for the first Rx charging rule that is installed as part of an Rx session. The number will continue to increment for each Rx charging rule installed until it reaches the value set in the **Precedence End Value** field. When the value is reached, the rxPrecedenceCounter is reset to the **Precedence Start Value**, and continues incrementing. 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**, and it must be greater than the **Precedence Start Value**.
Netloc Access Not Supported Configuration	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.
Extract Avps	

Field	Description
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.

Step 3 Click **Save**.

Create Gxx Clients

Perform the following steps to create Gxx clients:

Step 1 To create Gxx clients, select **Gxx Client**.

Step 2 Enter the values in each field as described in the following table:

Table 10: Gxx Client Parameters

Field	Description
Name	The client name 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. The first choice for Realm Pattern value should always be the exact peer realm name.
Load By Imsi	When enabled 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 not checked.
Load By Nai	When enabled attempts to load the session by NAI (Subscription-Id-Data AVP value under Subscription-Idgrouped AVP where Subscription-Id-Type AVP valueis END_USER_NAI (3)). Default value is not checked.

Field	Description
Load By Msisdn	When enabled 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 not checked.
Load By Framed Ip	When enabled attempts to load the session by IP v4 address(Framed-IP-Address AVP value). Default value is not checked.
Load By Ip V6 Prefix	When enabled attempts to load the session by IP v6 address (Framed-IPv6-Prefix AVP value). Default value is not checked.
Extract Avps	
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.

Step 3 Click **Save**.

Create Gy Clients

Perform the following steps to create Gy clients:

Step 1 To create Gy clients, select **Gy Client**.

Step 2 Enter the values in each field as described in the following table:

Table 11: Gy Client Parameters

Field	Description
Name	The client name 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. The first choice for Realm Pattern value should always be the exact peer realm name.
Load Options	

Field	Description
Load By Realm And User Id	Loads the session by realm (Origin-Realm AVP value) and User Id. Default value is not checked.
Load By APN And User Id	Loads the session by APN (Called-Station-Id AVP value) and User Id. Default value is not checked.
Extract Avps	
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.

Step 3 Click **Save**.

Create Sy Clients

Perform the following steps to create Sy clients:

Step 1 To create Sy clients, select **Sy Client**.

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.

For more information, see *CPS Mobile Configuration Guide*.

Diameter Defaults

Diameter Defaults provides global default values for different modules of the system. There should be one object for each diameter default type.

CPS supports the following Diameter Defaults:

- Gx Profile: Provides default values to be used for Gx default bearer QoS parameters as well as some specific behavior related to default bearer QoS.
- Custom AVP Profile: 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 used. It consists of the following components:
  - Custom Avp Table: Defines the custom AVP with all the standard attributes of an AVP.

- Avp Mappings: Maps the source and the destination for the custom AVP.

- MPS Profile: Provides MPS attributes required for priority service provisioning. The priority level value from service configuration takes precedence over MPS Profile value.
- Rx Profile: Provides default values and specific values to be used by the different QoS parameter mapping functions at PCRF as per 3GPP TS 29.213. Also provides a mechanism to authorize the Rx IMS sessions.
- Sd Push Rules: 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.
- Time of Day Schedule: Allows 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.

For more information, see *CPS Mobile Configuration Guide*.

Add Custom Avp Profiles

Perform the following steps to add Custom AVP Profiles:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Diameter Defaults** under **Reference Data**.

A Diameter Defaults editor page is displayed with the following options:

- Custom AVP Profiles
- Gx Profiles
- MPS Profiles
- Rx Profiles
- Sd Push Rules
- Tod Schedule

Step 4 To add custom AVP profiles, select **Custom Avp Profile**.

Step 5 Enter the values in each field as described in the following tables:

Table 12: Custom AVP Table

Field	Description
AVP Name	Any string that will be used to identify this custom AVP.

Field	Description
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. • 256-above: Used for Diameter, and are allocated by IANA. **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.
Vendor Id	Indicates if the Vendor Id field is there in the AVP or not.
Vendor Code	Vendor Id value as assigned by IANA. The Vendor Id bit known as the Vendor-Specific bit, indicates if 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 if the support of the AVP is required. If this Bit is enabled, 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 enabled, it 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.
Data Type	Any valid basic AVP data format: • Float32Avp • Float64Avp • Integer32Avp • Integer64Avp • OctetStringAvp • Unsigned32Avp • Unsigned64Avp • UTF8String

Avp Mappings

The custom AVP mapping includes the following mappings:

Table 13: Custom AVP to Custom AVP Mapping

Field	Description
Source Avp	Name of AVP for possible mapping.
Source Avp 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.

Field	Description
Source Cmd Type	The message indicated by Source Command Code that is a request or response.
Origin Host	Identification of the source point of the operation.
Origin Realm	Identification of the realm of the operation originator.
Target Avp	AVP Name mapped to Source AVP.
Target App Id	Target Application Identifier
Target Cmd Code	The command code of the message that goes on Target APP ID and has Target AVP.
Target Cmd Type	The message having Target Command Code request or a response.
Destination Host	Identification of the destination point of the operation.
Destination Realm	Realm of the operation destination

Table 14: 3GPP/SPR AVP to 3GPP AVP Mapping

Field	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.
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 APP ID that contains the Source AVP.
Source Cmd Type	The message indicated by Source Command Code is a request or response with the following types: • None • Request • Response
Origin Host	Identification of the source point of the operation.
Origin Realm	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).
Target Cmd Code	The command code of the message that goes on Target APP ID and have Target AVP.
Target Cmd Type	The message having Target Command Code request or a response with the following types: • Request • Response

Field	Description
Destination Host	Identification of the destination point of the operation.
Destination Realm	Realm of the operation destination.

Table 15: 3GPP/SPR AVP to Custom AVP Mapping

Field	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 APP ID that contains the Source AVP.
Source Cmd Type	The message indicated by Source Command Code is a request or response with the following types: • None • Request • Response
Origin Host	Identification of the source point of the operation.
Origin Realm	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).
Target Cmd Code	The command code of the message that goes on Target APP ID and have Target AVP.
Target Cmd Type	The message having Target Command Code request or a response with the following types: • Request • Response
Destination Host	Identification of the destination point of the operation.
Destination Realm	Realm of the operation destination.

Step 6 Click **Save**.

Add Gx Profiles

Perform the following steps to add Gx profiles:

Step 1 To add Gx profiles, select **Gx Profile**.

Step 2 Enter the values in each field as described in the following table:

Table 16: Gx Profile Parameters

Field	Description
Push Pre-Configured Rule Option	Determines if 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 as described below: **a.** A policy derived AVP having the same value as the Logical Apn. **b.** Called-Station-Id AVP from incoming Rx AAR. **c.** 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	Determines if the requested QoS should be granted or not as the default bearer QoS. Default value is not checked.
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 not checked.
Global Default Granted QoS	Select to enable Exclusion List

Field	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 U L	Defines the maximum bit rate allowed for the uplink direction.
Max Req Bandwidth D L	Defines the maximum bit rate allowed for the downlink direction.
Guaranteed Bit Rate U L	Defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bit Rate D L	Defines the guaranteed bit rate allowed for the downlink direction.
Apn Agg Max Bit Rate U L	Defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN.
Apn Agg Max Bit Rate D L	Defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN.
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.
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.
Realm Pattern	The pattern that peer realm name should match in order for this diameter client to be used.
Host Pattern	Host name pattern as received in Origin-Host AVP in AAR message. The pattern needs to follow standard Java pattern conventions.
QOS retry on APN-AMBR_FAILURE_MOFIDICATION	Select to receive APN-AMBR_FAILURE_MODIFICATION events from PCEF.
Number Of Retry	Number of retries to push calculated QoS information.

