Oracle® Communications

Policy and Charging Rules Function Cloud Native User's Guide

Release 1.0
F20759-01
July 2019

Oracle Communications Policy and Charging Rules Function Cloud Native User's Guide, Release 1.0

F20759-01

Contents

List of Figures

List of Tables

1 Introduction

This document provides information on how to use the Policy and Charging Rules Function (PCRF) and configure the services.

Overview

The Oracle Communications Cloud Native Policy and Charging Rules Function (PCRF) solution incorporates new architecture with spring micro-service framework as backend support technology stack and Kubernetes Cloud Native Environment as running environment. The PCRF core service is the main functionality among PCRF micro services with the following enhancements when compared to legacy PCRF:

- Remove the MIA module from MPE, and let the MPE talks to with configuration server to save/load related data
- PCRF core service have integrated the MPE functionalities which are under legacy PCRF
- When PCRF Core needs to talk with any data source, these traffic shall go with the Diameter connector rather than from the PCRF core itself

Acronyms

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

Table 1-1 Acronyms

Acronym	Definition
cnPCRF	Cloud Native Policy Charging & Rule Function
CP	Control Plane
DL	Downlink
DN	Data Network
DNAI	DN Access Identifier
DNN	Data Network Name
DRX	Discontinuous Reception
ePDG	evolved Packet Data Gateway
EBI	EPS Bearer Identity
FAR	Forwarding Action Rule
FQDN	Fully Qualified Domain Name
GFBR	Guaranteed Flow Bit Rate
GMLC	Gateway Mobile Location Centre
GPSI	Generic Public Subscription Identifier
GUAMI	Globally Unique AMF Identifier
HR	Home Routed (roaming)
LADN	Local Area Data Network

Table 1-1 (Cont.) Acronyms

Acronym	Definition
LBO	Local Break Out (roaming)
LMF	Location Management Function
LRF	Location Retrieval Function
MCX	Mission Critical Service
MDBV	Maximum Data Burst Volume
MFBR	Maximum Flow Bit Rate
MICO	Mobile Initiated Connection Only
MPS	Multimedia Priority Service
N3IWF	Non-3GPP InterWorking Function
NAI	Network Access Identifier
PSA	PDU Session Anchor
QFI	QoS Flow Identifier
QoE	Quality of Experience
(R)AN	(Radio) Access Network
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
S-NSSAI	Single Network Slice Selection Assistance Information
SSC	Session and Service Continuity
SSCMSP	Session and Service Continuity Mode Selection Policy
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TNL	Transport Network Layer
TNLA	Transport Network Layer Association
TSP	Traffic Steering Policy
VID	VLAN Identifier
VLAN	Virtual Local Area Network

References

User can refer to the following documents for information.

- Oracle Communications Policy and Charging Rules Function (PCRF) Cloud Native Installation and Upgrade Guide.

2

Policy and Charging Rules Function (PCRF) Services

This section provides information about the PCRF services which includes:

- PCRF Core Service

PCRF Core Service

PCRF core service includes all the features of 4G PCRF except those provided by MRA, including:

