Oracle® Communications

Policy Control Function Cloud Native User's Guide

Release 1.5

F29381-01

March 2020

Oracle Communications Policy Control Function Cloud Native User's Guide, Release 1.5

F29381-01

Contents

Part I Using Policy Control Function Console

8 Configuring Policy Control Function

9 Session Viewer

10 Managing Match Lists

11 Managing Policy

12 System Administration

List of Figures

List of Tables

What's New in This Guide

This section introduces the new features for Release 1.5 in Oracle Communications Policy Control Function (PCF) Installation Guide.

New Features for Release 1.5

For PCF Release 1.5, this guide has been updated to include the following new development features:

- Support for new PCF services has been added. See About Policy Control Function Services
- Added PCF Metrics. See Policy Control Function Metrics

Significant Documentation Updates for Release 1.5

For this release, the guide was updated to reflect the new user interface. Tasks affected by the user interface change were also updated. See Using Policy Control Function Console

1 Introduction

This document provides information on how to use the Policy Control Function and configure the services.

Overview

The Policy Control Function (PCF) is a functional element for policy control decision and flows based charging control functionalities. The PCF provides the following functions:

- Policy rules for application and service data flow detection, gating, QoS, and flow based charging to the Session Management Function (SMF)
- Access and Mobility Management related policies to the Access and Mobility Management Function (AMF)
- Provide UE Route Selection Policies (URSP) rules to UE via AMF

The PCF supports the above functions through the following services:

- Session Management Service
- Access and Mobility Service
- Policy Authorization Service
- User Equipment (UE) Policy Service

Acronyms and Terminology

The following table provides information about the acronyms and the terminology used in the document.

Table 1-1 Acronyms and Terminology

Acronym	Definition
AMF	Access and Mobility Management Function
BSF	Binding Support Function
CHF	Charging Function
CM	Configuration Management
CUSTOMER_REPO	The docker registry address in customer side, plus Port No. if registry has port attached
IMAGE_TAG	The image tag from release tar file is 1.5.0, You can decide to use any tag No. Then push related docker image with that specific tag to their registry.
MCC	Mobile Country code
METALLB_ADDRESS_POOL	The address pool which configured on metallb to provide external IPs

Table 1-1 (Cont.) Acronyms and Terminology

Acronym	Definition
MNC	Mobile Network code
NRF	Network Repository Function
PCF	Policy Control Function
SAN	Storage Area Network
SMF	Session Management Function
UDR	Unified Data Repository

References

User can refer to the following documents for information.

- Oracle Communications Cloud Native OAM User's Guide
- Oracle Communications Policy Control Function Cloud Native Installation Guide
- https://developers.google.com/blockly
- 3GPP Technical Specification 29.512 v15.3.0, Session Management Policy Control Service, Stage 3, Release 15
- 3GPP Technical Specification 29.514 v15.3.0, Policy Authorization Service, Stage 3, Release 15
- 3GPP Technical Specification 29.507 v15.3.0, Access and Mobility Policy Control Service, Stage 3, Release 15
- 3GPP Technical Specification 29.525 v15.5.1, UE Policy Control Service, Stage 3, Release 15
- 3GPP Technical Specification 29.518 v15.5.1, Access and Mobility Management Services, Stage 3, Release 15

2

Policy Control Function Architecture

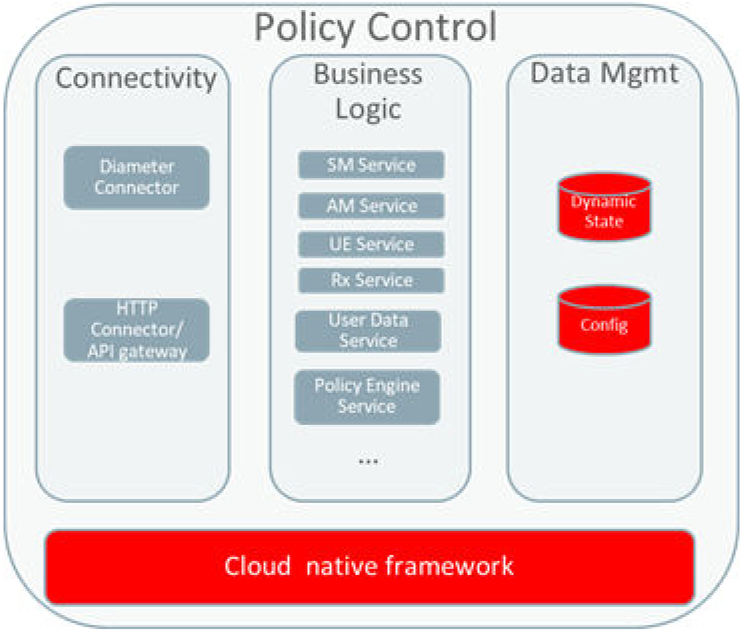
The Oracle Communications 5G Policy Control Function (PCF) solution provides:

- Micro-services based Cloud-Native Architecture
- Policy Design Evolution to support modular and flexible Domain Driven Policy design
- Compliant with 3GPP Release 15 specifications
- Product supports Session Management, Access management and Authorization policy control services
- Flexible, user friendly Policy Design Framework for rapid policy use case deployments
- Pluggable Data Sources to ingest input from a variety of data sources (UDR, LDAP, Analytics, etc.)
- Support of different Deployment Options - PLMN level, slice shared and slice specific

The Oracle Communications Policy Control Function is built as a cloud-native application composed of a collection of microservices running in a cloud-native environment. It separates processing/business logic and state concerns following the corresponding logical grouping of microservices/components:

- **Connectivity**: Components interfacing with external entities. This is where an API gateway is utilized to interface with external traffic to the PCF. These are stateless sets of components.
- **Business logic**: Application layer running the PCRF/PCF business logic, policy engine and various services that can be enabled based on deployment needs. These are stateless sets of components.
- **Data Management**: Data layer responsible for storing various types of persistent data. The PCF is built to be able to plug in different types of backend data layers that could be internal or external.

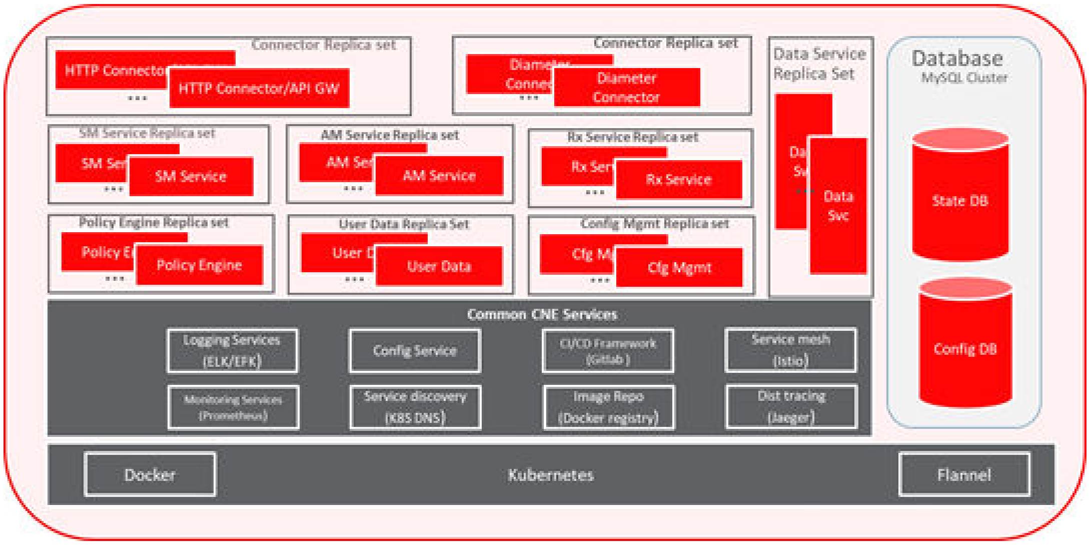
Figure 2-1   PCF Architecture



As a result, an actual policy function can be composed of the necessary micro-services to provide the desired function, For example, a subset of a PCF (e.g. one without usage monitoring, etc).

The Policy Control Function packages its micro-services into containers and leverages Kubernetes' constructs and abstractions such as Pods, ReplicaSets, and services so it can enable Kubernetes to manage and orchestrate the PCF. It also leverages Istio as a service mesh (including Envoy proxies as sidecars) for the internal communication amongst the various micro-services. The Oracle PCF integrates with a variety of common services for data collection, analysis, and visualization services for operational aspects like logs, metrics, and traces. The Oracle 5GC PCF comprises artifacts like Helm charts that encapsulate lifecycle instructions and resource dependencies for all member components.

The Oracle PCF is flexible to run in various cloud-native environments. The Policy Control Function can be configured to leverage common services provided by the cloud-native environment and/or provide its own set if certain common services aren't provided by the underlying environment. It gather inputs from various interfaces (For example, SMPolicyControl etc.) defined by 3GPP but it also has to be flexible to plug in additional data sources to adapt to an operator's environment and available data. Below is a diagram illustrating the above description:

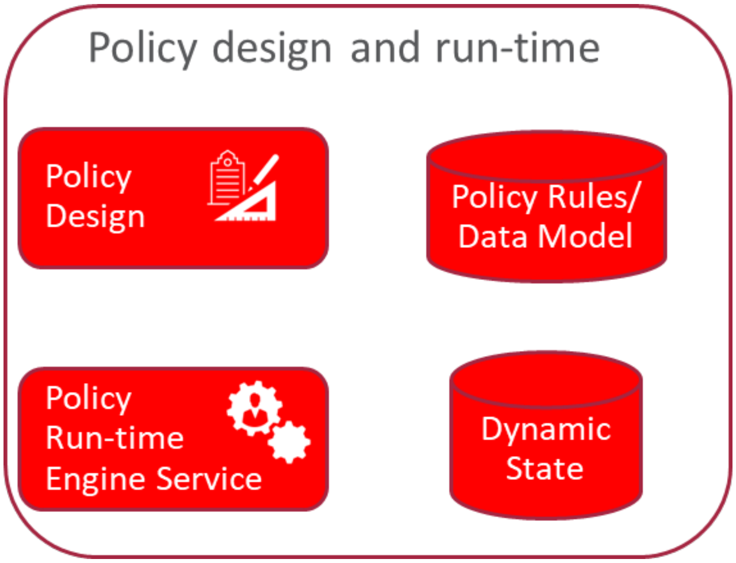

Connector Replica set
HTTP Connector
HTTP Connector/API GW
Connector Replica set
Diameter
Connec
Diameter
Connector
Data Service
Replica Set
Da
Sv
Data
Svc
Database
MySQL Cluster
SM Service Replica set
SM Ser
SM Service
AM Service Replica set
AM Se
AM Service
Rx Service Replica set
Rx Ser
Rx Service
State DB
Policy Engine Replica set
Policy E
Policy Engine
User Data Replica Set
User D
User Data
Config Mgmt Replica set
Cfg M
Cfg Mgmt
Common CNE Services
Logging Services
(ELK/EFK)
Config Service
CI/CD Framework
(Gitlab)
Service mesh
(Istio)
Config DB
Monitoring Services
(Prometheus)
Service discovery
(K8S DNS)
Image Repo
(Docker registry)
Dist tracing
(Jaeger)
Docker
Kubernetes
Flannel

3 About Policy Design Experience

Policy design experience allows an operator to craft and deploy, from scratch, operator policies in production in very less time. 5G brings the policy design experience to the next level by providing flexibility, extensibility, modularization, and assurance to the operator to rapidly, yet confidently deploy new operator policies and enable use cases more faster.

The following figure highlights the various components used by the policy design and run-time:

Figure 3-1 Policy Design Experience



Design

- Modular and flexible domain driven policy design
- Modules encompasses data model, triggers, conditions and actions
- Modules can be designed via a GUI (very intuitive, can be used by anyone) and allows any language supported by JVM for advances cases if needed (e.g. Java, Groovy, etc)
- Pre-packaged modules provided by Oracle
- Modules can be extended or built by operators

Run-time

- Run-time engine service to expose APIs
- Run-time engine service to be stateless and independently scalable
- Newly designed policies or policy updates can be rolled out in an incremental fashion (e.g. to a specific set of policy run-time engines) to enable canary releases and ensure updates are working as expected before being rolled out globally

Debugging and testing

- Debugging policy logic capability as a complementary tool to the design experience
- Automated testing framework to enable regression and validation of policy logic and modules before deployment

4
About Policy Control Function Services

About Session Management Service

Oracle Communications Policy Control Function (PCF) implements policy control for session management for service data flows. PCF implements N7 interface to trigger session management policies towards Session Management Function (SMF). SMF controls the User plane Function (UPF) . It translates policies received from the PCF to a set of directives/ information understood to the UPF and then forwards it to the UPF.