Field	Description
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.

Step 3 Click **Save**.

Add Mps Profiles

Perform the following steps to add Mps profiles:

Step 1 To add Mps profiles, select **Mps Profile**.

Step 2 Enter the values in each field as described in the following table:

Table 17: Mps Profile Parameters

Field	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.
Priority Level	Priority level is used to decide if a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (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.

Field	Description
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

Step 3 Click **Save**.

Add Rx Profiles

Perform the following steps to add Rx profiles:

Step 1 To add Rx profiles, select **Rx Profile**.

Step 2 Enter the values in each field as described in the following table:

Table 18: Rx Profile Parameters

Field	Description
Prefer answer Codec-Data	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.
Default QoS Policy	
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 Requested Bandwidth U L	Defines the maximum bit rate allowed for the uplink direction.

Field	Description
Max Requested Bandwidth D L	Defines the maximum bit rate allowed for the downlink direction.
Guaranteed Bit Rate U L	Defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bit Rate D L	Defines the guaranteed bit rate allowed for the downlink direction.
MPS QoS Policy	
M P S Id	The MPS Id contains the national variant for MPS service name indicating an MPS session.
Priority Level	Priority level is used to decide if a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (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.

Field	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
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.
Application QoS Policy	
Priority Level	Priority level is used to decide if a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (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.

Field	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.
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 Requested Bandwidth U L	Defines the maximum bit rate allowed for the uplink direction.
Max Requested Bandwidth D L	Defines the maximum bit rate allowed for the downlink direction.
Guaranteed Bitrate U L	Defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bitrate D L	Defines the guaranteed bit rate allowed for the downlink direction.
AF Application Identifier	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.
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.
Codec QoS Policy	
Codec Data Pattern	Contains codec related information known at the AF.
Codec Details Pattern	Contains codec related information.

Field	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 Requested Bandwidth U L	Defines the maximum bit rate allowed for the uplink direction.
Max Requested Bandwidth D L	Defines the maximum bit rate allowed for the downlink direction.
Guaranteed Bitrate U L	Defines the guaranteed bit rate allowed for the uplink direction.
Guaranteed Bitrate D L	Defines the guaranteed bit rate allowed for the downlink direction.
Reservation 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.
Priority Level	Priority level is used to decide if a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (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.

Field	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
AF Application Id Validation	
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.
Apn	Access point name is the name of the gateway between the mobile network and another network.
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.

Step 3 Click **Save**.

Add Sd Push Rules

Perform the following steps to add Sd Push Rules:

Step 1 To add Sd Push Rules, select **Sd Push Rules**.

Step 2 Enter the values in each field as described in the following table:

Table 19: Sd Push Rules Parameters

Field	Description
Input parameters	
Gx Realm	Origin-Realm
Gx host Pattern	Origin-Host
Output parameters	

Field	Description
TDF Realm	Destination-Realm
TDF Host	Destination-Host

Step 3 Click **Save**.

Add Tod Schedules

Perform the following steps to add Tod Schedules:

Step 1 To add Tod schedules, select **Tod Schedule**.

Step 2 Enter the values in each field as described in the following table:

Table 20: Tod Schedule Parameters

Field	Description
Code	Name of the Schedule.
Scheduled Switch Times	
Name	Name of the scheduled switch time.
Start Time	Start time of the scheduled switch time.
End Time	End time of the scheduled switch time.

Step 3 Click **Save**.

Rule Retry Profiles

The Rule Retry Profiles enables you to activate a retry timer with a number of retries for Traffic Detection functions that are INACTIVE. The number of retries and the timer interval between each retry can be configured.

Create Rule Retry Profile

Perform the following steps to create a rule retry profile:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Rule Retry Profiles** under **Reference Data**.

Step 4 To create a new rule retry profile, click **Rule Retry Profile**.

Step 5 Enter the values in each field as described in the following table:

Table 21: Rule Retry Profile Parameters

Field	Description
Retry Interval	Delay between retry attempts. The default interval is 10 seconds or is capped at 15 seconds (configurable). If value is less than 15 seconds, then the retries will be scheduled at second level granularity. If value is greater than 15 secs, then granularity is 1 minute.
Max Retry Attempts	The maximum times retry is attempted for a rule. Default value is 3 attempts.
BackoffAlgorithm	Determines the actual delay between retry attempts. You can use the following option: Constant Interval: Uses the configured retry interval for delay of all retry attempts.
Name	Name of the Rule Retry Profile.
Max Retry Interval (seconds)	Enter the maximum time in seconds between the first and the last retry. If set to zero, the PCRF will not enforce a time limit for sending the retry messages. Default is 0.
Rule Failure Code	Select the failure codes for which CPS will retry. If no Rule Failure Code is specified CPS will retry regardless of the failure code reported.

Step 6 Click **Save**.

Managing Quotas

This section includes the following topics:

- Account Balance Templates
- Tariff Times

Account Balance Templates

An account balance is a group of quotas. You can create a balance (quota grouping) called Data and have several quotas defined such as Monthly, Top-up, and Bonus. When the subscriber uses a particular account,

the usage is charged based on their Data balance and the MsBM determines which underlying quota should be debited based on rules set up in QNS.

The Quota templates defines the specifications of the quota. You can view existing account balance templates or create account balance templates with the available quota templates.

Create Account Balance Templates

Perform the following steps to create an account balance template:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Account Balance Templates** under **Reference Data**.

Step 4 To create account balance templates, click **Account Balance Template**.

Step 5 Enter the values in each field as described in the following table:

Table 22: Account Balance Template Parameters

Field	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 service provider 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.

Field	Description
Error On Provision With Non Zero Balance	If a provisioning request is made when there is remaining balance, 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. For example, 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. 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.

Step 6 Click **Save**.

Create One Time Quota Templates

Perform the following steps to create a one time quota template:

Step 1 To create a one time quota template, click **One Time Quota Template**.

Step 2 Enter the values in each field as described in the following table:

Table 23: One Time Quota Template Parameters

Field	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.

Field	Description
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 such that 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. The highest rank is 1 and 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 30.
Stackable	When selected the One Time quota becomes stackable. 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. 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. 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.

Step 3 Click **Save**.

Create Recurring Quota Templates

Perform the following steps to create a recurring quota template:

Step 1 To create a recurring quota template, click **Recurring Quota Template**.

Step 2 Enter the values in each field as described in the following table:

Table 24: Recurring Quota Template Parameters

Field	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 such that 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. The highest rank is 1 and 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.
Recurrence Frequency	Value used in conjunction with the Recurrence Frequency Amount to determine the refresh period. Default value is Months.
Rollover Quota	A Rollover Quota Template that the recurring quota will rollover 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. **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 will refresh 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 will refresh 6 times. If the quota is provisioned on January 1st, it will expire on June 30th. Default value is 0.

Field	Description
Auto Rollover (If checked, recurrence frequency must be >= 1 day)	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. Default value is False (unchecked).
Use Rollover Expiration Time for Change Priority	When selected, the Balance module will use 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).
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. For example, 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. 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.

Step 3 Click **Save**.

Create Rollover Quota Templates

Perform the following steps to create a rollover quota template:

Step 1 To create a rollover quota template, click **Rollover Quota Template**.