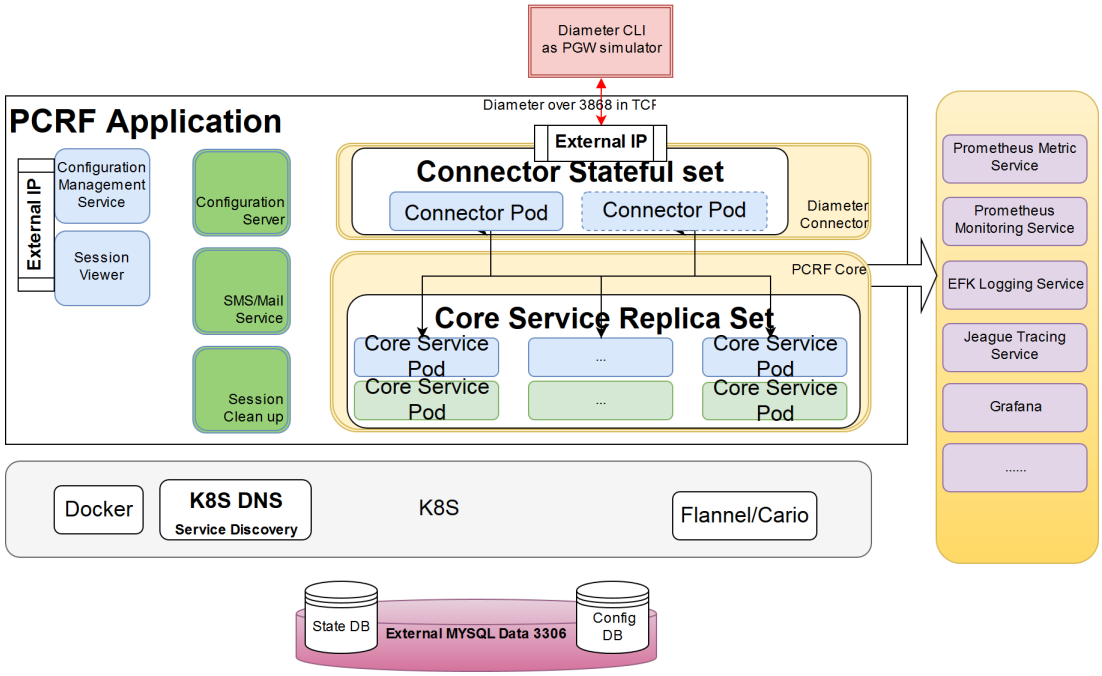
- Protocol implementation including the support of various call flows, validity check, etc.
- Session correlation
- Retrieval and storage of user information
- Invoker of policy service and process of policy actions

3

Policy and Charging Rules Function (PCRF) Architecture

The Oracle Communications Policy and Charging Rules Function (PCRF) 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:

Figure 3-1 PCRF Architecture



4

About Policy Design Experience

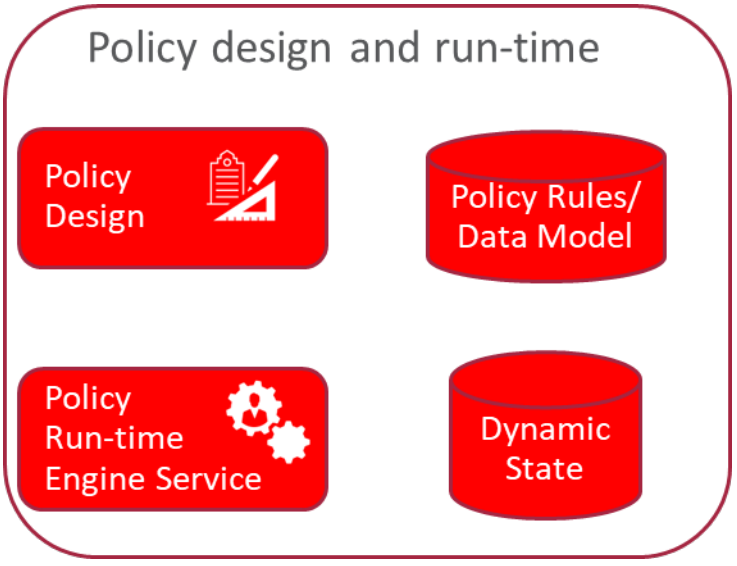
Policy design experience allows an operator to craft and deploy, from scratch, operator policies in production in very less time. 5G brings the policy design experience to the next level by providing flexibility, extensibility, modularization, and assurance to the operator to rapidly, yet confidently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

The Policy and Charging Rules Function (PCRF) 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 PCRF. It also leverages Istio as a service mesh (including Envoy proxies as sidecars) for the internal communication amongst the various micro-services. The Oracle PCRF integrates with a variety of common services for data collection, analysis, and visualization services for operational aspects like logs, metrics, and traces. The Oracle 5G PCRF comprises artifacts like Helm charts that encapsulate lifecycle instructions and resource dependencies for all member components.

The Oracle PCRF is flexible to run in various cloud-native environments. The PCRF 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.