Session Management Service supports the following:

- Enforcement control of policy decisions related to QoS, charging, gating, service flow detection, packet routing and forwarding, traffic usage reporting.
- Enforcement of QoS, charging, gating, service flow detection, packet routing and forwarding and traffic accounting and reporting policy decisions can be distributed among the UPF, Radio Access Network (RAN) and User Equipment (UE) depending on the policy type.

Oracle Communications PCF supports the following 3GPP defined services for Session Management:

Table 4-1 Session Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_SMPolicyControl_Create	Request to create an SM Policy Association with the PCF to receive the policy for a PDU session	SMF	{apiRoot}/npcf-smpolicycontrol/v1/sm-policies	POST
Npcf_SMPolicyControl_Delete	Request to delete the SM Policy Association and the associated resources	SMF	{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/delete	POST
Npcf_SMPolicyControl_Update	Request to update the SM Policy association with the PCF to receive the updated policy when Policy Control Request Trigger condition is met	SMF	{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/update	POST

Table 4-1 (Cont.) Session Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_SMPolicyControl_UpdateNotify	Update and/or delete the PCC rule(s) PDU session related policy context at the SMF and Policy Control Request Trigger information	PCF	{Notification URI}/update {Notification URI}/terminate	POST

About Access and Mobility Management Service

Oracle PCF implements access management service-related policies over N15 interface towards the Access and Mobility Management Function (AMF).

Access and Mobility Management Service supports the following:

- Enforcement control of policy decisions related to Radio Access Technology (RAT)/ Frequency Selection Priority
- Enforcement of Service Area Restrictions is executed in the UE
- Enable location tracking for a UE to get periodic updates on subscriber current location

Oracle Communications PCF supports the following 3GPP defined services for Access and Mobility Management:

Table 4-2 Access and Mobility Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_AMPolicyControl_Create	Creates an AM Policy Association and provides corresponding policies to the Network Function (NF) consumer	AMF	{apiRoot}/npcf-am-policy-control/v1/policies/	POST

Table 4-2 (Cont.) Access and Mobility Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_AMPolicyControl_Update	Updates of an AM Policy Association and provides corresponding policies to the NF consumer when the policy control request trigger is met or the AMF is relocated due to the UE mobility and the old PCF is selected	AMF	{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}/update	POST
Npcf_AMPolicyControl_UpdateNotify	Provides updated policies to the NF consumer	PCF	{{Notification URI}/update {Notification URI}/terminate	POST
Npcf_AMPolicyControl_Delete	Provides means for the NF consumer to delete the AM Policy Association	AMF	{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}	DELETE

About Policy Authorization Service

Oracle Communications Policy Control Function (PCF) implements policy authorization service that authorizes an Application Function (AF) request over N5 interface.

Policy Authorization Service supports the following:

- Creates policies as requested by AF for the Protocol Data Unit (PDU) session. Policy authorization service is a critical function for IP Multimedia Subsystem (IMS) integration and dynamic Policy and Charging Control (PCC) rule creation

Oracle Communications PCF supports the following 3GPP defined services for Policy Authorization:

Table 4-3 Policy Authorization Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_PolicyAuthorization_Create	Determines and installs the policy according to the service information provided by an authorized NF service consumer.	AF, Network Exposure Function (NEF)	{apiRoot}/npcf-policyauthorization/v1/app-sessions	POST
Npcf_PolicyAuthorization_Update	Determines and updates the policy according to the modified service information provided by an authorized NF service consumer.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}	PATCH
Npcf_PolicyAuthorization_Delete	Provides means to delete the application session context of the NF service consumer.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete	POST
Npcf_PolicyAuthorization_Notify	Notifies NF service consumer of the subscribed events.	PCF	{notifUri}/notify {notifUri}/terminate	POST
Npcf_PolicyAuthorization_Subscribe	Allows NF service consumers to subscribe to the notification of events.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription	PUT
Npcf_PolicyAuthorization_Unsubscribe	Allows NF service consumers to unsubscribe to the notification of events.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription	DELETE

About UE Management Service

Oracle PCF implements User Equipment (UE) management service-related policies over N15 interface towards the AMF.

UE Management Service supports the following:

- Transfer of UE Route Selection Policies (URSP) rules to UE

Oracle Communications PCF supports the following 3GPP defined services for UE Management:

Table 4-4 UE Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_UEPolicyControl_Create	Creates a UE Policy Association	AMF	{apiRoot}/npcf-ue-policy-control/v1/policies/	POST
Npcf_UEPolicyControl_Delete	Provides means for the NF consumer to delete the UE Policy Association	AMF	{apiRoot}/npcf-ue-policy-control/v1/policies/{polAssoId}	DELETE
N1N2MessageSubscribe	Creates a subscription for N1 Message Transfer	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions	POST
N1N2MessageUnSubscribe	Deletes a previously created subscription for N1 Message Transfer	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions/{subscriptionId}	DELETE
N1N2MessageTransfer	Transfer an N1 message (NAS message) that is to be delivered to the UE	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages	POST
N1MessageNotify	Indicate status of an N1 Message Transfer	PCF	{Notification URI}	POST

5 Configuring Policy Control Function

This section provides the information for configuring Oracle Communications Policy Control Function (PCF) for various services.

PCF offers the following interfaces to configure the PCF system:

- A web-browser based Graphical User Interface
- A REST API based Machine-to-Machine interface
- Kubernetes Configuration Maps

The minimum configurations required to bring up a working PCF instance is described in the below sections.

For more detailed and elaborate configuration information, please refer Using Policy Control Function Console.

For REST API information, please refer *Oracle Communications Policy Control Function (PCF) Cloud Native REST Specification Document*.

Network Repository Function (NRF) Configuration

A Kubernetes Configuration Map is provided to save the NRF address and the NF Profile information. You can edit the Kubernetes Configuration Map to register Policy Control Function (PCF) with the NRF.

To edit the Kubernetes Configuration Map

Open a console to the master node of the Kubernetes deployment and edit the config map named "*pcf-name*-application-config" where *pcf-name* is the HELM chart release name used at the time of installation, please refer

1. Get a list of all the config maps in the PCF deployment namespace by entering this command:

   ```
   kubectl get cm -n pcf-namespace
   ```

   where, *pcf-namespace* is the PCF deployment namespace used by helm command.
2. Edit the application configuration map by entering this command:

   ```
   kubectl edit cm pcf-name-application-config -n pcf-namespace
   ```

   where, *pcf-name* is the release name used by helm command.
   A standard unix vi editor is opened with the config map contents pre-filled. Use vi commands to edit the application configuration map.
3. Verify the NRF address (fqdn/IP) and the port number.
4. Check and add necessary NFs to "nrfClientSubscribeTypes". These NFs will be discovered and subscribed by PCF at the startup time. Leave this field empty if this onetime discovery and subscription for NFs is not required.

5. Check and edit, as necessary, the PCF Profile to be registered with the NRF. For example, if required enter the IP details of the PCF Services.
6. Save and exit the editor.

Global Configurations

You can manage and view the Global Configurations from this page.

To edit the Global Configurations:

1. From the navigation menu, under **PCF**, click **Global Configurations**.
   The Global Configurations screen appears.
2. Click **Edit** to edit the global configurations.
3. In the **API Gateway Host** field, enter the name for the API gateway host.
4. In the **API Gateway Port** field, enter the port number of the API gateway. (if a port other than the default is being used)
5. Click **Save**.

Diameter Configurations

You can manage and view the Diameter Configurations from this page.

Settings

To edit the Settings:

1. From the navigation menu, under **PCF**, and then under **Diameter Configurations**, click **Settings**.
   The Settings screen appears.
2. Click **Edit** to edit the settings.
3. Enter the following information:
   - **Reconnect Delay (sec)**- Enter the time frame to delay before attempting to reconnect after a connection failure in seconds. The default is 3 seconds.
   - **Response Timeout (sec)**- Enter the response timeout interval in seconds. The default is 5 seconds.
   - **Connection Timeout (sec)**- Enter the connection timeout interval in seconds. The default is 3 seconds.
   - **WatchDog Interval (sec)**- Enter the watchdog interval in seconds. The default is 6 seconds.
4. Click **Save**.

Peer Nodes

To edit the Peer Node Configurations:

1. From the navigation menu, under **PCF**, and then under **Diameter Configurations**, click **Peer Node**.
   The Peer Node Configurations screen appears.
2. Click **Add** to create peer node.

The Create Peer Node screen appears.

3. Enter the following information:
    - **Name**- Unique Name of the peer node.
    - **Type**- Defines which type of diameter service it should take up. The value can be Application function (af) or diameter routing agent(dra).
    - **Initiate Connection**- Set it to True to initiate a connection for this peer node.
    - **Port**- Enter the port number. Enter a number from 0 to 65535.
    - **Host**- Enter the host name. Enter a FQDN, ipv4 or ipv6 address available for establishing diameter transport connections to the peer node .
    - **Realm**- Enter the realm name, that is, FQDNs to all of that computers that transact diameter traffic.
    - **Identity**- Enter a identity to define a node in a realm.
4. Click **Save**.

> **Note:**
>
> You can import and export the Peer Node configurations by clicking on the **Import** and **Export** on the Peer Node Configurations screen.

Service Configurations

You can tailor the PCF services as per network operator's requirements using the Service configuration pages. The configurations include setting up end point addresses, setting up log levels and other debug information like tracing etc. and customizing and/or optimizing NF interactions for example with UDR etc.

Configuring Session Management Service

You can configure the session management service from this page.

To configure the Session Management Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **Session Management Service**.
   The Session Management Service screen appears.
2. Click **Edit** to edit the session management service configurations.
3. Check the default configuration for all the fields in all groups and edit as necessary.
4. Click **Save**.

Refer Using Policy Control Function Console for the fields details.

Configuring Access and Mobility Service

You can configure the access and mobility service from this page.

To configure the Access and Mobility Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **Access and Mobility Service**.

The Access and Mobility Service screen appears.

2. Click **Edit** to edit the access and mobility service configurations.
3. Check the default configuration for all the fields in all groups and edit as necessary
4. Click **Save**.

Refer Using Policy Control Function Console for the fields details.

Configuring User Service

You can configure the user service from this page.

To configure the User Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **User Service**.
   The User Service screen appears.
2. Click **Edit** to edit the user service configurations.
3. In the **Server Root URL** field, enter the callback URI for notifications to be received by the User service (For example, while creating a subscription for the user with the UDR)
4. Check the default configuration for all the fields in all groups and edit as necessary
5. Click **Save**.

Refer Using Policy Control Function Console for the fields details.

Configuring Policy Authorization Service

You can configure the policy authorization service from this page.

To configure the Policy Authorization Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **Policy Authorization Service**.
   The Policy Authorization Service screen appears.
2. Click **Edit** to edit the policy authorization service configurations.
3. Check the default configuration for all the fields in all groups and edit as necessary
4. Click **Save**.

Refer Using Policy Control Function Console for the fields details.

Configuring UE Policy Service

You can configure the UE policy service from this page.

To configure the UE Policy Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **UE Policy Service**.
   The UE Policy Service screen appears.
2. Click **Edit** to edit the UE policy service configurations.
3. In the **Notification URI Root** field, enter the callback URI for notifications to be received by the UE Policy service (For example, while creating a subscription for the NAS Message Transfer with the AMF)
4. Check the default configuration for all the fields in all groups and edit as necessary

5. Click **Save**.

Refer Using Policy Control Function Console for the fields details.

Note:

- The **NAS Message Maximum Packet Size** field is not supported in this release of PCF and will not take effect.
- The **Validate User** and **Query User** fields must always be set to **false** in this release of PCF.