Step 2 Enter the values in each field as described in the following table:

Table 25: Rollover Quota Template Parameters

Field	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.

Field	Description
Priority	Priority ranks the template such that 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. The highest rank is 1 and 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. For example, 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. 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.

Step 3 Click **Save**.

Tariff Times

Tariff Times is the CPS nomenclature for defining rates. Rates provide a mechanism to alter a quota that is billed.

You can view existing tariff times and create a new Tariff Time.

Create Tariff Times

Perform the following steps to create a new tariff time:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Tariff Times** under **Reference Data**.

Step 4 To create a new tariff time, click **Tariff Time**.

Step 5 Enter the values in each field as described in the following table:

Table 26: Tariff Time Parameters

Field	Description
Code	Name of the code.
Timezone	Select timezone based on the place of business. For example, America/New_York
Tariff Switch Times	Enables you to change usage rates for a subscriber.
Name	Readable name.
Start Time (hh:mm)	Enables you to set start time
End Time (hh:mm)	Enables you to set end time.
Tariff Time Identifier	Enables you to determine rates.
Associated Valid Dates Valid Days of the Week	Enables you to associate days of the week to various tariff times, according to your business rules.
Additional Valid Dates (Holidays)	Enables you to add additional dates such as holidays.

Note
- Tariff Times are not allowed to cross over midnight which means you have to create two tariff switch times to cover a single logical period. For example 10 p.m. to midnight and midnight to 5 a.m defines your night time tariff time.
- A Start Time of midnight assumes it is midnight today.
- An End Time of midnight assumes it is midnight tomorrow (Start Time and End Time of 00:00 and 00:00 covers the whole day).

Step 6 Click **Save**.

Custom Reference Data Configuration

This section includes the following topics:

- Search Table Groups
- Custom Reference Data Triggers
- Custom Reference Data Tables

Search Table Groups

Search Table Groups enables logical grouping of multiple customer reference data tables.

The following parameters can be configured under Search Table Group:

Table 27: Search Table Group Parameters

Parameter	Description
Name	Name of the Search Table Group.
Evaluation Order	Order in which groups are evaluated. Evaluation order value is in ascending order starting with 0. **Note** Search table groups and their respective CRD tables are listed based on the evaluation order value. If the evaluation order value is the same for two or more tables, then they are listed alphabetically.
Result 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	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	More human readable name of the AVP.
Use In Conditions	Represents the availability of the row for conditions in Policies or Use Case Templates. There is a performance cost to having these checked, so it is recommended to uncheck unless they are required.
Default Value	The default value if no results are found from a Customer Reference Data Table.
Table Search Initiators (OR Together)	This section controls whether or not the Search Table Group and all tables below will be executed.
Name	Name of the table search initiators.

Custom Reference Data Triggers

Custom Reference Data Trigger is a group of conditions used to evaluate a table. This can be used to derive the same data in different ways depending on the conditions.

The following parameters can be configured under Custom Reference Data Triggers:

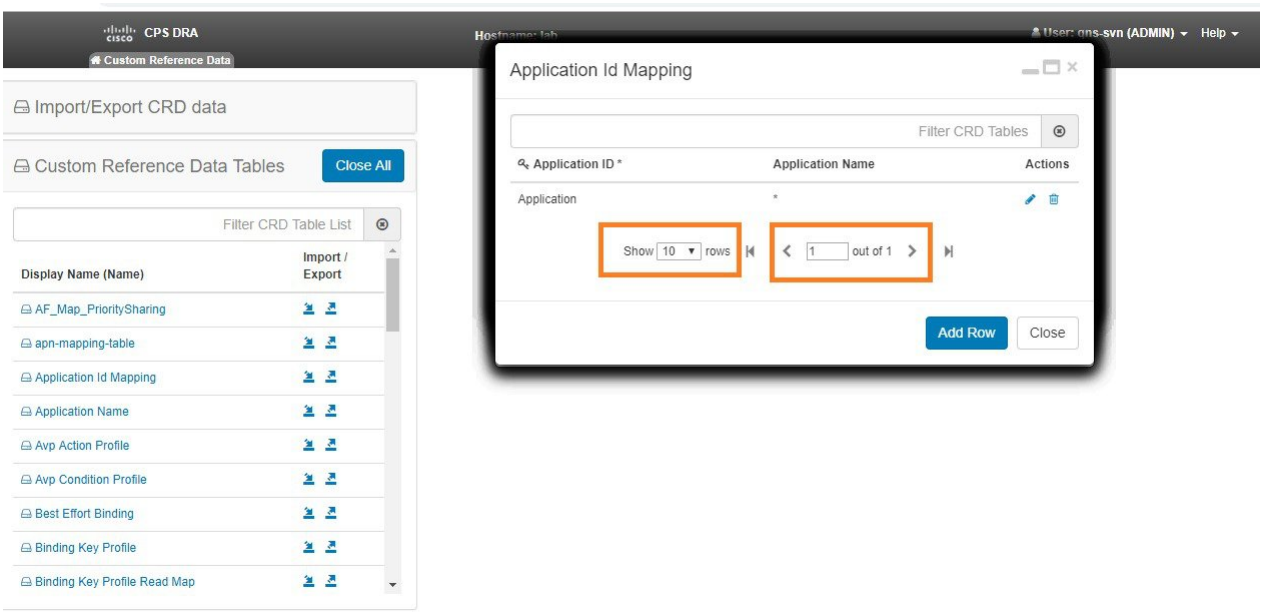
Table 28: Custom Reference Data Trigger Parameters

Parameter	Description
Name	Name of the table that will be stored in the database.
Custom Reference Data Initiators (OR Together)	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.

Custom Reference Data Tables

Custom Reference Data tables define custom derived data for installation and to make decisions based on that data.

CRD also supports the pagination component in which the data is displayed according to the number of rows configured per page. You can change the number of rows to be displayed per page. Once you set the value for rows per page, the same value is used across the Central unless you change it. Also, you can navigate to other pages using the arrows.



The following parameters can be configured under Custom Reference Data Tables:

Table 29: Custom Reference Data Table Parameters

Field	Description
Name	Name of the table that will be stored in the database. It should start with alphanumeric characters, should be lowercase or uppercase but not mixed case, and should not start with numbers, no special characters are allowed, use "_" to separate words. For example, logical_apn = GOOD, logicalAPN = BAD, no_spaces.

Field	Description
Display Name	Name of the table that will be displayed in Control Center.
Cache Results	Indicates if the tables should be cached in memory and should be checked for production.
Activation Condition	Custom Reference Data Trigger that needs to be true before evaluating this table. It can be used to create multiple tables with the same data depending on conditions or to improve performance if tables do not need to be evaluated based on initial conditions.
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	When enabled, 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 (*)
Evaluation Order	Indicates the order the tables within the search table group should be evaluated. Starting with 0 and increasing.
Columns	
Name	Name of the column in the database.
Display Name	More readable display name.
Use In Conditions	Represents the availability of the row for conditions in Policies or Use Case Templates. There is a performance cost to having these enabled, so it is recommended to disable unless they are required.
Type	Determines the values in the control centre as described below: • Text: Value can be any character. For example, example123!. • Number: Value should be a whole number. For example, 1234. • Decimal: Value can be any number. For example, 1.234. • True/False: Value can be true or false. For example, true. • Date: Value should be a date without time component. For example, May 17th 2020. • DateTime: Value should be a date and time. For example, May 17th, 2020 5:00pm.