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

Figure 4-1 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

5

How the Services Talk to Each Other

In general, most services under Policy and Charging Rules Function (PCRF) would use ClusterIP as deployment type under Kubernetes cluster environment. However, the following two services need LoadBalancer deployment type which require external access:

- diam-gateway service
- cm service

Given above deployment structure, a public IP would allocate to the above two services which accept external request, the inner communication rely on cluster IP to find each other.

6

Configuring Policy and Charging Rules Function

This section provides the information for configuring Policy and Charging Rules Function (PCRF) for various services.

Managing Session Rules

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.

1. From the navigation menu, under **Configurations**, click **Session Rule**. The Session Rule Management screen appears.
2. Click **Create**. The create session page appears.
3. In the **ID** field, enter the session ID details.
4. In the **Name** field, enter the name for the session.
5. (Optional) In the **Description** field, enter the information about the session rule.
6. In **Authorized Session AMBR** section, enter the following:
   a. In the **Up Link Bandwidth** field, enter the bandwidth details.
   b. In the **Down Link Bandwidth** field, enter the bandwidth details. The bandwidth can be entered in bps, Kbps, Mbps, Gbps, and Tbps.
7. Click **Save** to create the session rule or click **Cancel**. If you have clicked **Save**, a new session rule is created.
8. Click **Edit** to edit the details of session rule.
9. Click **Delete** to delete the session rule.

Managing Session Rule Profile

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

> **Note:**
>
> Only administrators can create a session rule profile.

To create a session rule profile:

1. From the navigation menu, under Configurations, click **Session Rule Profile**.
   The Session Rule Profile Management screen appears.
2. Click **Create**.
   The create session page appears.
3. In the **ID** field, enter the session ID details.
4. In the **Name** field, enter the name for the session.
5. (Optional) In the **Description** field, enter the information about the session rule.
6. In **Authorized Session AMBR** section, enter the following:
   a. In the **Up Link Bandwidth** field, enter the bandwidth details.
   b. In the **Down Link Bandwidth** field, enter the bandwidth details.
      The bandwidth can be entered in bps, Kbps, Mbps, Gbps, and Tbps.
7. Click **Save** to create the session rule profile or click **Cancel**. If you have clicked **Save**, a new session rule profile is created.
8. Click **Edit** to edit the details of session rule.
9. Click **Delete** to delete the session rule.

Managing Service Area Restriction

You can create and manage service restrictions from Service Area Restriction Management screen. The page provides information about the existing service restrictions. You can create or refresh the session rule profiles from this page.

> **Note:**
>
> Only administrators can create a session rule profile.

To create a session rule profile:

1. From the navigation menu, under **Configurations**, click **Service Area Restriction**.
   The Service Area Restriction Management screen appears.
2. Click **Create**.
   The create session page appears.
3. In the **ID** field, enter the session ID details.
4. In the **Name** field, enter the name for the session.
5. (Optional) In the **Description** field, enter the information about the session rule.
6. In **Restriction Type** drop-down, select the restriction type. The available types are:
   a. • ALLOWED_AREAS

- NOT_ALLOWED_AREAS

7. In **Areas** section, click **Create**.
   The Create screen appears.
   a. In the **Tacs** field, enter the Tac details.
   b. In the **Area Codes** field, enter the area code.
   c. Click **Save** to create the area or click **Cancel**. The area is created. You can create multiple areas.
8. Click **Save** to create the session rule profile or click **Cancel**. If you have clicked **Save**, a new session rule profile is created.
9. Click **Edit** to edit the details of session rule.
10. Click **Delete** to delete the session rule.

Managing Authorized Default Qos

You can create and manage QoS from Authorized Default Qos Management screen. The page provides information about the existing QoS. You can create or refresh the QoS profiles from this page.