6 Managing Policy

Policy Control Function (PCF) offers a Policy Design editor based on Blockly interface. You can create and manage a policy project for each of the policy services that you wished to deploy:

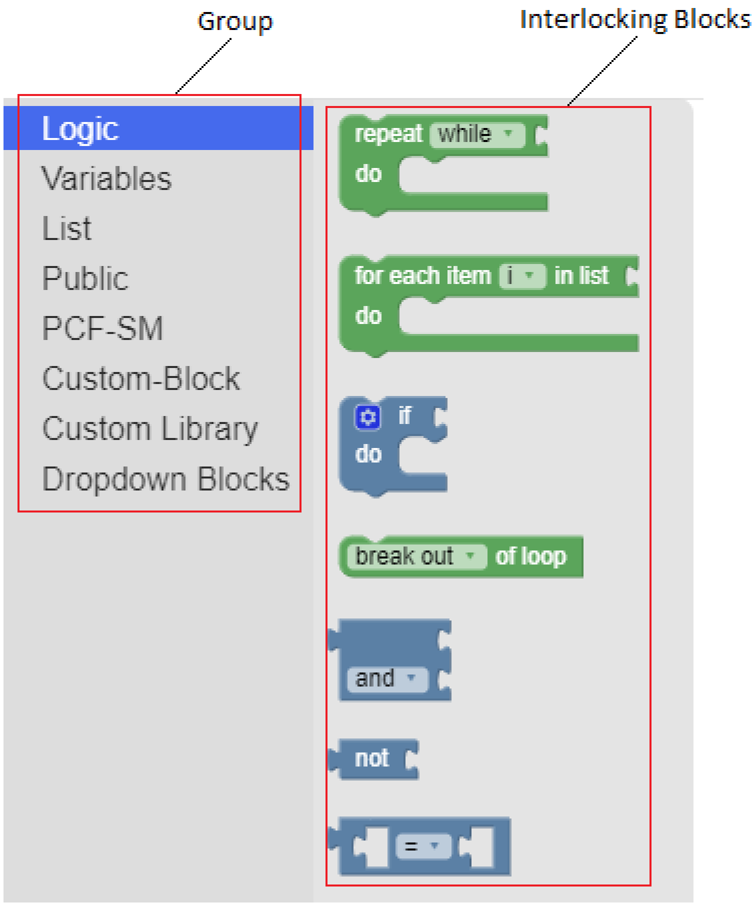
- Session Management
- Policy Authorization
- Access and Mobility Management
- UE Management

Creating a Policy Project

To create a policy project:

1. From the **Policy Management** section of the navigation pane, select **Policy Projects**.
2. Click **Create**.
   The Create Project window opens.
3. In the **Name** field, enter the name for the project.
4. In the **Description** field, enter the description for the project.
5. In the **Service Type**, select the service.
6. Click **Save**.
   The policy project is created.
7. Select the policy project created and click **Open**. This opens a Blockly editor.
   You can construct one or more policies as required using the building blocks provided in the Left Side Panel of the editor.

   The following screen capture shows an example of how the policies can be created using the building blocks.



8. Click **Save**.
   The policy for the selected policy project is created.

7

Policy Control Function Metrics

This chapter includes information about Metrics for Oracle Communications Policy Control Function (PCF).

Table 7-1 Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
1	association_number_per_dnn{application="pcf_smservice",dnn="internet"}	SM Service	counter	Number of active SM session	None
2	requests_total{Request="Get",application="pcf_smservice",}	SM Service	counter	Number of SM policy association get request messages received by PCF	
3	pcf_sm_success_requests_total{Code="2xx",Request="Get"}	SM Service	counter	Number of SM policy association get success response messages received by PCF	
4	pcf_sm_fail_requests_total{Request="Get"}	SM Service	counter	Number of SM policy association get fail response messages received by PCF	
5	pcf_sm_requests_total{Code="4xx",Request="Get"}	SM Service	counter	Number of SM policy association get fail with 4xx error response messages received by PCF	
6	pcf_sm_requests_total{Code="5xx",Request="Get"}	SM Service	counter	Number of SM policy association get fail response messages with 5xx error received by PCF	
7	requests_total{Request="Create",application="pcf_smservice",}	SM Service	counter	Number of SM policy association create request messages received by PCF	PCF receives POST message for resource URL of sm-policies from SMF
8	pcf_sm_success_requests_total{Code="2xx",Request="Create"}	SM Service	counter	Number of SM policy association create success response messages sent by PCF	PCF sends "201 Created" response message

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
9	pcf_sm_fail_requests_total{Request="Create"}	SM Service	counter	Number of SM policy association create Failed response messages sent by PCF.	Count when code is not "2XX" in response message of SM policy association creation sent by PCF, classfied by Application errors. The value of Application errors could be ERROR_INITIAL_PARAMETERS、ERROR_TRIGGER_EVENT、TRAFFIC_MAPPING_INFO_REJECTED、ERROR_CONFLICTING_REQUEST, etc, For details, refer to 3GPP TS 29.512.
10	pcf_sm_requests_total{Code="4xx",Request="Create"}	SM Service	counter	Number of SM policy association create Failed response messages sent by PCF, classfied by Application errors	
11	pcf_sm_requests_total{Code="5xx",Request="Create"}	SM Service	counter	Number of SM policy association create Failed response messages sent by PCF, classfied by Application errors	
12	requests_total{Request="Modify",application="pcf_smservice",}	SM Service	counter	Number of SM policy association update request messages received by PCF from SMF	PCF receives Update(POST) message for resource URL of "sm-policies/{smPolicyId}/update" from SMF

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
13	pcf_sm_success_requests_total{Code="2xx",Request="Update"}	SM Service	counter	Number of SM policy association update success response messages sent by PCF	PCF sends "200 OK" response message
14	pcf_sm_fail_requests_total{Request="Update"}	SM Service	counter	Number of SM policy association update Failed response messages sent by PCF	Count when code is not "2XX" in response message of SM policy association update sent by PCF, classfied by Application errors. The value of Application errors could be ERROR_INITIAL_PARAMETERS、ERROR_TRIGGER_EVENT、TRAFFIC_MAPPING_INFO_REJECTED、ERROR_CONFLICTING_REQUEST, etc. For details, refer to 3GPP TS 29.512
15	pcf_sm_requests_total{Code="4xx",Request="Update"}	SM Service	counter	Number of SM policy association update Failed response messages sent by PCF, classfied by Application errors	
16	pcf_sm_requests_total{Code="5xx",Request="Update"}	SM Service	counter	Number of SM policy association update Failed response messages sent by PCF, classfied by Application errors	

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
17	requests_total{Request="UpdateNotify"}	SM Service	counter	Number of SM policy association update notification request messages sent from PCF to SMF	PCF receives POST message for resource URL of "{NotificationUri}/update" from SMF
18	pcf_sm_success_requests_total{Code="2xx",Request="UpdateNotify"}	SM Service	counter	Number of SM policy association update notification Success messages received by PCF from SMF	SMF sends "200 OK" or "204 No Content" response message
19	pcf_sm_fail_requests_total{Request="UpdateNotify"}	SM Service	counter	Number of SM policy association update notification failed messages received by PCF from SMF	Count when code is not "2OO OK" or "204 No Content" in response message of SM policy association update sent by PCF, classfied by Application errors. The value of Application errors could be PCC_RULE_EVENT or PCC_QOS_FLOW_EVEN, etc. For details, refer to 3GPP TS 29.512.
20	pcf_sm_requests_total{Code="4xx",Request="UpdateNotify"}	SM Service	counter	Number of SM policy association update notification failed messages received by PCF from SMF, classfied by Application errors	
21	pcf_sm_requests_total{Code="5xx",Request="UpdateNotify"}	SM Service	counter	Number of SM policy association update notification failed messages received by PCF from SMF, classfied by Application errors	

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
22	requests_total{Request="Delete",application="pcf_smservice",}	SM Service	counter	Number of SM policy association delete notification request messages received by PCF from SMF	PCF receives Delete(POST) message for resource URL of "sm-policies/{smPolicyId}/delete" from SMF
23	pcf_sm_success_requests_total{Code="2xx",Request="Delete")	SM Service	counter	Number of SM policy association delete notification success messages sent by PCF	PCF sends "204 No Content" response message
24	pcf_sm_fail_requests_total{Request="Delete"}	SM Service	counter	Number of SM policy association delete notification fail messages sent by PCF	
25	pcf_am_associations_count	AM Service	counter	Number of active AM session	None
26	pcf_am_associations_count	AM Service	counter	Number of maximum active AM sessions	None
27	pcf_am_associations_count	AM Service	counter	Number of total AM policy association in PCF	When AM Policy association is created
28	pcf_am_requests_fail_total{Request="Get",}	AM Service	counter	Number of AM policy association get request messages received by PCF	
29	pcf_am_requests_total{Request="Create",}	AM Service	counter	Number of AM policy association create request messages received by PCF	PCF receives POST message for resource URL of policies from AMF
30	pcf_am_requests_success_total{Request="Create",}	AM Service	counter	Number of AM policy association create success response messages sent by PCF	PCF sends "201 Created" response message
31	pcf_am_requests_fail_total{Request="Create",}	AM Service	counter	Number of AM policy association create failed messages	

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
32	pcf_am_requests_total{Request="Update",}	AM Service	counter	Number of AM policy association update request messages received by PCF from AMF	PCF receives Update(POST) message for resource URL of policies/{polAssoId}/update from AMF
33	pcf_am_requests_success_total{Request="Update",}	AM Service	counter	Number of AM policy association update success messages sent from PCF	PCF sends "200 OK" response message
34	pcf_am_requests_fail_total{Request="Update",}	AM Service	counter	Number of AM policy association update fail messages sent from PCF	
35	pcf_am_requests_total{Request="UpdateNotify",}	AM Service	counter	Number of AM policy association update notification request messages sent from PCF to AMF	PCF sends POST message to AMF for resource URL of {Notification URI}/update
36	pcf_am_requests_success_total{Request="UpdateNotify",}	AM Service	counter	Number of AM policy association update notification success messages received by PCF from AMF	PCF receives "204 No Content" response message from AMF
37	pcf_am_requests_fail_total{Request="UpdateNotify",}	AM Service	counter	Number of AM policy association update notification fail messages received by PCF from AMF	
38	pcf_am_requests_total{Request="Delete",}	AM Service	counter	Number of AM policy association delete request messages received by PCF from AMF	PCF receives delete message for resource URL of policies/{polAssoId} from AMF
39	pcf_am_requests_success_total{Request="Delete",}	AM Service	counter	Number of AM policy association delete success response messages sent by PCF	PCF sends "204 No Content" response message

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
40	pcf_am_requests_fail_total{Request="Delete",}	AM Service	counter	Number of AM policy association delete fail response messages sent by PCF	
41	pcf_am_requests_total{Request="UpdateTerminate",}	AM Service	counter	Number of AM policy association termination create request messages received by PCF	
42	pcf_am_requests_success_total{Request="UpdateTerminate",}	AM Service	counter	Number of AM policy association termination success response messages sent by PCF	
43	pcf_am_requests_fail_total{Request="UpdateTerminate",}	AM Service	counter	Number of AM policy association termination fail response messages sent by PCF	
44	pcf_am_requests_time_seconds{Request="Create"}	AM Service	GAUGE	Max time recorded to create AM Policy Association	
45	pcf_am_requests_time_seconds_sum{Request="EvaluatePolicy",}	AM Service	GAUGE	Max time recorded to evaluate AM Policy Association	
46	pcf_am_requests_time_seconds{Request="GetUser"}	AM Service	GAUGE	Max time recorded to get AM Policy Association	
47	pcf_userservice_outbound_count_total{RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="DELETE"}	UDR Service	counter	Number of Request message for Policy Data removal (Data repository Notify Req) from PCF to UDR	Policy Term Initiated by PCF
48	pcf_userservice_outbound_count_total{DataSourceType="UDR",QueryType="REQUEST",RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="SUBSCRIBE",}	UDR Service	counter	Number of Request message for "PolicyDataSubscriptions" from PCF to UDR	The PCF may request notifications from the UDR on changes in the subscription information, and in this case,
49	pcf_userservice_outbound_count_total{DataSourceType="UDR",QueryType="SUCCESS",RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="SUBSCRIBE",}	UDR Service	counter	Number of Response message for "PolicyDataSubscriptions" from UDR to PCF	The UDR sends an HTTP "201 Created" response to acknowledge the subscription from the PCF.