Field	Description
Key	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 also are allowed to set the Runtime Binding fields to populate this data from the current message/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	Indicates whether this field will be marked required in Control Center. A key is always required.
Column Details	
Valid Values	
All	All the values of the type selected by the user.
List of Valid	A list of name/display name pairs that will be used to create the list. Valid values can also contain a name which will be the actual value of the column and a display value which allows the Control Center to display use name.
Name	The name of the column in the database.
Display Name	Readable display name.
Validation	
Regular Expression	The Java regular expression that will be run on the proposed new cell value to validate it.
Regular Expression Description	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 should match (equals, less than, etc).
None	
Bind to Subscriber AVP	This pulls the value from an AVP on the subscriber. It will also pull values from a session AVP or a Policy Derived AVP.
Bind to Session/Policy State	This pulls the value from a Policy State Data Retriever which knows how to retrieve a single value for a session.
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 on giant table with a lot of duplicated values.
Bind to Diameter request AVP code	This allows the key be filled out from an AVP on the diameter request.

Field	Description
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

For more information, see *CPS Mobile Configuration Guide*.

Subscriber Database Integration

This section includes the following topic:

- LDAP Server Sets

LDAP Server Sets

The LDAP Server Set represents a connection to a logical set of LDAP servers that is reusable across Domain definitions.

You can create a new LDAP Server Set.

Create LDAP Server Sets

Perform the following steps to create a new LDAP Server Set:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **LDAP Server Sets** under **Reference Data**.

Step 4 To create a new LDAP Server Set, click **Ldap Server Set**.

Step 5 Enter the values in each field as described in the following table:

Table 30: 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.

Parameter	Description
Use Asynchronous Operations	This should be is checked (true). Setting to unchecked (false) can result in unpredictable performance and is not supported.

Step 6 Click **Save**.

Other Services

This section includes the following topics:

- Notifications
- Domains

Notifications

Notification enables sending messages to subscribers. Service Providers can use messages to alert the subscriber on issues and offers on their network.

The CPS for Mobile supports the following notification types:

- Apple Push Notifications: To configure CPS to send a message to a subscriber with an Apple iPhone or other iOS device.
- Email Notifications: To configure CPS to send an email notification to a subscriber.
- SMS Notifications: To configure CPS to send a text notification to a subscriber.
- Real Time Notifications: Realtime Notifications allows you to send SOAP/XML messages to a defined server when policy thresholds are breached.
- GCM: Google Cloud Messaging enables you to send messages to a subscriber on an android device.

Add Apple Push Notification

Perform the following steps to add an apple push notification:

Step 1 Log in to the **CPS Central**.
Step 2 Click **Policy Builder**.
Step 3 Select **Notifications** under **Reference Data**.
Step 4 To create an apple push notification, click **Apple Push Notification**.
Step 5 Enter the values in each field as described in the following table:

Table 31: Apple Push Notification Parameters

Field	Description
Name	Name of the notification message.

Field	Description
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. For 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 does not 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 example: sound1, alert7, buzzSound_A
Send Once Per Session	Select this check box to send the notification once per session.
Custom Fields	You can add custom fields with values that can be sent to the application.
Field Name/Field Value	String For example: • “high_score”: “1000” • “custom_field_1”: “display1” • “custom_field_2”: “false”
Alert (limit 163 characters)	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 them into production. If you want to use a string and substitute session information, use the syntax $Name to insert the receiver’s name in the email. Alerts are limited to 160 characters. Alerts longer than that are truncated.

Step 6 Click **Save**.

Add Email Notification

Perform the following steps to add an email notification:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Notifications** under **Reference Data**.

Step 4 To create an email notification, click **Email Notification**.

Step 5 Enter the values in each field as described in the following table:

Table 32: Email Notification Parameters

Field	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.
Send Once Per Session	When enabled realtime notifications are generated for each session and not for all messages within that session. Default is checked (true).
Subject	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.

Step 6 Click **Save**.

Add SMS Notification

Perform the following steps to add an SMS notification:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Notifications** under **Reference Data**.

Step 4 To create an SMS notification, click **SMS Notification**.

Step 5 Enter the values in each field as described in the following table:

Table 33: SMS Notification Parameters

Field	Description
Name	Name of the notification message. This name is used later in the policy definition to send the SMS.

Field	Description
Source Address	Source address of the SMS message.
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.
Addresses 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. Default value is INTERNATIONAL.
Addresses NPI	Numbering Plan Indicator. It defines the format of the addresses. Values: DATA, ERMES, INTERNET, ISDN, LAND_MOBILE, NATIONAL, PRIVATE, TELEX, UNKNOWN, WAP. Default value is UNKNOWN.
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(7 bit).
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. Because if space in the message submitted from CPS does not allow for header information, such as the User Data Header (UDH), then many SMSC do not accept the messages.
Send Once Per Session	When enabled realtime notifications are generated for each session and not for all messages within that session. Default is checked (true).
Compressed (DCS)	Select this check box to set whether compression is used per the SMPP specification. Default is false.
Contain Message Class (DCS)	Select this check box to set whether the contain message class options is used per the SMPP specification. Default is false.
Use Plugin Config Data Coding Instead (DCS Advanced)	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.

Field	Description
Use Message Encoding with Plugin Config Data Coding (DCS Advanced)	Select this check box when the "Use Plugin Config Data Coding Instead" check box above is enabled. 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.
WAP Push Configuration (WAP Push via SMS)	Select to enable WAP Push
Message (or custom data of WAP Push via SMS)	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.

For more information of WAP Push configuration, refer to *CPS Mobile Configuration Guide*.

Step 6 Click **Save**.

Add Real Time Notification

Perform the following steps to add a real time notification:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Notifications** under **Reference Data**.

Step 4 To create an real time notification, click **Real Time Notification**.

Step 5 Enter the values in each field as described in the following table:

Table 34: Real Time Notification Parameters

Field	Description
Name	Name of the realtime notification message.
No of Retries	When CPS sends realtime notification to the provided HTTP URL and if it is not reachable then this field specifies how many times CPS should send the notification. Same is true for HTTP Fallback URL. Default is 3.

Field	Description
Retry Interval (secs)	Interval during two retries. Default is 2.
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. Default value is text/xml.
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.

Field	Description
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.

For more information, see *CPS Mobile Configuration Guide*.

Step 6 Click **Save**.

Add GCM Notification

Perform the following steps to add a GCM notification:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Notifications** under **Reference Data**.

Step 4 To create a GCM notification, click **GCM Notification**.

Step 5 Enter the values in each field as described in the following table:

Table 35: GCM Notification Parameters

Field	Description
Name	Name of the GCM notification message.
Collapse Key	String - This parameters identifies a group of messages (for example, with collapse_key: “Updates Available”) that can be collapsed, so that only the last message gets sent when delivery can be resumed. This is intended to avoid sending too many of the same messages when the device comes back online or becomes active.
Time To Live (Days)	Integer - Overrides setting in the GCM Notifications Plug-in Configuration for this message. Default is checked (true).

Field	Description
Send Once Per Session	When enabled realtime notifications are generated for each session and not for all messages within that session.
Delay While Idle	When enabled it overrides setting in GCM Notifications Plug-in Configuration for this message.
Message (Text/Plain or JSON)	JSON or Plain text can be used for the templates. JSON must be a complete JSON document, not a partial document. For example: {"json":{"id":"$id","some":"thing","someother":"$thing"}, "additional":"$replacement"} is valid but "id":"$id","some":"thing","someother":"$thing", "additional":"$replacement" is not valid because it is not a complete document.