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

To create a QoS:

1. From the navigation menu, under **Configurations**, click **QoS Information**.
   The Authorized Default Qos Management screen appears.
2. Click **Create**. The create QoS page appears.
3. The **ID** field, enter the session ID details.
4. In the **Name** field, enter the name for the QoS.
5. (Optional) In the **Description** field, enter the information about the session rule.
6. In **Default 5G QoS Identifier** field, enter a number between 0 to 255.
7. In the **Priority Level** field, enter a number between o and 127.
8. In the **Average Window** field, enter?
9. In **Max DataBurstVol** field, enter?
10. In the **arp** section, do the following:
    a. In the **Priority Level** field, enter a number between o and 15.
    b. From **Preemption Capacity** drop-down, select one of the following:
       - NOT_PREEMPT
       - MAY_PREEMPT
    c. From **Preemption Vulnerability** drop-down, select one of the following:
       - NOT_PREEMPTABLE

- PREEMPTABLE

11. Click **Save** to create the session rule profile or click **Cancel**. If you have clicked **Save**, a new session rule profile is created.

Managing PCC Rule

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

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

To create a PCC rule:

1. From the navigation menu, under **Configurations**, click PCC Rule. The PCC Rule Management screen appears.
2. Click **Create**. The create PCC Rule page appears.
3. The **PCC Rule** field is not editable.
4. In the **Name** field, enter the name for the QoS.
5. (Optional) In the **Description** field, enter the information about the session rule.
6. In **Type** drop-down, select the type of PCC rule. The available PCC rules are:
   - Predefined PCC Rule
   - Dynamic PCC Rule
7. (Optional) If selected predefined PCC Rule in step 6, click **Save** to create PCC Rule or click **Cancel** to discard changes.
8. (Optional) If selected dynamic PCC Rule in step 6, perform the following:
   a. In **Flow Infos** section, select the existing flow info or create a new one by clicking **Create** and filling in the detail as mentioned in the below table.
9. In the **APP ID** field,
10. In the **Content Version** field,
11. In the **Precedence** field,
12. In the AF Signalling Protocol drop-down, select one of the following options:
    - NO_INFORMATION
    - SIP
13. In the **Application Relocation** field,
14. In the **QoS Data** field,
15. In the **Traffic Control Data** field,
16. In the **Charging Data** field,
17. In the **Usage Monitoring Data** field,

18. In the **Condition Data** field,
19. Click **Save** to create PCC Rule or click **Cancel** to discard changes.

Table 6-1 Flow Info Fields

Field	Description
Name	Indicates the name 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
Flow Description	Indicates the details about flow. Enter a description for the flow.
Ethernet Flow Description	
Dset Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	Indicates the ethernet.
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	Indicates the VLAN tags.
Save	Click to create a Flow.
Cancel	Click to discard changes.

Managing PCC Rule Profile

You can manage, view, import, export and create the PCC rule profiles from PCC Rule Profile screen.

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

To create a PCC rule profile:

1. From the navigation menu, under **Configurations**, click **PCC Rule Profile**.

   The PCC Rule Profile Management screen appears.
2. Click **Import** and drag the files or click to upload the files from your local machine.

   The supported formats are application/json files.
3. Click **Export All** to export the PCC Rule profiles.
4. Click **Create**.

   The create PCC Rule page appears.
5. Follow the instructions in the Managing PCC Rule.

Managing QoS Data

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

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

To create a QoS Data:

1. From the navigation menu, under **Configurations**, click **QoS Data**.
   The QoS Data Management screen appears.
2. Click **Import** and drag the files or click to upload the files from your local machine.
   The supported formats are application/json files.
3. Click **Export All** to export the QoS Data.
4. Click **Create** and fill the details as mentioned in the below table o create QoS Data.

Field	Description
QoS Id	Univocally identifies the QoS control policy data within a PDU session.
Name	The name of the Qos Data
Description	The description of the Qos Data
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 and "defQosFlowIndication" is not included or is included and set to false.
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.
ARP	
Priority Level	Defines the relative importance of a resource request.