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
50	pcf_userservice_outbound_count_total{DataSourceType="CHF",QueryType="REQUEST",RequestMapping="/nchf-spendinglimitcontrol/v1/subscriptions",RequestMethod="UNSUBSCRIBE",}	UDR Service	counter	Number of Request message for "PolicyDataUnSubscribe" from PCF to UDR	UEPolicy Termination response received from AMF to PCF.
51	pcf_userservice_outbound_count_total{DataSourceType="UDR",QueryType="SUCCESS",RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="UNSUBSCRIBE",}	UDR Service	counter	Number of Response message for "PolicyDataUnSubscribe" from UDR to PCF	UDR sends an HTTP "204 No Content" to PCF
52	pcf_userservice_inbound_count_total{RequestMapping="/udr-service",RequestMethod="NOTIFY"}	UDR Service			
53	pcf_userservice_inbound_count_total{RequestMapping="/udr-service",RequestMethod="GET"}	UDR Service			
54	pcf_userservice_inbound_count_total{RequestMapping="/udr-service",RequestMethod="DELETE"}	UDR Service			
55	pcf_userservice_inbound_count_total{RequestMapping="/udr-service",RequestMethod="PUT"}	UDR Service			
56	pcf_userservice_inbound_count_total{RequestMapping="/udr-service",RequestMethod="PATCH"}	UDR Service			
57	pcf_userservice_inbound_count_total{RequestMapping="/udr-service",RequestMethod="POST"}	UDR Service			
58	pcf_userservice_outbound_count_total{RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="GET"}	UDR Service	counter	Number of GET requests sent to UDR from PCF	

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
59	pcf_userservice_outbound_count_total{RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="POST"}	UDR Service	counter	Number of POST requests sent to UDR from PCF	
60	pcf_userservice_outbound_count_total{RequestMapping="/nudr-dr/v1/policy-data",RequestMethod="PATCH"}	UDR Service	counter	Number of PATCH requests sent to UDR from PCF	
61	pcf_userservice_outbound_count_total{DataSourceType="CHF",QueryType="REQUEST",RequestMapping="/nchf-spendinglimitcontrol/v1/subscriptions",RequestMethod="SUBSCRIBE"}	CHF Service	counter	Number of Request message for "Spending Limit Retrieval Subscriptions" from PCF to CHF	Initial Spending Limit Report Request Received
62	pcf_userservice_outbound_count_total{DataSourceType="CHF",QueryType="SUCCESS",RequestMapping="/nchf-spendinglimitcontrol/v1/subscriptions",RequestMethod="SUBSCRIBE"}	CHF Service	counter	Number of Response message for "Spending Limit Retrieval Subscriptions" from CHF to PCF	
63	pcf_userservice_outbound_count_total{DataSourceType="CHF",QueryType="REQUEST",RequestMapping="/nchf-spendinglimitcontrol/v1/subscriptions",RequestMethod="UNSUBSCRIBE",}	CHF Service	counter	Number of Request message for "Spending Limit Retrieval UnSubscribe" from PCF to CHF	Final Spending Limit Report Request Received
64	pcf_userservice_outbound_count_total{DataSourceType="CHF",QueryType="SUCCESS",RequestMapping="/nchf-spendinglimitcontrol/v1/subscriptions",RequestMethod="UNSUBSCRIBE"}	CHF Service	counter	Number of Response message for "Spending Limit Retrieval UnSubscribe" from CHF to PCF	
65	pa_requests_total_total{Request="Create"}	PA Service	counter	Number of Request message to create Nnpcf policy authorization from network function(NEF or AF) to PCF	

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
66	pa_success_total{Request="Create"}	PA Service	counter	Number of Response message to create Nnpcf policy authorization from PCF to network function	
67	pa_requests_total{Request="Modify"}	PA Service	counter	Number of Request message to update Nnpcf policy authorization from network function to PCF	
68	pa_success_total{Request="Modify"}	PA Service	counter	Number of Response message to update Nnpcf policy authorization from PCF to network function	
69	pa_requests_total{Request="Delete"}	PA Service	counter	Number of Request message to delete Nnpcf policy authorization from network function to PCF	
70	pa_success_total{Request="Delete"}	PA Service	counter	Number of Response message to delete Nnpcf policy authorization from PCF to network function	
71	audit_notifications_sent	SM Service	counter	Number of notifications send by Sm Service to SMF to check whether the session is stale or not.	
72	audit_update_notify_response_4xxcnt	SM Service	counter	Number of 404 response sent by SMF for the records which are identified as stale by Audit Service.	
73	audit_update_notify_response_2xxcnt	SM Service	counter	Number of 204 response sent by SMF for the records which are identified as stale by Audit Service.	

Table 7-1 (Cont.) Supported Metrics in PCF

Sr No	Prometheus Metric Name	Measurement Group	Measurement Type	Description	Peg Condition
74	audit_update_timestamp_cnt	SM Service	counter	Number of records whose LASTACESSTIME column is updated by SM Service when it receives 204 response from SMF	
75	audit_delete_records_count	SM Service	counter	Number of records deleted by SM Service when it receives 404 response from SMF	
76	audit_recs_visited	Audit Service	counter	Number of records visited	
77	audit_recs_stale	Audit Service	counter	Number of records detected as stale	
78	audit_recs_notif	Audit Service	counter	Number of stale record notifications sent, applicable for modes: NOTIFY and DELETE_NOTIFY	
79	audit_recs_remv	Audit Service	counter	Number of stale records deleted, applicable for modes: DELETE and DELETE_NOTIFY	
80	audit_recs_remv_ex	Audit Service	counter	Number of exceptions hit during attempt to delete a stale record	
81	audit_recs_notif_ex	Audit Service	counter	Number of exceptions hit during attempt to delete a stale record	
82	audit_recs_notif_er	Audit Service	counter	Number of exceptions hit during attempt to delete a stale record	

Part I

Using Policy Control Function Console

Part I describes how to configure different services in Oracle Communications Policy Control Function (PCF) and how to create policies and manageable objects in PCF.

8

Configuring Policy Control Function

This chapter describes how to configure different services in Oracle Communications Policy Control Function (PCF) and how to create policies and manageable objects to which policies can refer.

Global Configurations

You can manage and view the Global Configurations from this page.

To edit the Global Configurations:

1. From the navigation menu, under **PCF**, click **Global Configurations**.
   The Global Configurations screen appears.
2. Click **Edit** to edit the global configurations.
3. Enter the following information:
   - **Enable Tracing**- Specifies whether to enable tracing. The default value is true.
   - **Enable Metrics**- Specifies whether to enable system metrics. The default value is true.
   - **API Gateway Host**- The name of the API gateway host.
   - **API Gateway Port**- The port number of the API gateway. (if a port other than the default is being used) The default value is 80.
   - **Enable TLS**- Specifies whether to enable TLS. The default value is false.
4. Click **Save**.

Diameter Configurations

You can manage and view the Diameter Configurations from this page.

Settings

To edit the Settings:

1. From the navigation menu, under **PCF**, and then under **Diameter Configurations**, click **Settings**.
   The Settings screen appears.
2. Click **Edit** to edit the settings.
3. Enter the following information:
   - **Reconnect Delay (sec)**- Enter the time frame to delay before attempting to reconnect after a connection failure in seconds. The default is 3 seconds.
   - **Response Timeout (sec)**- Enter the response timeout interval in seconds. The default is 5 seconds.

- **Connection Timeout (sec)**- Enter the connection timeout interval in seconds. The default is 3 seconds.
- **WatchDog Interval (sec)**- Enter the watchdog interval in seconds. The default is 6 seconds.

4. Click **Save**.

Peer Nodes

To edit the Peer Node Configurations:

1. From the navigation menu, under **PCF**, and then under **Diameter Configurations**, click **Peer Node**.
   The Peer Node Configurations screen appears.
2. Click **Add** to create peer node.
   The Create Peer Node screen appears.
3. Enter the following information:
   - **Name**- Unique Name of the peer node.
   - **Type**- Defines which type of diameter service it should take up. The value can be Application function (af) or diameter routing agent(dra).
   - **Initiate Connection**- Set it to True to initiate a connection for this peer node.
   - **Port**- Enter the port number. Enter a number from 0 to 65535.
   - **Host**- Enter the host name. Enter a FQDN, ipv4 or ipv6 address available for establishing diameter transport connections to the peer node .
   - **Realm**- Enter the realm name, that is, FQDNs to all of that computers that transact diameter traffic.
   - **Identity**- Enter a identity to define a node in a realm.
4. Click **Save**.

> **Note:**
>
> You can import and export the Peer Node configurations by clicking on the **Import** and **Export** on the Peer Node Configurations screen.

Service Configurations

You can tailor the PCF services as per network operator's requirements using the Service configuration pages. The configurations include setting up end point addresses, setting up log levels and other debug information like tracing etc. and customizing and/or optimizing NF interactions for example with UDR etc.

Note:

- The **NAS Message Maximum Packet Size** field is not supported in this release of PCF and will not take effect.
- The **Validate User** and **Query User** fields must always be set to **false** in this release of PCF.

Configuring Session Management Service

You can configure the session management service from this page.

To configure the Session Management Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **Session Management Service**.
   The Session Management Service screen appears.
2. Click **Edit** to edit the session management service configurations.
3. Check the default configuration for the fields available in respective groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Field Name	**Description**
System	
Log Level	Indicates the log level of PCF Session Management (SM) service. **Default Value**: WARN **Allowed Values**: DEBUG, INFO, WARN, ERROR
Component Tracing	Determines if component tracing is enabled. Component tracing is used to evaluate system process latency in detail level. **Default Value**: FALSE
FQDN	This is the PCF FQDN used by the PCF to register Binding data to BSF. AF may use this FQDN to communicate with PCF on N5 reference point. **Default Value**: pcfsmservice.pcf
Diameter Realm	This is the PCF diameter realm used by the PCF to register Binding data to BSF. Diameter based AF may use this diameter realm to communicate with PCF on Rx reference point. **Default Value**: pcf-smservice.svc
Diameter Identity	This is the PCF diameter identity used by the PCF to register Binding data to BSF. Diameter based AF may use this diameter identity to communicate with PCF on Rx reference point. **Default Value**: pcf-smservice

Field Name	Description
Snssai	This is the PCF SNSSAI used by the PCF to register Binding data to BSF. AF/BSF may use this SNSSAI to discover proper PCF. **Default Value**: 0,000000
Enable Metrics	This determines if system metrics is enabled. This will take priority on global metrics configuration. **Default Value**: True
Override Supported Features	**Default Value**: PRA
User	
Validate User	Determines if user validate is enabled. HTTP 400 with cause **USER_UNKNOWN** returns, if this is enabled and user not found in UDR. **Default Value**: FALSE
Query User	Determines if user query from UDR is enabled. **Default Value**: TRUE
Query User On Update	Determines if user query from UDR on update is enabled. **Default Value** : FALSE
Query User On Delete	Determines if user query from UDR on delete is enabled. **Default Value** : FALSE
Query User On Reauth	Determines if user query from UDR on reauth is enabled. **Default Value** : FALSE
Subscribe to Notify	Determines if subscribe to nofity about subscriber data change is enabled. **Default Value**: TRUE
Ignore Subs Notification Check	**Default Value**: FALSE
Enable CHF Query All	**Default Value**: FALSE
Policy	
Evaluate	This determines if policy evaluate is enabled. **Default Value**: TRUE
Policy Control Request Trigger	
Default Policy Control Request Triggers	**Values**: PLMN_CH, UE_IP_CH, DEF_QOS_CH, and AC_TY_CH
Binding Configuration	
Binding Operation	This determines if binding operation (register and deregister) to the BSF is enabled. **Default Value**: TRUE
Binding Use Local Configured Bsf Always	Whether to use local configured BSF without Always discovering. **Default Value**: FALSE
Binding Use Local Configured Bsf When Not Discovered	Whether to use local configured (if having) BSF when not discovered or discover failed. **Default Value**: TRUE

Field Name	Description
Use HTTP2	Determines if using http/2 to communicate with BSF. Otherwise use http/1.1. **Default Value** : TRUE
QOS	
Qos Data Id Prefix	This is the prefix of qos data id used by PCF to generate qos data id. For example, prefix is "qosdata_", the generated qos data id is qosdata_0, chgdata_1, etc. **Default Value** : qosdata_
update Default Pcf Rule With Auth Def Qos	This determines whether to update Qos of default PccRule with the authDefQos of session rule. **Default Value** : TRUE
Install Default Qos If Not Requested	This determines whether to install default Qos to the PDU session if UE not requested. **Default Value** : TRUE
Default Qos 5qi	This is the 5Qi of default Qos which will be applied if no default Qos is requested by UE. **Default Value**: 9
Default Qos Arp Preempt Cap	This is the ARP PreemptionCapabi lity of default Qos which will be applied if no default Qos is requested by UE. **Default Value** : MAY_PREEMPT
Default Qos Arp Preempt Vuln	This is the ARP PreemptionVulner ability of default Qos which will be applied if no default Qos is requested by UE. **Default Value** : NOT_PREEMPTABLE
Default Qos Arp Priority Level	This is the ARP Priority Level of default Qos which will be applied if no default Qos is requested by UE. **Default Value**: 1
Rule	
Install Default Pcc Rule	**Default Value** : IF_NO_RULE
Rule Id Prefix	**Default Value** : 0_
Default Pcc Rule 5qi	This is the 5Qi of default pcc rule. **Default Value**: 9
Default Pcc Rule Precedence	This is the precedence of default pcc rule. **Default Value** : 3000
Default Pcc Rule Arp Preempt Cap	This is the ARP PreemptionCapabili ty of qos of default PCC rule. **Default Value** : NOT_PREEMPT
Default Pcc Rule Arp Preempt Vuln	This is the ARP PreemptionVulnerability of qos of default pcc rule. **Default Value** : PREEMPTABLE

Field Name	Description
App Rule Precedence Min	This value defines the minimum value for precedence of a PCC rule as authorized by the establishment of an application flow by the AF. If multiple rules are applied to the same packet flow or UE resource (i.e., overlapping rules) a rule with lower precedence value takes the priority over a rule with higher precedence value. The value of -1 is used to not set the precedence of a rule (NOT RECOMMENDED). **Default Value**: 400
App Rule Precedence Max	This value defines the maximum value for precedence of a PCC rule as authorized by the establishment of an application flow by the AF. If multiple rules are applied to the same packet flow or UE resource (i.e., overlapping rules) a rule with lower precedence value takes the priority over a rule with higher precedence value. The value of -1 is used to not set the precedence of a rule (NOT RECOMMENDED). **Default Value**: 899
Default Pcc Rule Arp Priority Level	This is the ARP Priority Level of qos of default pcc rule The range is 1 to 15. Values are ordered in decreasing order of priority, for example, with 1 as the highest priority and 15 as the lowest priority. **Default Value** : 15
Switch Flow In To Out Enabled	**Default Value**: FALSE
Charging	
Charging Data Id Prefix	**Default Value**: chgdata_
Primary CHF Address	Address of the primary CHF
Secondary CHF Address	Address of the secondary CHF
Online	Indicates the online charging is applicable to the PDU session.
Offline	Indicates the offline charging is applicable to the PDU session.
Traffic Control	
Traffic Control Id Prefix	**Default Value**: tcdata_
IMS Emergency Session	
Emergency DNNs	
Priority Level	Defines the relative importance of a resource request. **Default Value**: 1
Preemption Capability	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. **Default Value**: MAY_PREEMPT
Preemption Vulnerability	Defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. **Default Value**: NOT_PREEMPTABLE

4. Click **Save**.

Configuring Access and Mobility Service

You can configure the access and mobility service from this page.