Step 6 Click **Save**.

Domains

You can create domains to authorize a user, view existing domains and to perform CRUD on Domain.

Domain controls the authorization of a user. If a user is authorized, the domain can auto-provision a user in USuM (including a default Service). If a user is not auto-provisioned, the user is provisioned by an API into USuM before being assigned to a service on the network.

After logging in, you can go through a single domain authorization process. Your domain is determined by location and if it does not match any of the domains you will be marked as default.

Create Authorized Domains

Perform the following steps to create an authorized domain:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select **Domains** under **Reference Data**.

Step 4 To authorize a domain, click **Domains**.

Step 5 Enter the values in each field as described in the following table:

Table 36: Domain Parameters

Field	Description
Name	Name of the domain that describes the APN mapped to the domain node. For example, VOLTE would imply that the domain contains all VOLTE sessions. The name should be short and descriptive to find the associated business rules. **Restriction** After a domain is defined changing the name of an APN will invalidate 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	Indicates that the domain is the default domain if the incoming message does not map to any of the other domains. **Restriction** 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).
General	
Authorization	Valid options that can be used in mobile configuration. For more information, see *CPS Mobile Configuration Guide*.
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	
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.
Domain Naming	
Domain Prefix	Optional
Append Location	When enabled the user location will be appended with credential ID and will happen while authenticating the user on the network.
Provisioning	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 more information about provisioning tab options, refer to *CPS Mobile Configuration Guide*.
Additional Profile Data	Enables retrieving subscriber profile from Home Subscriber Server (HSS) and LDAP/Ud Server.
Profile Mappings	

Field	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.

Field	Description
Sh Realm	Enter the HSS Diameter realm name.
Subscribe to Notifications	When enabled CPS subscribes to HSS notifications by sending SNR and when disabled CPS will send UDR. By default, this option is enabled.
Enable External Profile Cache Lookup	When enabled allows 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. 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.
Broadcast Profile Change	Select 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
User Identity Avp Formatting	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.
Sip Parsing Rules	In the **Sip Parsing Rules** table, click **Add** to define a parsing rule.
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.
Service Indications	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.
Sh Parsing Rules	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.
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

Field	Description

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']
Retry Interval	Select this check box to open the **Retry Profile** parameters.
Retry Interval	The number of minutes between retry attempts.
Max Retry Attempts	The maximum number of retries that will occur after a failed attempt. The default value is 3 attempts.
Backoff Algorithm	The back-off algorithm is used while determining the actual delay between retry attempts. You can select from two 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. The default setting is **Constant Interval**.

Field	Description
Granularity in Seconds (Default is minutes)	When selected, the granularity of the retry interval is in seconds. By default, the check box is unchecked, that is, retry granularity is in minutes. **Note** • To achieve seconds level granularity, the retry interval should be up to 60 seconds. • 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 at a time 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. 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.
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.
Result Code Based Retries	• Result Code: The result codes for which Sh SNR/UDR needs to be retried by QNS. If this list is empty, the Sh SNR/UDR 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.
Locations	
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.
Name	Enter a name that is equal to the logical APN.

Field	Description
Mapping Values	Enter mapping value equal to the CRD column code (for example, logical_apn) with a "\" and then the logical APN value.
Timezone	Timezone attribute is not used in mobility configurations and should be left blank.
Advanced Rules	
Transparent Auto-Login (TAL) Type	Enables subscribers to maintain an always-on connection without the need to authenticate on each connect.
Tal with no domain	When enabled the operator allows user to auto login without including the Domain in credential.
EAP Correlation Attribute	EAP Correlation attribute will look up into the EAP reference table. **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.
Imsi to Mac Format	When enabled the user IMSI is converted to MAC format before the user can log on to the network.
Unknown Service	Unknown service assigned to subscriber when it is not found in SPR.
Autodelete Expired Users	When enabled the expired users are deleted from SPR.
Default Service	Used when service is not found for subscriber in SPR.
Anonymous Subscriber Service	Used for Anonymous Authorization method of authentication. The service configured in this will be assigned to anonymous subscriber.
Authentication Dampening	Subscribers or unknown subscribers who tried number of failed attempts for authorization can be blocked for configurable time period with Authentication Dampening. When enabled the following fields are enabled: • Retry Period In Minutes • Retry Attempts • Lock Out Period In Minutes

Step 6 Click **Save**.

Advanced Services

The Advanced tab includes the following options:

- Policies

- Blueprints
- Class Categories
- Phrase Book

Important The Advanced tab options should be used only under Cisco guidance. For further assistance 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.

CPS Service Configuration

The Import/Export option enables you to perform the following operations:

- Export CPS Service Configuration into a single file
- Import CPS Service Configuration to another environment.

For more information, see *Export and Import Service Configuration*s in *CPS Operations Guide*.

View Versioned Custom Reference Data Tables

You can view the SVN CRD data of a specific versioned CRD table under the **Versioned Custom Reference Data** option. The versioned CRD tables represents a combined list of custom reference data tables present under Custom Reference Data tables and different Search Table Groups whose **Svn Crd Data** checkbox is enabled.

View Details of Versioned CRD Tables

Perform the following steps to view the CRD data of a versioned CRD table:

Step 1 Navigate to **Versioned Custom Reference Data** under **Policy Builder**.

Step 2 To view details, select a versioned CRD table listed.

The versioned CRD table details is displayed.

Import Data of Versioned CRD Tables

Perform the following steps to import CRD data of a versioned CRD table:

Step 1 Navigate to **Versioned Custom Reference Data** under **Policy Builder**.

Step 2 Click **Import** option provided against the CRD table whose data you want to import.

The **File to Import** dialog box is displayed from where you can select a CSV file containing CRD data to be imported.

Step 3 Select a file.

Step 4 After the file is loaded, select **Import**.

File imported success message is displayed.

View Graphical Illustration of CRD Tables

The **Experimental CRD visualization** option under Policy Builder enables you to view Search Table Group relationships graphically. The nodes displayed are Search Table Groups and the links show where column data for a search table group is pulled from another table with the "Bind to a result column from another table" setting.

You can select an STG element, view its details in the Selected Info dialog box and save the layout.

STG displays the following information:

- Layout nodes.
- Switched display of STG elements to list STG result columns instead of CRD Columns.
- Indicates columns in CRD tables under STG displaying 'keys' (key symbol) or 'required' (*).
- Indicates where columns get their values from such as subscriber AVP, other CRD column, and session data field.

Note This is a proof of concept (POC) feature and is subject to change at the sole discretion of Cisco. Accordingly, Cisco will have no liability in the failure of its functionality.

View Details of STG Element

Perform the following steps to view details of the STG element:

Step 1 Log in to the **CPS Central**.

Step 2 Select **Experimental CRD visualization** under **Policy Builder**.

Step 3 To view details, select an STG element.

The following details are displayed:

Table 37: STG Element Parameters

Field	Description
STG Name	Name of the search table group.
STG Columns	Search table group columns.
Child Custom Reference Data Tables	Child custom reference data tables.

Step 4 Enter STG name in the **Search for Table Name** field.

Suggestions are provided as you type STG names.