Field	Description
Preemption Capacity	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level.
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.
QoS Notification Control	Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR can no longer (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow. Default value is "FALSE", if not present and has not been supplied previously.
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 UI	Indicates, by containing the same value, what PCC rules may share resource in uplink direction.
Sharing Key DI	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 5G-AN PDB (NOTE).
Maximum Packet Loss Rate DI	Indicates the downlink maximum rate for lost packets that can be tolerated for the service data flow.
Maximum Packet Loss Rate DI	Indicates the downlink maximum rate for lost packets that can be tolerated for the service data flow.
Maximum Packet Loss Rate UI	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.
Save	Click to create qos data record.
Cancel	Click to cancel the changes.

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 access a Charging Data:

1. From the navigation menu, under **Configurations**, click **Charging Data**.
   The Charging Data Management screen appears.
2. Click **Import** and drag the files or click to upload the files from your local machine.
   The supported formats are application/json files.
3. Click **Export All** to export the charging data.
4. Click **Create** and fill the details as mentioned in the below table o create Charging Data.

Field	Description
Chg Id	Univocally identifies the charging control policy data within a PDU session.
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 pre-configured 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	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 pre-configured 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 Sv Prov Id	Indicates the application service provider identity.
Af Charging Identifier	Indicates the identifier of the service or service component the service data flow in a PCC rule relates to.
Save	Click to create charging data record.
Cancel	Click to cancel the changes.

Managing Usage Monitoring Data

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

> **Note:**
>
> Only administrators can create usage monitoring data.

To create a usage monitoring data:

1. From the navigation menu, under **Configurations**, click **Usage Monitoring Data**. The Usage Monitoring Data Management screen appears.
2. Click **Import** and drag the files or click to upload the files from your local machine. The supported formats are application/json files.
3. Click **Export All** to export the Usage Monitoring Data.
4. Click **Create** and fill the details as mentioned in the below table o create Usage Monitoring Data.

Field	Description
Um Id	Univocally identifies the usage monitoring policy data within a PDU session.
Name	The name of the UsageMonitoring Data
Description	The description of the UsageMonitoring Data

Field	Description
Volume Threshold	Indicates the total 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 Uplink	Indicates a volume threshold in uplink after the Monitoring Time.
Next Vol Threshold Downlink	Indicates al 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.
Save	Click to create usage monitoring data record.
Cancel	Click to cancel the changes.

Managing Traffic Control Data

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

To create traffic conditional data:

1. From the navigation menu, under **Configurations**, click **Traffic Control Data**. The Traffic Control Data Management screen appears.
2. Click **Import** and drag the files or click to upload the files from your local machine. The supported formats are application/json files.
3. Click **Export All** to export the Traffic Control Data.
4. Click **Create** and fill the details as mentioned in the below table to create the Traffic Control Data.

Field	Description
Tc Id	Univocally identifies the traffic control policy data within a PDU session.
Name	The name of the Traffic Control policy data
Description	The description of the Traffic Control policy data

Field	Description
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.
Redirect Information	
Redirect Enabled	Indicates the redirect is enable
Redirect Access 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 pre-configured traffic steering policy for downlink traffic at the SMF.
Traffic Steering Pol Id UI	Reference to a pre-configured traffic steering policy for uplink traffic at the SMF.
Route To Locs	
Dnai	Identifies the location of the application.
Route Information	Includes the traffic routing information.
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.
Up Path Chg Event	
Notification Uri	
Notification Correlation Id	It is used to set the value of Notification Correlation ID in the notification sent by the SMF.

Field	Description
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 forward-compatibility with future extensions to the enumeration but is not used to encode content defined in the present version of this API.
Save	Click to create traffic control data record.
Cancel	Click to cancel the changes.

Managing Condition Data

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

> **Note:**
>
> Only administrators can create condition data

To create a condition Data:

1. From the navigation menu, under **Configurations**, click **Condition Data**.
   The Condition Data Management screen appears.
2. Click **Import** and drag the files or click to upload the files from your local machine.
   The supported formats are application/json files.
3. Click **Export All** to export the Condition Data.
4. Click **Create** and fill the details as mentioned in the below table o create Condition Data.

Field	Description
Cond Id	Uniquely identifies the condition data within a PDU session.
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.
Save	Click to create condition data record.
Cancel	Click to cancel the changes.