To configure the Access and Mobility Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **Access and Mobility Service**.
   The Access and Mobility Service screen appears.
2. Click **Edit** to edit the access and mobility service configurations.
3. Check the default configuration for all the fields in all groups and edit as necessary
   The following table describes the input fields available under each group:

Field Name	Description
System	
Root Log Level	**Default Value**: WARN
Log Level	
Use Policy Service	**Default Value**: true
Use User Service	**Default Value**: true
Subscribe	**Default Value**: true
Enable HTTP2.0	**Default Value**: false
Validate User	Determines if user validate is enabled. HTTP 400 with cause USER_UNK NOWN returns, if this is enabled and user not found in UDR. **Default Value**: false
App	
Default Service Area Restriction	
Default Rfsp	
Default Triggers	

4. Click **Save**.

Configuring User Service

You can configure the user service from this page.

To configure the User Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **User Service**.
   The User Service screen appears.
2. Click **Edit** to edit the user service configurations.
3. In the **Server Root URL** field, enter the callback URI for notifications to be received by the User service (For example, while creating a subscription for the user with the UDR)
4. Check the default configuration for all the fields in all groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Field Name	Description
System	
Log Level	**Default Value**: WARN
Server Root URL	
Common	
Resource Get Subscribe	**Default Value**: false
Request Timeout	**Default Value**: 1000
DB	
Keys Precedence	
User Index Keys	
Indexing	
Index By Msisdn	**Default Value**: true
Index By Extid	**Default Value**: true
Index By Imsi	**Default Value**: true
Index By Nai	**Default Value**: true
UDR	
Base Uri	**Default Value**: /nudr-dr/v1
Supported Features	**Default Value**: f
AM Data Uri	**Default Value**: /policy-data/ues/{ueId}/am-data
UE Policy Set Uri	**Default Value**: /policy-data/ues/{ueId}/ue-policy-set
SM Data Uri	**Default Value**: /policy-data/ues/{ueId}/sm-data
Usage Mon Uri	**Default Value**: /policy-data/ues/{ueId}/sm-data/{usageMonId}
Subs To Notify Uri	**Default Value**: /policy-data/subs-to-notify
Subs To Notify Subs Id Uri	**Default Value**: /policy-data/subs-to-notify/{subsId}
Request Timeout	**Default Value**: 1000
Explode Snssai	**Default Value**: false
Enable HTTP1.1	**Default Value**: false
Enable Discovery On Demand	**Default Value**: true

5. Click **Save**.

Configuring Policy Authorization Service

You can configure the policy authorization service from this page.

To configure the Policy Authorization Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **Policy Authorization Service**.
   The Policy Authorization Service screen appears.
2. Click **Edit** to edit the policy authorization service configurations.
3. Check the default configuration for all the fields in all groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Field Name	Description
System	
Af Direct Reply	**Default Value**: true
Override Supported Features	
AF Terminate Uri Segment	**Default Value**: termination
AF Subscriber Notify Segment	**Default Value**: termination
IMS Emergency Session	
Emergency Service URNs	
Reservation Priority Types	**Default Value**: PRIO_6

4. Click **Save**.

Configuring UE Policy Service

You can configure the UE policy service from this page.

To configure the UE Policy Service:

1. From the navigation menu, under **PCF**, then under **Service Configurations**, click **UE Policy Service**.
   The UE Policy Service screen appears.
2. Click **Edit** to edit the UE policy service configurations.
3. In the **Notification URI Root** field, enter the callback URI for notifications to be received by the UE Policy service (For example, while creating a subscription for the NAS Message Transfer with the AMF)
4. Check the default configuration for all the fields in all groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Field Name	Description
System	
Log Level	**Default Value**: WARN
Notification URI Root	
AMF	
Enable HTTP/1.1	**Default Value**: false
NAS Message Maximum Packet Size (bytes)	enter a range in [0-65535] number
User	
Validate User	**Default Value**: false
Query User	**Default Value**: false

5. Click **Save**.

Policy Configurations

This chapter describes how to create manageable objects in Policy Control Function (PCF).

Common

You can configure the common services from this page. To configure the common service, navigate to **PCF**, then under **Policy Configurations**, click **Common**.

The Common configuration includes Managing Presence Reporting Area.

Managing Presence Reporting Area

You can manage, view, import, export and create the Presence Reporting Area from Pra Management screen.

> **Note:**
>
> Only administrators can create presence reporting area.

To configure the service:

1. From the navigation menu, under **Policy Configurations**, then under **Common**, click **Presence Reporting Area**.
   The **Pra Management** screen appears with the listing of all the available reports. You can create or import new reports from this page.

   > **Note:**
   >
   > Click Export to download the available reports to your system.

2. Click **Add**.
   The **Create Pra** screen appears.
3. On the **Create Pra** screen, enter values for the input fields common to all the groups available on the screen. .
   The following table describes the fields:

Field Name	Description
Name	The unique name assigned to the PRA.
Pra Id	The unique identifying number of the PRA list. The ID must be numeric value between 0 and 16777125. This field is present if the Area of Interest subscribed or reported is a Presence Reporting Area.

Field Name	Description
Presence State	Indicates whether the UE is inside or outside of the area of interest (e.g presence reporting area or the LADN area), or if the presence reporting area is inactive in the serving node. Select any one of the following values: • IN_AREA : Indicates that the UE is inside or enters the presence reporting area. • OUT_OF_AREA : Indicates that the UE is outside or leaves the presence reporting area. • UNKNOWN : Indicates it is unknown whether the UE is in the presence reporting area or not. • INACTIVE : Indicates that the presence reporting area is inactive in the serving node.

4. Expand the **Tracking Area List** group.
   The expanded window displays the available tracking area lists. To create new lists:

   a. Click **Add**.
      The **Add Tracking Area List** window appears on the screen.

   b. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Mnc	Defines the Mobile Network Code. Two to three digit number.
Mcc	Defines the Mobile Country Code. Three digit number.
Tac	28-bit string identifying an E-UTRA Cell Id as specified, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the Cell Id shall appear first in the string, and the character representing the 4 least significant bit of the Cell Id shall appear last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRA Cell Id 0x5BD6007 shall be encoded as "5BD6007".

> **Note:**
>
> Click **Cancel** to cancel the changes.

   c. Click **Save**.
      The value gets listed in the **Tracking Area List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

5. Expand the **Ecgi List** group.
   The expanded window displays the available Eutra Cell Ids. To create new Ids:

   a. Click **Add**.
   The **Add Ecgi List** window appears on the screen.

   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Mnc	Defines the Mobile Network Code of the PLMN. Two to three digit number.
Mcc	Defines the Mobile Country Code of the PLMN. Three digit number.
Eutra Cell Id	28-bit string identifying an E-UTRA Cell Id as specified in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the Cell Id shall appear first in the string, and the character representing the 4 least significant bit of the Cell Id shall appear last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRA Cell Id 0x5BD6007 shall be encoded as "5BD6007".

> **Note:**
>
> Click **Cancel** to cancel the changes.

   c. Click **Save**.
   The value gets listed in the **Ecgi List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

6. Expand the **Ncgi List** group.
   The expanded window displays the available Nr Cell Ids. To create new Ids:

   a. Click **Add**.
   The **Add Ncgi List** window appears on the screen.

   b. Enter the applicable values in the input fields available on the window.

The following table describes the fields:

Field Name	Description
Mnc	Defines the Mobile Network Code of the PLMN. Two to three digit number.
Mcc	Defines the Mobile Country Code of the PLMN. Three digit number.
Nr Cell Id	36-bit string identifying an NR Cell Id as specified in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the Cell Id shall appear first in the string, and the character representing the 4 least significant bit of the Cell Id shall appear last in the string. Pattern: '^[A-Fa-f0-9]{9}$' Example: An NR Cell Id 0x225BD6007 shall be encoded as "225BD6007".

> **Note:**
>
> Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed in the **Ncgi List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

7. Expand the **Global Ran NodeId List** group.
The expanded window displays the available **N3 lwf Ids**. To create new Ids:

a. Click **Add** displayed in the window.
The **Add Global Ran NodeId List** window appears on the screen.

b. Enter the applicable values in the input fields available on the window.
The following table describes the fields:

Field Name	Description
Plmn Id	
Mnc	Defines the Mobile Network Code of the PLMN. Two to three digit number.
Mcc	Defines the Mobile Country Code of the PLMN. Three digit number.

Field Name	Description
N3 lwf Id	This field is included if the RAN node belongs to non 3GPP access (i.e a N3IWF). If included, this field contains the FQDN of the N3IWF.
gNb Id	
Bit Length	Unsigned integer representing the bit length of the gNB ID within the range 22 to 32
gNb Value	This represents the identifier of the gNB. The string shall be formatted with following pattern: '^[A-Fa-f0-9]{6,8}$' The value of the gNB ID shall be encoded in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the gNB ID shall appear first in the string, and the character representing the 4 least significant bit of the gNB ID shall appear last in the string. Examples: "382A3F47" indicates a gNB ID with value 0x382A3F47
Nge Nb Id	This field is included if the RAN Node Id represents a NG-eNB. When present, this field contains the identifier of an NG-eNB.

> **Note:**
>
> Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed under **Global Ran NodeId List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

8. Click **Save**.
The Pra details are listed on the **Presence Reporting Area** screen.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

Importing the Presence Reports

To import the reports:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload** button.

SM Policy

You can configure the SM Policy from this page. To configure the SM Policy, navigate to **PCF**, then under **Policy Configurations**, click **SM Policy**.

The SM Policy configurations includes:

- Managing Session Rule
- Managing Session Rule Profile
- Managing Qos Information
- Managing PCC Rule
- Managing PCC Rule Profile
- Managing Qos Data
- Managing Charging Data
- Managing Usage Monitoring Data
- Managing Traffic Control Data
- Managing Condition Data
- Managing Policy Counter Id

Managing Session Rule

You can create and manage session rules from the Session Rule Management screen. The page provides information about the existing session rules. You can create or refresh the session rules from this page.

> **Note:**
>
> Only administrators can create session rules.

To configure the session rules from this page:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Session Rule**.
   The **Session Rule Management** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

> **Note:**
>
> Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Session Rule** screen appears.
3. On the **Create Session Rule** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
ID	Specifies the Session Rule ID.
NAME	Specifies the name assigned to the session rule.
Description	Free-form text that identifies the session rule.

4. Expand the **Authorized Session AMBR** group to add the AMBR details:
   a. Click **Add** displayed in the window.
   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Uplink Bandwidth	Specifies the bandwidth in uplink.
Downlink Bandwidth	Specifies the bandwidth in downlink.

> **Note:**
>
> Click **Remove** to cancel the changes.

5. Select value for **Authorize Default Qos** from the drop down menu.

> **Note:**
>
> The drop down gets its data from the QoS Information created.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

6. Click **Save**.
   The value gets listed on the **Session Rule Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Session Rules

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Managing Session Rule Profile

You can manage and configure the session rule profiles from this page.