The respective STG cell is selected in the graph. The following details are displayed in Details box:

Table 38: STG Cell Details

Field	Description
STG Name	Name of the STG table.
Evaluation order	Evaluation order of STG table.
STG result columns	Display STG result column name. If any STG result column is getting referenced with another STG then plus symbol is provided which when clicked displays the STG tables name.
Child CRD details	Display of child customer reference data tables details. If any CRD column is getting referenced with another CRD then plus symbol is provided against same CRD column which when clicked displays the CRD tables name.

The table format are as follows:

- From: {STG-NAME}.{CRD-COLUMN-NAME} – RESULT column is reference by a column.
- From: {CRD-TABLE-NAME}.{CRD-COLUMN-NAME} – CRD column is referenced by a column.

Plus symbol is provided against number of references which when clicked displays the table names that reference the column. The plus symbol changes to minus which when clicked displays the table names collected.

View Repository Details

Policy Builder displays an option that enables you can view a list of repositories as follows:

- Select **Repository** to navigate repositories list page, to view repository details and to reload configurations of the selected repository.
- Select the drop-down to view the available repositories.

To switch to a new repository by selecting a repository from the dropdown list, user will have to re-login to authenticate the user with the selected repository.

The following table describes the various URL/fields available in repository:

Table 39: Repository Parameters

Fields	Description
Name	Name of the repository
URL	URL of the branch of the version control software server that are used to check in this version of the data.
SVN Username	Username that is configured to view Policy Builder data.
Temp Directory	Temporary working local directory for the policy configurations.
Reload Repository	Select to reload the repository from the file system. **Note** Reload link is available only when the repository matches the selected (working) repository.

Add New Repository

Perform the following steps to add a new repository:

Step 1 In CPS Central, navigate to **Policy Builder Overview**.

A **Choose Policy Builder Data Repository** dialog box is displayed.

Step 2 Click **Add Repository** link.

An **Add Repository** dialog box is displayed with the following fields/URL:

Fields	Description
Name	Name of the repository.
URL	URL of the branch of the version control software server that is used to check in this version of the data.
Local Directory	Local directory for the policy configurations. The standard path for Local Directory is /var/broadhop/pb/workspace/tmp-repository_name.

Step 3 Enter valid values.

Note If the mandatory fields are not entered, an error message is displayed.

Step 4 Click **OK**.

a. After entering values in the repository fields, the progress bar should display and hide when the response from API is returned.

b. If there is an error response from the API, it should be displayed in the error modal. On closing the error modal the add repository modal with the old values is displayed.

Select Repository

When you select Policy Builder option in the CPS Central interface, a **Choose Policy Builder Data Repository** dialog box is displayed which enables you to select a repository.

Note The dialog box to select a repository is displayed only if you have not loaded any repository earlier. In case any error occurs while loading the available repositories, an error dialog is displayed. When you click **Close**, the Central landing page is displayed.

Perform the following steps to select a repository:

Step 1 In CPS Central, navigate to **Policy Builder Overview**.

A **Choose Policy Builder Data Repository** dialog box is displayed.

Step 2 Click the **Select Repository** drop-down.

Step 3 Select a repository from the drop-down list.

Step 4 Click **Done**.

The selected repository is loaded.

Note If you click **Cancel**, the application is redirected to the central landing page as there is no repository loaded.

Switch Repository

Perform the following steps to switch repositories:

Step 1 In CPS Central, navigate to **Policy Builder Overview**.

Step 2 Select the **Switch Repository** icon.

A **Choose Policy Builder Data Repository** dialog box is displayed.

Note The repository which is currently loaded is displayed as selected in the repository drop-down.

Step 3 Click the **Select Repository** drop-down.

Step 4 Select a repository from the drop-down list.

Step 5 Click **Done**.

The selected repository is loaded.

Note You are notified with appropriate error messages during switching repositories in the following scenarios:

- Failure from API end.
- When SVN is down.
- When the request gets timed out.

Publish Configuration Changes

Publish enables you to publish all the changes made in the Policy Builder.

Perform the following steps to publish changes:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Policy Builder**.

Step 3 Select Publish.

The following table describes the various URL/fields available in Publish:

Table 40: Publish Parameters

Field	Description
Enter a comment for the commit operation	Select to enter a commit comment.
Changes	Displays all the configuration changes made.
Revert All	Select to revert all the changes made in Policy Builder.
Publish To	Points to CPS server SVN configurations repository where CPS server polls for SVN changes. After receiving the update notification, CPS server will check out the latest configurations from SVN.
Commit and Publish	Select to commit and publish.

View Notifications

You can view notifications regarding various stages of all CPS products by selecting the **Alert** option provided in the toolbar.

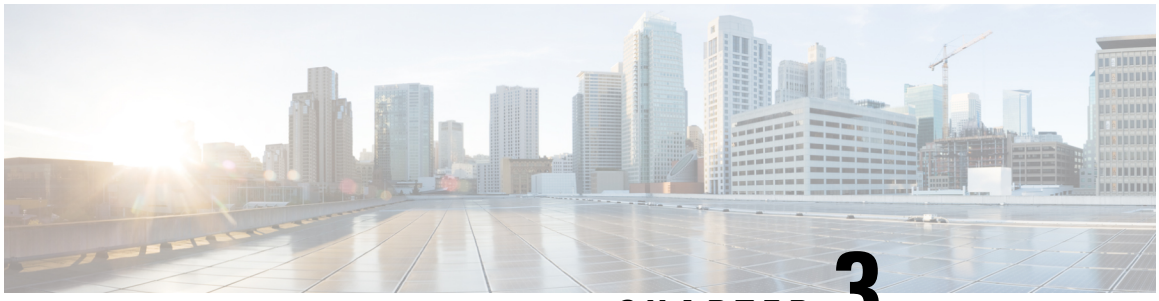
Perform the following steps to view notifications:

Step 1 Click **Alert**.

A notification message is displayed.

Step 2 Click **Accept**.

Note
- After the notification is accepted, the toolbar reverts to the default color.
- If the system upgrade deadline is approaching, the accept option is not displayed and the toolbar continues to display the alert link and notification.



CHAPTER 3

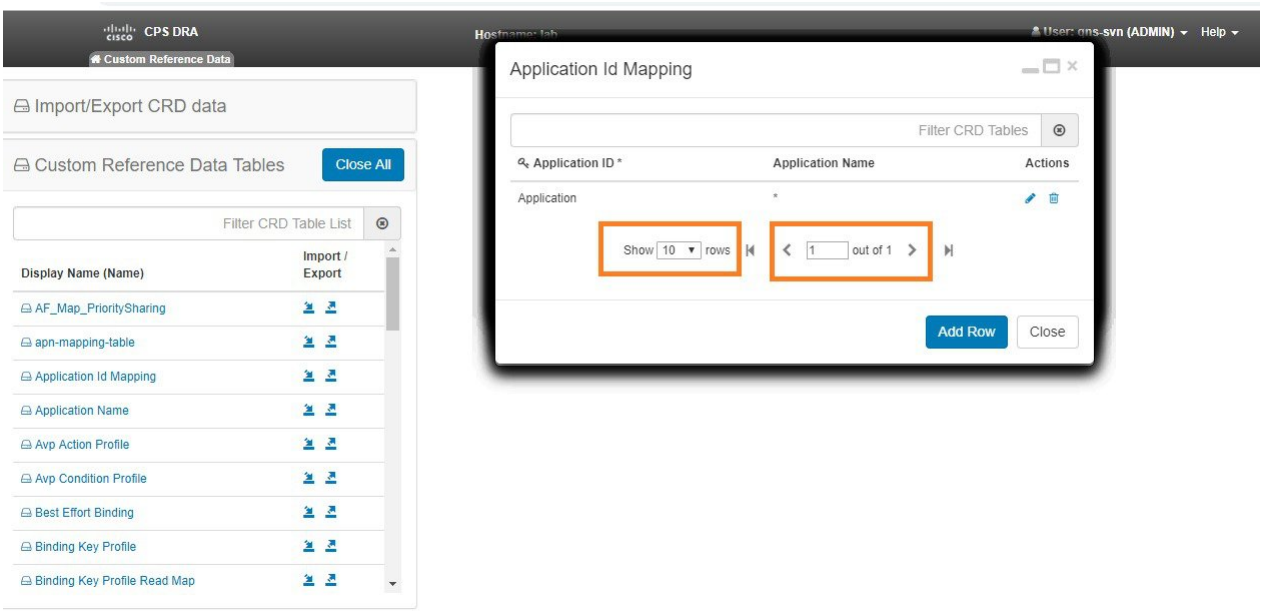
Managing Custom Reference Data

Custom Reference Data Overview

Custom reference data is data specific to a service provider and provides a way to create their own data tables and to populate them. It adds variations of existing use cases configured in Policy Builder.

Note All Policy Servers (qns) must be restarted after a CRD table schema is modified (for example, column added/removed).

CRD also supports the pagination component in which the data is displayed according to the number of rows configured per page. You can change the number of rows to be displayed per page. Once you set the value for rows per page, the same value is used across the Central unless you change it. Also, you can navigate to other pages using the arrows.



Import And Export CRD Data

The Import/Export CRD data option enables you to perform the following operations:

- Enables users to export the CRD data packaged in .crd file
- Enables users to import the CRD tables in a CSV format

A valid imported file should follow CRD schema and should have all required files.

Export Custom Reference Data

Perform the following steps to export CRD data:

Step 1 Log in to the **CPS Central**.

Step 2 Click **Custom Reference Data**.

Step 3 Click **Import/Export CRD Data**.

Under **Export Custom Reference Data**, the following options are displayed:

- *Use 'zip' file extension*. Enables easier viewing of export contents for advanced users.
- *Export CRD to Golden Repository*. When system is in BAD state then crd cache will be built by using golden-crd data.

Export CRD in Zip File

Step 1 Select *Use 'zip' file extension* check box to export contents of the CRD table in a csv format in zip file.

Step 2 Click **Export**. The zip file pops up and lets you save or open the file.

Step 3 Click **Save File**.

Step 4 Click **OK**.

Export CRD to Repository

Step 1 Select *Export CRD to Golden Repository* check box to export CRD to golden repository which can be used to restore cust_ref_data in case of error scenario(s). A new input text box is displayed.

Step 2 Add a hostname or IP address to push CRD to repository. You can add multiple hostnames or IP addresses by clicking on the plus sign.

Note During adding of SVN destination, you can complete the entry by clicking on the button with the plus sign or pressing Enter. Upon completing the entry, the input is validated. If the input is invalid, it is rejected and an error message is displayed. Valid entries are stored in chronological order of entry, into separate input fields which are disabled. If you choose not to have a particular SVN destination, you can delete the entry by clicking the delete sign.

Step 3 Click **Export** to push the CRD to golden-crd svn location. A success message is displayed.

In case of exceptions, error response message is sent to client with response code as “500”.

Export CRD using CLI

You can execute the following curl command to export existing CRD data into SVN.

```
curl -s -S -k -u <username>:<password>-H Content-Type:application/json -X
GET https://<server-ip>:<port>/proxy/custrefdata/_export?goldenCrdSvnUrl=<SVN_HOST>
```

After sucessful curl command execution , CRD data is pushed to golden-crd location and success response is sent to client in JSON format.

```
{"statusCode" : "200","message":"Golden CRD exported sucessfully"}
```

You can provide different SVN locations with comma separated. goldenCrdHost must contains only valid IPv4 address or a hostname. On executing curl command with multiple SVN locations is validated. If goldenCrdHost is invalid, it is rejected and an error message is sent to client.

```
{"statusCode" : "500","message":" goldenCrdHost must contains only valid IPv4
address or a hostname"}
```

In case of any other exceptions, error response message is sent to client with response code as “500”.

Manually Pushing CRD

You can also push CRD to golden_crd SVN location. You can download CRD data from Control Center or PB Central then extract the zip/crd archive file.`%;`

Create a `.metadata` file in same CRD extracted directory and add crdversion into `.metadata` file. You can get CRD version from cust_ref_data collections from MongoDB.

```
crdversion=MONGO_CRD_VERSION
```

You can push all the contents from CRD extracted directory to Golden CRD SVN location (http://<*IP* | *Hostname*>/repos/golden-crd.

Push all the contents using SVN Import command from CRD extracted directory using the following command:

```
svn import http://<IP | Hostname>/repos/golden-crd -m "pushing golden-crd manually"
```

Import Custom Reference Data

Perform the following steps to import CRD tables:

Step 1 Log in to the **CPS Central**.

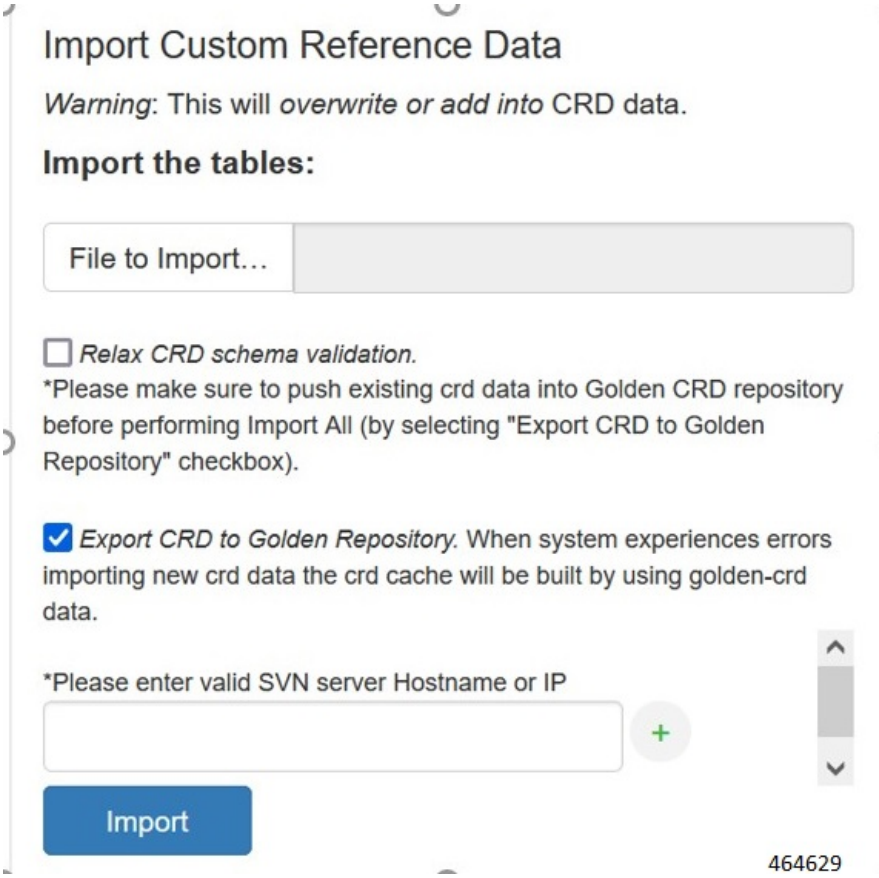
Step 2 Click **Custom Reference Data**.