To configure the profile:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Session Rule Profile**.
   The **Session Rule Profile Management** screen appears with the listing of all the available rules. You can create or import new profiles from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Session Rule Profile** screen appears.
3. On the **Create Session Rule Profile** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
ID	Specifies the Session Rule Profile ID.
NAME	Specifies the name assigned to the session rule profile.
Description	Free-form text that identifies the session rule profile.

4. Expand the **Authorized Session AMBR** group to add the AMBR details:
   a. Click **Add** displayed in the window.
   b. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Uplink Bandwidth	Specifies the bandwidth in uplink.
Downlink Bandwidth	Specifies the bandwidth in downlink.

> **Note:**
>
> Click **Remove** to cancel the changes.

5. Select value for **Authorize Default Qos** from the drop down menu.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

6. Click **Save**.
The value gets listed on the **Session Rule Profile Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Session Rule Profiles

To import the session rule profiles:

1. Click **Import**.
The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload** button.

Managing Qos Information

You can manage, view, import, export and create the QoS Information from QoS Information Management screen.

> **Note:**
>
> Only administrators can create QoS Information data.

To configure the QoS Information data:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Qos Information**.
The **Authorized Default Qos Management** screen appears with the listing of all the available rules. You can create or import the Qos details from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.
The **Create Authorized Default Qos** screen appears.

3. On the **Create Authorized Default Qos** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	Specifies the name assigned to the QOS information.
Description	Free-form text that identifies the QOS information.
Default 5G QoS Identifier	Identifier for the authorized QoS parameters for the service data flow. It shall be included when the QoS information decision is initially provisioned.
Priority Level	Unsigned integer indicating the 5QI Priority Level, within a range of 1 to 127.
Average Window	Represents the duration over which the guaranteed and maximum bitrate shall be calculated (NOTE).
Max DataBurstVol	Denotes the largest amount of data that is required to be transferred within a period of 5GAN PDB (NOTE).

4. Expand the **arp** group to add the arp details:

   a. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Priority Level	Unsigned integer indicating the ARP Priority Level, within the range 1 to 15.
Preemption Capability	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. Possible values are: • NOT_PREEMPT : Shall not trigger pre-emption. • MAY_PREEMPT : May trigger pre-emption.
Preemption Vulnerability	Defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. Possible values are: • NOT_PREEMPTABLE : Shall not be pre-empted. • PREEMPTABLE : May be pre-empted.

> **Note:**
>
> Click the **Remove** button to cancel the changes.

   b. Click the **ADD** button to add the changes.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

5. Click **Save**.
   The value gets listed on the **Authorized Default Qos Management** screen.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Qos Information

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload** button.

Managing PCC Rule

You can create and manage PCC Rule from the PCC Rule Management screen. The page provides information about the existing rules. You can create or refresh the PCC rules from this page.

> **Note:**
>
> Only administrators can create PCC rules.

To configure the rule:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **PCC Rule**.
   The **PCC Rule Management** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create PCC Rule** screen appears.
3. On the **Create PCC Rule** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
PCC Rule Id	Specifies the PCC Rule ID.
Name	Specifies the name assigned to the PCC rule.
Description	Free-form text that identifies the PCC rule.
Type	Select the required type. Possible Values are: • Predefined PCC Rule • Dynamic PCC Rule If you have selected Dynamic PCC Rule, then go to Step 4 else, go to Step 5.

4. Expand the **Flow Infos** group to add the Flow information:

   a. Click the **Add** icon displayed in the window.
   The **Add Flow Infos** appears.

   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Name	Indicates the name for the flow.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Pack Filt Id	An identifier of packet filter.
Packet Filter Usage	The packet shall be sent to the UE. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.
Tos Traffic Class	Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class field and mask field.
Spi	The security parameter index of the IPSec packet.
Flow Label	The Ipv6 flow label header field.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Ethernet Flow Description	
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.

Field Name	Description
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

c. Click **Add** under the **Ethernet Flow Description** group name to expand the group. The screen displays the available input fields. Enter the applicable values in the input fields.

The following table describes the fields:

Field Name	Description
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F

Field Name	Description
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

> **Note:**
>
> Click **Remove** to cancel the changes.

d. Click **Save** on the **Add Flow Infos** window, under the **Flow Infos** group.
The value gets listed on the **Create PCC Rule** screen

e. Under the **Flow Infos** group, enter values for the rest of the input fields:

Field Name	Description
App Id	A reference to the application detection filter configured at the UPF.
Content Version	Indicates the content version of the PCC rule.
Precedence	Determines the order in which this PCC rule is applied relative to other PCC rules within the same PDU session. It shall be included if the "flowInfos" attribute is included or may be included if the "appId" attribute is included when the PCF initially provisions the PCC rule.
AF Signalling Protocol	Indicates the protocol used for signalling between the UE and the AF. The default value "NO_INFORMATION" shall apply, if the attribute is not present and has not been supplied previously.
Application Relocation	Indication of application relocation possibility. The default value "NO_INFORMATION" shall apply, if the attribute is not present and has not been supplied previously.
Qos Data	A reference to the QoSData policy type decision type.
Traffic Control Data	A reference to the TrafficControlData policy decision type.
Charging Data	A reference to the ChargingData policy decision type.
Usage Monitoring Data	A reference to UsageMonitoringData policy decision type.
Condition Data	A reference to the condition data.

5. Click **Save**.
The value gets listed on the **PCC Rule Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the PCC Rules

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Managing PCC Rule Profile

You can create and manage PCC Rule Profile from the PCC Rule Profile Management screen. The page provides information about the existing profiles. You can create or refresh the profiles from this page.

> **Note:**
>
> Only administrators can create PCC Rule Profile.

To configure the PCC Rule Profile:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **PCC Rule Profile**.
   The **PCC Rule Profile Management** screen appears with the listing of all the available rules. You can create or import new profile details from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create PCC Rule Profile** screen appears.
3. On the **Create PCC Rule Profile** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
ID	Specifies the PCC Rule Profile ID.
Name	Specifies the name assigned to the PCC rule profile.
Description	Free-form text that identifies the PCC rule profile.

Field Name	Description
Type	Select the required type. Possible Values are: - Predefined PCC Rule - Dynamic PCC Rule If you have selected Dynamic PCC Rule, then go to Step 4 else, go to Step 5.

4. Expand the **Flow Infos** group to add the Flow information:

   a. Click the **Add** icon displayed in the window.
   The **Add Flow Infos** appears.

   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Name	Indicates the name for the flow.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Pack Filt Id	An identifier of packet filter.
Packet Filter Usage	The packet shall be sent to the UE. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.
Tos Traffic Class	Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class field and mask field.
Spi	The security parameter index of the IPSec packet.
Flow Label	The Ipv6 flow label header field.
Flow Direction	Indicates the flow direction. Select from the following options: - DOWNLINK - UPLINK - BIDIRECTIONAL - UNSPECIFIED
Ethernet Flow Description	
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.

Field Name	Description
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

c. Click **Add** under the **Ethernet Flow Description** group name to expand the group. The screen displays the available input fields. Enter the applicable values in the input fields.

The following table describes the fields:

Field Name	Description
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F

Field Name	Description
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

Note:

Click **Remove** to cancel the changes.

d. Click **Save** on the **Add Flow Infos** window, under the **Flow Infos** group.
The value gets listed on the **Create PCC Rule** screen

e. Under the **Flow Infos** group, enter values for the rest of the input fields:

Field Name	Description
App Id	A reference to the application detection filter configured at the UPF.
Content Version	Indicates the content version of the PCC rule.
Precedence	Determines the order in which this PCC rule is applied relative to other PCC rules within the same PDU session. It shall be included if the "flowInfos" attribute is included or may be included if the "appId" attribute is included when the PCF initially provisions the PCC rule.
AF Signalling Protocol	Indicates the protocol used for signalling between the UE and the AF. The default value "NO_INFORMATION" shall apply, if the attribute is not present and has not been supplied previously.
Application Relocation	Indication of application relocation possibility. The default value "NO_INFORMATION" shall apply, if the attribute is not present and has not been supplied previously.
Qos Data	A reference to the QoSData policy type decision type.
Traffic Control Data	A reference to the TrafficControlData policy decision type.
Charging Data:	A reference to the ChargingData policy decision type.
Usage Monitoring Data	A reference to UsageMonitoringData policy decision type.
Condition Data	A reference to the condition data.

5. Click **Save**.
   The value gets listed on the **PCC Rule Profile Management** screen.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the PCC Rule Profiles

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Managing Qos Data

You can create and manage Qos Data from the Session Rule Management screen. The page provides information about the existing Qos Data. You can create or refresh the Qos Data from this page.

> **Note:**
>
> Only administrators can create Qos Data.

To configure the Qos Data:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Qos Data**.
   The **Qos Data Management** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Qos Data** screen appears.
3. On the **Create Qos Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	Specifies the name assigned to the QOS data.
Description	Free-form text that identifies the QOS data.

Field Name	Description
Default 5G QoS Identifier	Identifier for the authorized QoS parameters for the service data flow. It shall be included when the QoS data decision is initially provisioned.
Maximum Bit Rate UL	Indicates the max bandwidth in uplink.
Maximum Bit Rate DL	Indicates the max bandwidth in downlink.
Guaranteed Bit Rate UL	Indicates the guaranteed bandwidth in uplink
Guaranteed Bit Rate DL	Indicates the guaranteed bandwidth in downlink.
QoS Notification Control	
Reflective Qos	Indicates whether the QoS information is reflective for the corresponding service data flow. Default value is "FALSE", if not present and has not been supplied previously.
Sharing Key Ul	Indicates, by containing the same value, what PCC rules may share resource in uplink direction.
Sharing Key Dl	Indicates, by containing the same value, what PCC rules may share resource in downlink direction.
Priority Level	Defines the relative importance of a resource request.
Averaging Window	Represents the duration over which the guaranteed and maximum bitrate shall be calculated (NOTE).
Maximum Data Burst Volume	Denotes the largest amount of data that is required to be transferred within a period of 5GAN PDB (NOTE).
Maximum Packet Loss Rate Dl	Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow.
Max Packet Loss Rate Ul	Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow.
Default Qos Flow Indication	Indicates that the dynamic PCC rule shall always have its binding with the QoS Flow associated with the default QoS rule. Default value is "FALSE", if not present and has not been supplied previously.

4. Expand the **arp** group to add the arp details:

   a. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Priority Level	Defines the relative importance of a resource request.
Preemption Capability	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. Possible values are: • NOT_PREEMPT • MAY_PREEMPT

Field Name	Description
Preemption Vulnerability	Defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. Possible values are: • NOT_PREEMPTABLE • PREEMPTABLE

> **Note:**
>
> Click the **Remove** button to cancel the changes.

b. Click the **ADD** button to add the changes.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

5. Click **Save**.
   The value gets listed on the **Qos Data Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Qos Data

To import the Qos Data:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload** button.

Managing Charging Data

You can manage, view, import, export and create the Charging Data from Charging Data Management screen.

> **Note:**
>
> Only administrators can create Charging data.

To configure the service:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Charging Data**.

The **Charging Data Management** screen appears with the listing of all the available rules. You can create or import new data from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Create**.
   The **Create Charging Data** screen appears.
3. On the **Create Charging Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	**Description**
Name	The name of the Charging Data.
Description	The description of the Charging Data.
Metering Method	The following options are available • DURATION • VOLUME • DURATION_VOLUME • EVENT Defines what parameters shall be metered for offline charging. If the attribute is not present but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but the attribute is set to NULL, the metering method preconfigured at the SMF is applicable as default metering method.
Offline	Indicates the offline charging is applicable to the PDU session or PCC rule. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously. (NOTE)
Online	Indicates the online charging is applicable to the PDU session or PCC rule. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously. (NOTE)
Rating Group	The charging key for the PCC rule used for rating purposes.

Field Name	Description
Reporting Level	The following options are available: • SER_ID_LEVEL • RAT_GR_LEVEL • SPON_CON_LEVEL Defines on what level the SMF reports the usage for the related PCC rule. If the attribute is not present but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but it is set to NULL, the reporting level preconfigured at the SMF is applicable as default reporting level.
Service Id	Indicates the identifier of the service or service component the service data flow in a PCC rule relates to.
Sponsor Id	Indicates the sponsor identity.
App Svc Prov Id	Indicates the application service provider identity.
Af Charging Identifier	Univocally identifies the charging control policy data within a PDU session.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Charging Data Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Charging Data

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Managing Usage Monitoring Data

You can create and manage Usage Monitoring Data from the Session Rule Management screen. The page provides information about the existing Usage Monitoring Data. You can create or refresh the Usage Monitoring Data from this page.