Step 3 Select **File to Import…**

The **File Upload** dialog box is displayed from where you can select a file to be imported.

Step 4 (Optional) Check the **Export CRD to Golden Repository** check box to first export the CRD data to the Golden Repository before Importing CRD. Enter a valid SVN server Hostname or IP.

Figure 2: Export CRD to Golden Repository



Note

- Check the **Export CRD to Golden Repository** only for bulk import and export. If the export fails an error message is displayed.
- If you do not select the **Export CRD to Golden Repository** check box, CRD data files are imported to the Database.
- If export is successful, then, import process of CRD takes effect.

Step 5 Click **Import**.

Note A warning message is displayed in the success modal for bulk import of CRD tables when the archive file to import has CRD tables with Svn Crd Data flag enabled.

View Custom Reference Data Tables

Custom Reference Data Tables section lists the custom reference data (CRD) tables in an alphabetic order along with its description.

You can select a CRD table from the displayed list and view its data. The search filter is added to support full and partial string match.

A key icon is displayed before the column name of the selected CRD tables. This provides the following information:

- Indicates whether the column in the selected CRD table is a key column or non-key column.
- Indicates the type of Runtime Binding and its value in a tooltip when you hover over it.

The following operations can be performed:

- Add a record to the table
- Edit record of the table
- Delete a record of the table

The results are paginated for easy access and scrollbars can be used when there are more number of columns.

Note The edit, delete and add options are disabled for CRD tables with Svn Crd Data flag enabled.

View Multiple CRD Tables

Step 1 Navigate to **Custom Reference Data**.

Step 2 In the left-hand pane, select CRD tables listed under **Display Name**.

The tables are displayed on the right-hand side. You can drag and resize the tables horizontally.

Step 3 Click **Close**.

Note
- By default the **Custom Reference Data Tables** tab is expanded. Only one of the panels can be expanded at a time. For example, when the **Import/Export CRD data** tab is expanded, the **Custom Reference Data Tables** tab is closed and vice versa.
- You can use the scroll bar to view records in a large CRD table.
- You can use the **Add Row** option to enter records.
- You can use the **Close** option to close a CRD table.
- You can click **Close All** option to close multiple tables.

Edit Multiple CRD Tables

Step 1 Navigate to **Custom Reference Data**.

Step 2 In the left-hand pane, select CRD tables listed under **Display Name**.

The tables are displayed on the right-hand side.

a. To modify record values, click edit icon. A CRD record modal popup is displayed.

b. To enter record values, click **Add Row**.

c. To delete records, click delete icon.

Step 3 Click **Done**.

Step 4 Click **Close**.

Note
- You can edit only one CRD table at a time.
- The SVN CRD tables have only read only option.
- You can click **Close All** option to close multiple tables.

Import Custom Reference Data Table

Perform the following steps to import a custom reference data table:

Step 1 In CPS Central, navigate to **Custom Reference Data**.

Step 2 Select any CRD table.

Step 3 Click the **Import** option provided against the selected CRD table.

The **File to Import** dialog box is displayed from where you can select a file to be imported.

Note The import link is disabled for CRD tables with Svn Crd Data flag enabled.

Step 4 Select a file.

Step 5 After the file is loaded, Click **Import**.

Note

a. The selected file should be of XLS or CSV format.

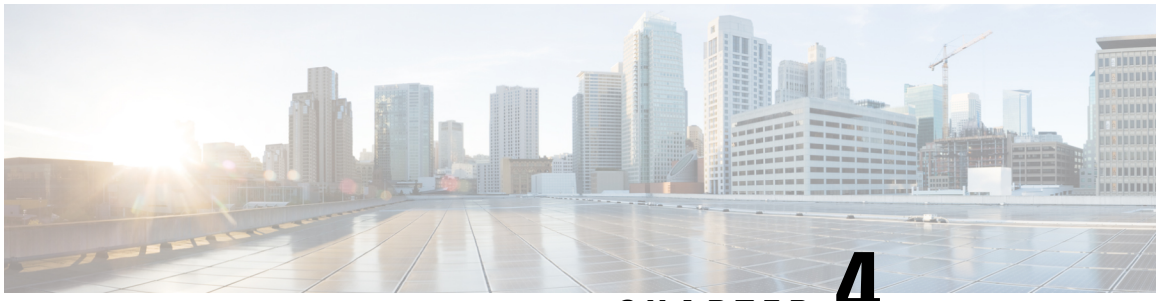
b. The name of the selected file should match that of the CRD table name.

c. If you try to import data with wrong headers, "Mismatch found between imported csv headers and policy builder table columns" error message is displayed.

d. If you try to import data having duplicate records, "Duplicate rows found in the imported data for table: (table_name). Duplicate records count: (duplicate_count)? error message is displayed.

e. If you try to import multiple CRD tables during traffic it may have call flow impact. It is recommended to import multiple CRD tables during maintenance window.

Data Imported success message is displayed.



CHAPTER 4

Managing Central Operations

Access User Interfaces

This section includes the following topics:

- Monitoring Installation Using Grafana
- Managing Subscribers Using Control Center

Monitoring Installation Using Grafana

Grafana is a third-party metrics dashboard and graph editor. Grafana provides a graphical or text-based representation of statistics and counters collected in the Graphite database.

For more information about Grafana in CPS, refer to the Graphite and Grafana chapter in the *CPS Operations Guide*.

Managing Subscribers Using Control Center

The Control Center Interface enables you to manage subscribers and perform various operations to get information about subscribers, track subscriber sessions, to construct and populate custom reference data tables and so on.

CPS enables users to be aware of its current privileges while accessing Control Center as describes 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.

Depending on your role and permissions, you can view certain screens in Control Center Interface. The following table describes the two roles and their respective access of Control Center Interface.

Table 41: Control Center Tasks

Task	Full Privilege Administrator	View Only Administrator
Find a Subscriber	√	√
Create a Subscriber	√	NA
Edit a Subscriber	√	NA
Change the Credential ID of a Subscriber	√	NA
Deactivating or Activating a Subscriber	√	NA
Delete a Subscriber	√	NA
Overview Screen	√	√
Details Screens	√	√
General Screen	√	√
Credentials Screen	√	√
Services Screen	√	√
Add a Service to a Subscriber	√	NA
Remove a Service from a Subscriber	√	NA
Notifications Screen	√	√
Subaccount Screen	√	√
Sessions Screen	√	√
Session Details Table	√	√
Remove a Session	√	NA
Balance Screen	√	√
Balances	√	√
Quotas	√	√
Managing Quotas and Balances	√	NA
Viewing Quotas and Balances	√	√
Add a Balance Type	√	NA
Credit or Debit an Existing Balance	√	NA

Task	Full Privilege Administrator	View Only Administrator
Delete a Balance	√	NA
Delete a Quota	√	NA
Check the History of Balances	√	√
View a Subscriber Session	√	√
Find Network Sessions	√	√

For more information on Control Center, see *CPS CCI Guide for Full Privilege Administrators* and *CPS CCI Guide for View-Only Administrators*.

Viewing APIs

API documentation includes the following APIs:

- Service Orchestration API: to manage Policy Builder data
- Unified API Schema/Docs: to manage subscribers

Select the link to the API documentation on the CPS home page to view the documentation and usage examples.