> **Note:**
>
> Only administrators can create Usage Monitoring Data.

To configure the service:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Usage Monitoring Data**.
   The **Usage Monitoring Data Management** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Usage Monitoring Data** screen appears.
3. On the **Create Usage Monitoring Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	The name of the Usage Monitoring Data.
Description	The description of the Usage Monitoring Data.
Volume Threshold	Indicates a volume threshold.
Volume Threshold Uplink	Indicates a volume threshold in uplink.
Volume Threshold Downlink	Indicates a volume threshold in downlink.
Time Threshold	Indicates a time threshold.
Monitoring Time	Indicates the time at which the UP function is expected to reapply the next thresholds (e.g. nextVolThreshold).
Next Vol Threshold	Indicates a volume threshold after the Monitoring.
Next Vol Threshold Uplink	Indicates a volume threshold in uplink after the Monitoring Time.
Next Vol Threshold Downlink	Indicates a volume threshold in downlink after the Monitoring Time.
Next Time Threshold	Indicates a time threshold after the Monitoring.
Inactivity Time	Defines the period of time after which the time measurement shall stop, if no packets are received.
ex Usage PccRule Ids	Contains the PCC rule identifier(s) which corresponding service data flow(s) shall be excluded from PDU Session usage monitoring. It is only included in the UsageMonitoringData instance for session level usage monitoring.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Usage Monitoring Data Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Usage Monitoring Data

To import the Usage Monitoring Data:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Managing Traffic Control Data

You can manage, view, import, export and create the Traffic Control Data from Traffic Control Data Management screen.

> **Note:**
>
> Only administrators can create traffic control data.

To configure the traffic control data:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Traffic Control Data**.
   The **Traffic Control Data Management** screen appears with the listing of all the available rules. You can create or import new data from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Traffic Control Data** screen appears.
3. On the **Create Traffic Control Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	The name of the Traffic Control policy data.
Description	The description of the Traffic Control policy data.
Flow Status	The following options are available: • ENABLED-UPLINK • ENABLED-DOWNLINK • ENABLED • DISABLED • REMOVED Enum determining what action to perform on traffic. Possible values are: [enable, disable, enable_uplink, enable_downlink] . The default value "ENABLED" shall apply, if the attribute is not present and has not been supplied previously.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Expand the **Redirect Information** group and enter values of the available input fields.
   The following table describes the fields:

Field Name	Description
Redirect Enabled	Indicates the redirect is enabled.
Redirect Address Type	This string provides forward-compatibility with future extensions to the enumeration but is not used to encode content defined in the present version of this API.
Redirect Server Address	Indicates the address of the redirect server.
Mute Notification	Indicates whether application's start or stop notification is to be muted. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.
Traffic Steering Pol Id Dl	Reference to a preconfigured traffic steering policy for downlink traffic at the SMF.
Traffic Steering Pol Id Ul	Reference to a preconfigured traffic steering policy for uplink traffic at the SMF.

5. Expand the **Route To Locs** group.
   The expanded window displays the available routes. To create new routes:

   a. Click **Add** in the window.
      The **Add Route To Locs** window appears on the screen.

   b. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Dnai	Identifies the location of the application.

Field Name	Description
Ipv4 Addr	Ipv4 address of the tunnel end point in the data network.
Ipv6 Addr	Ipv6 address of the tunnel end point in the data network.
Port Number	UDP port number of the tunnel end point in the data network.
Route Profile Id	Identifies the routing profile Id.

> **Note:**
>
> Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed in the **Tracking Area List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

6. Expand the **Up Path Chg Event** group and enter values of the available input fields.
The following table describes the fields:

Field Name	Description
Notification Uri	Defines the notification Uri sent by the SMF.
Notification Correlation Id	It is used to set the value of Notification Correlation ID in the notification sent by the SMF.
Dnai Change Type	The following options are available: • EARLY • EARLY_LATE • LATE Possible values are EARLY: Early notification of UP path reconfiguration. - EARLY_LATE: Early and late notification of UP path reconfiguration. This value shall only be present in the subscription to the DNAI change event. LATE: Late notification of UP path reconfiguration. This string provides forwardcompatibility with future extensions to the enumeration but is not used to encode content defined in the present version of this API.

7. Click **Save**.
The value gets listed on the **Traffic Control Data Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Traffic Control Data

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Condition Data

You can create and manage Condition Datas from the Condition Data Management screen. The page provides information about the existing Condition Datas. You can create or refresh the Condition Datas from this page.

> **Note:**
>
> Only administrators can create Condition Data.

To configure the service:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Condition Data**.
   The **Condition Data Management** screen appears with the listing of all the available rules. You can create or import new data from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Condition Data** screen appears.
3. On the **Create Condition Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	The name of the Condition Data policy data.
Description	The description of the Condition Data policy data.
Activation Time	The time when the decision data shall be activated.
Deactivation Time	The time when the decision data shall be deactivated.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Condition Data Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Condition Data

To import the Condition Datas:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Policy Counter Id

You can create and manage Policy Counter Ids from the Policy Counter Id Management screen. The page provides information about the existing Policy Counter Ids. You can create or refresh the Policy Counter Ids from this page.

> **Note:**
>
> Only administrators can create Policy Counter Ids.

To configure the service:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Policy Counter Id**.
   The **Policy Counter Id Management** screen appears with the listing of all the available rules. You can create or import new data from this page.

> **Note:**
>
> Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Policy Counter Id** screen appears.
3. On the **Create Policy Counter Id** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	Policy Counter Id's Name.
Desc	Policy Counter Id's description.
Default Status	

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Policy Counter Id Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Policy Counter Id Data

To import the Policy Counter Ids:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

AM Policy

You can configure the AM Policy services from this page. To configure the AM Policy service, navigate to **PCF**, then under **Policy Configurations**, click **AM Policy**.

The AM Policy configuration includes Managing Service Area Restriction.

Service Area Restriction

You can create and manage Service Area Restrictions from the Service Area Restriction Management screen. The page provides information about the existing Service Area Restrictions. You can create or refresh the Service Area Restrictions from this page.

> **Note:**
>
> Only administrators can create Service Area Restrictions.

To configure the service:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **Service Area Restriction**.
   The **Service Area Restriction Management** screen appears with the listing of all the available rules. You can create or import new data from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Create**.
   The **Create Service Area Restriction** screen appears.
3. On the **Create Service Area Restriction** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	Specifies name of the service area restriction.
Description	Specifies description of the service area restriction.
Restriction Type	Specifies the restriction type. Possible values are: • ALLOWED_AREAS • NOT_ALLOWED_AREAS This field is present if and only if the areas attribute is present.

4. Expand the **Areas** group.
   The expanded window displays the available areas. To create new area details:
   a. Click the **Create** button displayed in the window.
      The **Create** window appears on the screen.
   b. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Tacs	Specifies Type Allocation Codes. A decimal number between 0 and 65535. This fields is present if and only if Area Codes is absent.
Area Codes	Specifies area codes. This fields is present if and only if Tacs is absent.

   c. Click on the **Save** button.
      The value gets listed in the **Tracking Area List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

5. Enter value of the **Max Number of TAs** input field.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

6. Click **Save**.
   The value gets listed on the **Service Area Restriction Management** screen.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Service Area Restrictions

To import the Service Area Restrictions:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

UE Policy

You can configure the UE Policy from this page. To configure the UE Policy, navigate to **PCF**, then under **Policy Configurations**, click **UE Policy**.

The UE Policy configurations includes:

- Managing URSP Rule
- Managing UPSI

Managing URSP Rule

You can create and manage URSP Rules from the URSP Rule Management screen. The page provides information about the existing URSP Rules. You can create or refresh the URSP Rules from this page.

> **Note:**
>
> Only administrators can create URSP Rules.

To configure the URSP Rules:

1. From the navigation menu, under **Policy Configurations**, then under **Common**, click **URSP Rule**.
   The **URSP Rule Management** screen appears with the listing of all the available reports. You can create or import new rules from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available reports to your system.

2. Click **Add**.
   The **Create URSP Rule** screen appears.

3. On the **Create URSP Rule** screen, enter values for the input fields common to all the groups available on the screen. .
   The following table describes the fields:

Field Name	Description
Name	Name of the URSP rule.
Precedence	Precedence value of the URSP rule.

4. Expand the **Traffic Descriptor** group.
   The expanded window displays the available traffic descriptor types. To create new types:

   a. Click **Add** displayed in the window.
   The **Add Traffic Descriptor** window appears on the screen.

   b. Select a value from the **Type** drop down menu. Possible values are:

   - MATCH_ALL
   - OS_ID_OS_APP_ID
   - IPV4_REMOTE_ADDRESS
   - IPV6_REMOTE_ADDRESS
   - PROTOCOL_IDENTIFIER
   - SINGLE_REMOTE_PORT
   - REMOTE_PORT_RANGE

   c. Click **Save**.
   The value gets listed under the **Traffic Descriptor** group.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

5. Expand the **Route Selection Descriptor List** group.
   The expanded window displays the available precedence. To create new data:

   a. Click **Add** displayed in the window.
   The **Add Route Selection Descriptor List** window appears on the screen.

   b. Enter the value in the **Precedence** field.

   c. Click **Add** to create a new Route Selection Descriptor Components in the **Route Selection Descriptor Components** group. .
   The Add Route Selection Descriptor Components window appears on the screen.

   d. Select a value from the **Type** drop down menu.

   e. Select a value from the **SSC Mode** drop down menu.

   f. Click **Save**.
   The value gets listed in the **Route Selection Descriptor List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

6. Click **Save**.
   The Pra details are listed on the **Presence Reporting Area** screen.

   > **Note:**
   >
   > Click **Cancel** to cancel the configuration.

Importing the URSP Rule

To import the reports:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Managing UPSI

You can manage, view, import, export and create UPSI from UPSI Management screen.

> **Note:**
>
> Only administrators can create UPSI.

To configure UPSI:

1. From the navigation menu, under **Policy Configurations**, then under **SM Policy**, click **UPSI**.
   The **UPSI Management** screen appears with the listing of all the available rules. You can create or import new profile details from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create UPSI** screen appears.
3. On the **Create UPSI** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	Name of the UPSI.

Field Name	Description
UPSC	Defines UE Policy Section Code. Enter a number between 0 and 65,535.
URSP Rules	Defines URSP rules.

4. Expand the **PLMN** group and enter values of the available input fields.
   The following table describes the fields:

Field Name	Description
MCC	Defines the Mobile Country Code. Enter a number between 0 and 999.
MNC	Defines the Mobile Network Code. Enter a number between 0 and 999.

5. Click **Save**.
   The value gets listed on the **UPSI Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the UPSI

To import the UPSIs:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload** button.

9

Session Viewer

The Session Viewer displays detailed session information for a specific subscriber. Within the session viewer, you can enter query parameters to render session data for a specific subscriber. This section provides information about viewing the sessions.

To view the sessions:

1. From the navigation menu, under **PCF**, click **Session Viewer**. The Session Viewer page appears.
2. From the **Session Type** drop-down menu, select the service whose sessions you want to view. Possible values are:
   - SM Policy Association
   - AM Policy Association
   - PA Policy Association
3. From the **Identifier Type** drop-down menu, select the identifier type for the selected session type. Possible values are:
   - SUPI
   - GPSI
   - IPV4
   - IPV6
   - POLICY_ASSOC_ID
   - MAC

   > **Note:**
   >
   > AM Policy Association and PA Policy Association fetches session data using **POLICY_ASSOC_ID** (Session ID) only.

4. Enter the value in the **Identifier Value** field for the selected identifier type.
5. Click **Query**. Information about the subscriber session(s) is displayed.

If session data is not available, the error is displayed along with No session found.

10

Managing Match Lists

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

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

Creating a Match List

To create a match list:

1. From the navigation pane, under **Common Configurations**, select **Match List**.
   The **Match List Management** page opens in the work area.
2. Click **Create**.
   The Create Match List page opens.
3. Enter the following information:
   - **ID**: The ID assigned to the match list.
   - **Name**: The name assigned to the match list.
     The name can only contain the characters A-Z, a-z, 0-9, period (.), hyphen (-), and underline (_). The maximum length is 40 characters.
   - **Description**: Free-form text
   - **Type**: Select from the following:
     - **string** (default) - The list consists of strings.
     - **wildcard string** - The list consists of wildcard match patterns that use an asterisk (*) to match zero or more characters or a question mark (?) to match exactly one character.
   - **Items**:
4. Click **Save**.

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

Modifying a Match List

To modify a match list:

1. From the navigation pane, under **Common Configurations**, select **Match List**.
   The **Match List Management** page opens in the work area, displaying the list of defined match lists.
2. Select the match list you want to modify.

3. Click **Edit**.
   The Edit Match List page opens.
4. Modify match list information as required.
5. Click **Save**.
   The match list is modified.

Deleting a Match List

To delete a match list:

1. From the navigation pane, under **Common Configurations**, select **Match List**.
   The **Match List Management** page opens in the work area, displaying the list of defined match lists.
2. Select the match list you want to delete.
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK**.
   The match list is deleted.

Importing the Match Lists

To import the match lists:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

Exporting the Match Lists

You can export the match lists by clicking **Export All**. The Match Lists will be downloaded in a local machine.

11 Managing Policy

You can create and manage Policy projects.

Policy Control Function (PCF) offers a Policy Design editor based on Blockly interface. You can create a Policy Project for each of the policy services that you wished to deploy:

- Session Management
- Policy Authorization
- Access and Mobility Management
- UE Management

Settings

You can manage and view the PCF supported services from this page.

To edit the Settings:

1. From the navigation menu, under **Policy Management**, click **Settings**.
   The Policy Runtime Environment screen appears.
2. Click **Edit** to edit the settings.
3. Enter the value in **Log Level** field. The default value is WARN.
4. Click **Add** in the **Supported Services** group.
   The Add Supported Services screen appears.
5. Enter the following information to create service:
   - **Service Name**: Enter the service name.
   - **Service Label**: Enter the service label.
   - **Relative URL**: Enter the relative URL.
6. Click **Save**. The services get listed in the Supported Services list.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the services.

Creating a Policy Project

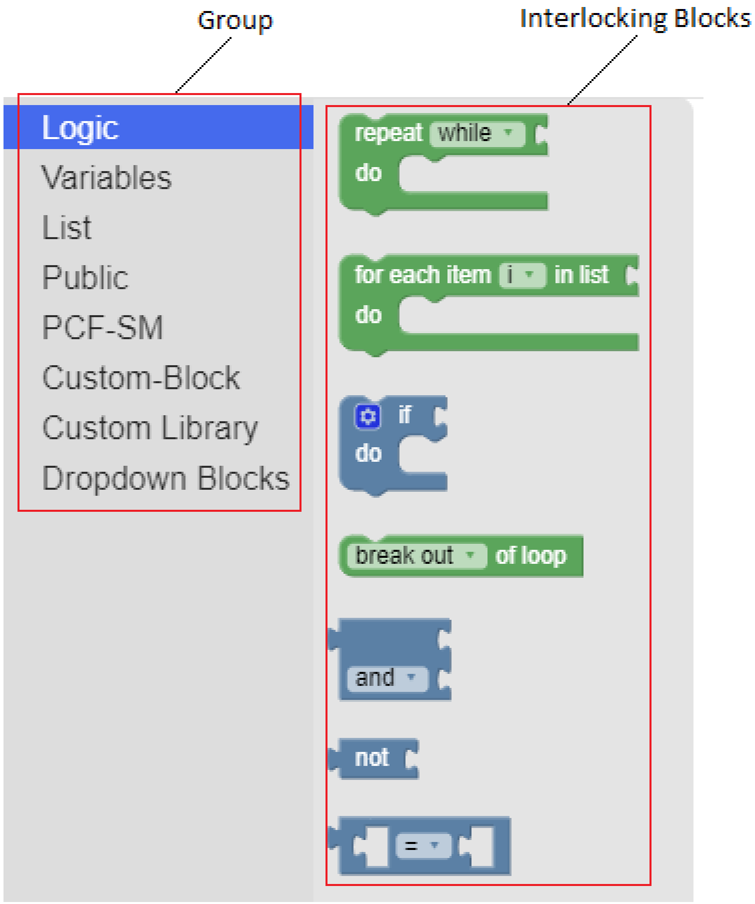
To create a policy project:

1. From the **Policy Management** section of the navigation pane, select **Policy Projects**.
2. Click **Create**.

The Create Project window opens.

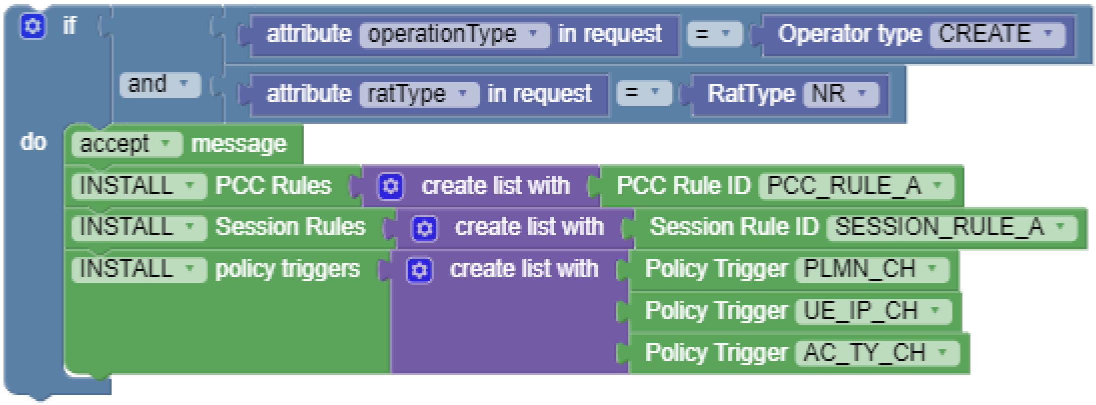
3. In the **Name** field, enter the name for the project.
4. In the **Description** field, enter the description for the project.
5. In the **Service Type**, select the service.
6. Click **Save**.
   The policy project is created.
7. Select the policy project created and click **Open**. This opens a Blockly editor.
   You can construct one or more policies as required using the building blocks provided in the Left Side Panel of the editor construct one or more Policies as required.

   The following screen capture shows an example of how the policies can be created using the building blocks.



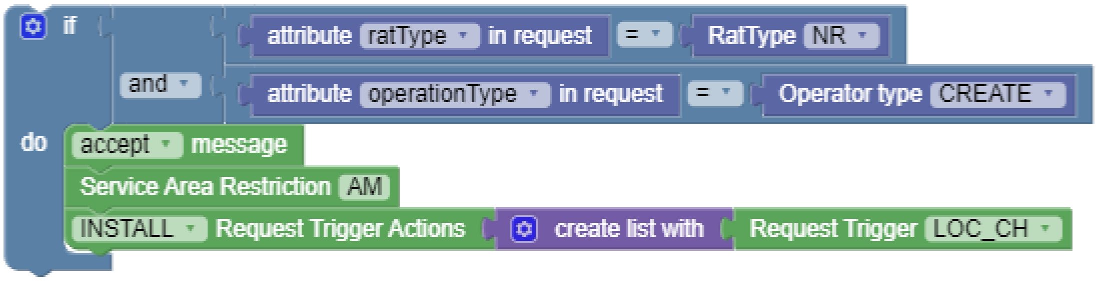
8. Click **Save**.
   The policy for the selected policy project is created.

The following screen capture shows a sample policy for the Session Management policy service:



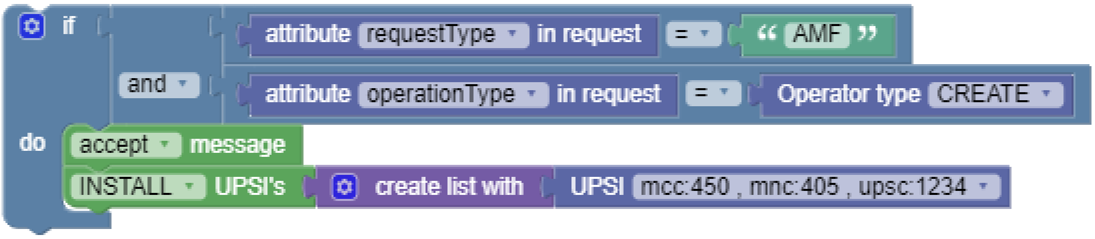
```
if    attribute operationType in request = Operator type CREATE
  and attribute ratType in request = RatType NR
do  accept message
    INSTALL PCC Rules       create list with  PCC Rule ID PCC_RULE_A
    INSTALL Session Rules   create list with  Session Rule ID SESSION_RULE_A
    INSTALL policy triggers create list with  Policy Trigger PLMN_CH
                                              Policy Trigger UE_IP_CH
                                              Policy Trigger AC_TY_CH
```

The following screen capture shows a sample policy for the Access and Mobility Management policy service:



```
if    attribute ratType in request = RatType NR
  and attribute operationType in request = Operator type CREATE
do  accept message
    Service Area Restriction AM
    INSTALL Request Trigger Actions create list with  Request Trigger LOC_CH
```

The following screen capture shows a sample policy for the UE Management policy service:



```
if    attribute requestType in request = " AMF "
  and attribute operationType in request = Operator type CREATE
do  accept message
    INSTALL UPSI's create list with  UPSI mcc:450 , mnc:405 , upsc:1234
```

Data Model

You can create and manage sample attributes for policy. This is used for testing the policies.

To create the Data Model from this page:

1. From the navigation menu, under **Policy Management**, click **Dropdown Blocks**.
   The **Dropdown Blocks** screen appears with the listing of all the attributes created. You can create or import new attributes from this page.

> **Note:**
>
> Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Dropdown Block** screen appears.
3. On the **Create Dropdown Block** screen, enter values for the input fields.
   The following table describes the fields:

Field Name	Description
Attribute Name	Name of the attribute
Description	Description of the attribute
Type	Select one of the values: static or dynamic

4. In the **Block Options** group, click **Add** to add the field details:
   a. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Label Name	Name of the block
Value	Specify the value

> **Note:**
>
> Click **Remove** to cancel the changes.

   b. Click **Save**.
5. Click **Save**.
   The value gets listed on the **Dropdown Blocks** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Dropdown Blocks

To import the dropdown blocks:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

12 System Administration

This chapter describes functions reserved for system administrators.

Importing Configurable Objects

This section describes how to perform a bulk import of configurable objects into the system.

Importing Configuration Object Files

To import json or ZIP files:

1. From the navigation pane, under **System Administration**, click **Bulk Import**.
   The **Upload** option appears on the screen.
2. Click **Upload**.
   Locate the file to be imported.
3. Select a processing option to use to **Handle collisions between imported items and existing items**:
   - **Delete all before importing** The system deletes all objects for each object type matching the import file before importing the object type json file.
     Attention: This import strategy can result in object inconsistency. For example, if you import a ZIP file that only contains traffic profiles, all the traffic profiles are deleted first. However, if existing policies depend on the existing traffic profiles, and the import file does not contain them, the policies can become invalid.
   - **Overwrite with imported version** For each object in the import file, if the object exists in the system, the import updates the object with the configuration contained in the import file. If an object does not exist, the system adds the object to the system.
4. Click **Import**.

The configuration objects and their configuration settings are imported into the database. After the import is complete, the window reports the results for each json file contained in the ZIP file.

Exporting Configurable Objects

This section describes how to perform a bulk export of configurable objects.

Exporting All Configuration Object Files

To export all configuration objects:

1. From the navigation pane, under **System Administration**, click **Bulk Export**.
   The **Export All** option appears on the screen.
2. Click **Export All** .
   A ZIP file is downloaded to your local computer.

Data Model

You can create and manage sample attributes for policy. This is used for testing the policies.

To create the Data Model from this page:

1. From the navigation menu, under **System Administration**, click **Data Model**.
   The **Data Model Management** screen appears with the listing of all the attributes created. You can create or import new attributes from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Data Model** screen appears.
3. On the **Create Data Model** screen, enter values for the input fields.
   The following table describes the fields:

Field Name	Description
ID	ID of the attribute, not displayed on the GUI.
Name	Name of the attribute, not displayed on the GUI.
Label Name	Name of the attribute, displayed on the GUI.
Description	Description of the attribute
Type	Select one of the values: enum or object

4. In the **Fields** group, click **Add** to add the field details:
   a. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Name	Name of the field, not displayed on the GUI.
Description	Description of the field
Label Name	Name of the field, displayed on the GUI.
Type	Select either of the values from drop-down (primitive, object, array)
Primitive Type	Defines the primitive type
Units	Specifies the units
Object Type	Defines the object type
Item Type	
Type	Select either of the values from drop-down (primitive, object)
Primitive Type	Defines the primitive type
Object Type	Defines the object type

> **Note:**
>
> Click **Remove** to cancel the changes.

   b. Click **Save**.

5. In the **Enum Items** group, click **Add** to add the field details:
   a. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Name	Name of the field, not displayed on the GUI.
Value	Specify the value.

   b. Click **Save**.

6. Click **Save**.
   The value gets listed on the **Data Model Management** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Data Model

To import the session rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.