Oracle® Communications

Cloud Native Core, Converged Policy Design Guide

Release 24.2.8
F99295-10
November 2025

Oracle Communications Cloud Native Core, Converged Policy Design Guide, Release 24.2.8

F99295-10

Contents

My Oracle Support

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

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

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms

This section provides information about the acronyms used in the document.

Table Acronyms

Acronym	Definition
5GC	5G Core Network
5GS	5G System
5G-AN	5G Access Network
5G-EIR	5G-Equipment Identity Register
5G-GUTI	5G Globally Unique Temporary Identifier
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
5QI	5G QoS Identifier
AF	Application Function
AMF	Access and Mobility Management Function
AS	Access Stratum
AUSF	Authentication Server Function
BSF	Oracle Communications Cloud Native Core, Binding Support Function
CAPIF	Common API Framework for 3GPP northbound APIs
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
LBO	Local Break Out (roaming)
LMF	Location Management Function
LRF	Location Retrieval Function
MCPTT	Mission-critical push-to-talk
MCX	Mission Critical Service
MDBV	Maximum Data Burst Volume
MFBR	Maximum Flow Bit Rate
MICO	Mobile Initiated Connection Only

Table (Cont.) Acronyms

Acronym	Definition
MPS	Multimedia Priority Service
N3IWF	Non-3GPP InterWorking Function
NAI	Network Access Identifier
NEF	Network Exposure Function
NF	Network Function
NGAP	Next Generation Application Protocol
NR	New Radio
NRF	Network Repository Function
NSI ID	Network Slice Instance Identifier
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSP	Network Slice Selection Policy
NWDAF	Network Data Analytics Function
PCF	Policy Control Function
PDR	Packet Detection Rule
PEI	Permanent Equipment Identifier
PER	Packet Error Rate
PFD	Packet Flow Description
PPD	Paging Policy Differentiation
PPF	Paging Proceed Flag
PPI	Paging Policy Indicator
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
SA NR	Standalone New Radio
SBA	Service Based Architecture
SBI	Service Based Interface
SD	Slice Differentiator
SEAF	Security Anchor Functionality
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
SMSF	Short Message Service Function
S-NSSAI	Single Network Slice Selection Assistance Information
SRA	Successful Resource Allocation
SSC	Session and Service Continuity
SSCMSP	Session and Service Continuity Mode Selection Policy
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier

Table (Cont.) Acronyms

Acronym	Definition
SUPI	Subscription Permanent Identifier
TNL	Transport Network Layer
TNLA	Transport Network Layer Association
TSP	Traffic Steering Policy
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function
UL	Uplink
UL CL	Uplink Classifier
UPF	User Plane Function
URSP	UE Route Selection Policy
VID	VLAN Identifier
VLAN	Virtual Local Area Network

What's New in This Guide

This section introduces the documentation updates for release 24.2.x.

Release 24.2.8 - F99295-10, November 2025

There are no updates for this document in this release.

Release 24.2.7 - F99295-09, July 2025

There are no updates for this document in this release.

Release 24.2.6 - F99295-08, June 2025

There are no updates for this document in this release.

Release 24.2.5 - F99295-07, April 2025

There are no updates for this document in this release.

Release 24.2.4 - F99295-06, March 2025

There are no updates for this document in this release.

Release 24.2.3 - F99295-05, January 2025

There are no updates for this document in this release.

Release 24.2.2 - F99295-04, November 2024

There are no updates for this document in this release.

Release 24.2.1 - F99295-03, October 2024

There are no updates for this document in this release.

Release 24.2.0 - F99295-02, October 2024

- Updated description of attributes **in Request Type** and **in AMF Request** in PCF UE Policy as **n1TransferFailureCause** option is deprecated for **in Request Type** and is now available under **in AMF Request**.

Release 24.2.0 - F99295-01, August 2024

- Added details of *Successfully Installed UPSI in N1 Notify Message* block in PCF UE Policy, which notifies successfully installed UPSIs during a N1N2Transfer.

1 Introduction

This document provides information about designing and configuring Oracle Communications Cloud Native Core Converged Policy Projects.

1.1 Overview

Cloud Native Core Policy Design Guide provides information about how to design operator defined policies using the Cloud Native Core Policy Design studio accessible through the Oracle Communications Cloud Native Configuration Console (CNC Console). The policy design studio allows users to build powerful logic yet using intuitive and user friendly building blocks. This document describes how operators can use various building blocks to design logic used in following elements:

- conditions. Example: if statements
- actions. Example: to install a PCC Rule

In addition, the Policy design guide provides detailed information about various building blocks available to build policies specific to a domain, e.g. to handle PCRF use cases versus PCF Session Management or Access and Mobility Management Policy to name a few. Sample policies, given as examples throughout the document, enable users to handle common use cases conveniently.

For more information about the User Interface (UI) elements of Policy services, see *Oracle Communications Cloud Native Core, Converged Policy User's Guide*.

1.2 References

You can refer to the following documents for information.

- Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide
- https://developers.google.com/blockly
- Oracle Communications Cloud Native Core, Converged Policy User's Guide

2
Managing Policy Projects

This chapter describes how to create new policy projects, edit an existing policy project, and create new policies from the blocks using the **Policy Projects** option in CNC Console. This option is available under **Policy**, and then **Policy Management** in the left navigation menu of the CNC Console.

You can use blocks to create policies for the following services:

- Session Management
- Access and Mobility Management
- UE Management
- PCRF-Core
- Policy Data Source

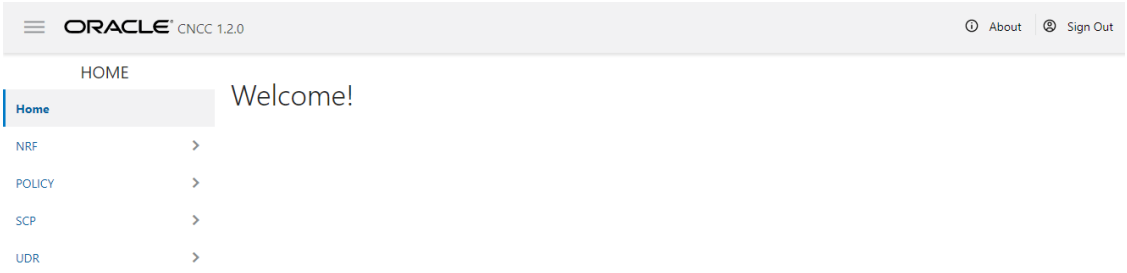
Cloud Native Configuration Console

This section provides an overview of the Oracle Communications Cloud Native Configuration (CNC) Console, which includes an interface to aid in creating cloud native policies.

To log in:

1. Open a web browser and enter the IP address of the CNC Console system.
   The login page opens.
2. Enter your **Username** and **Password**, and click **Login**.

The main page opens.



You can now access policy configurations by clicking on **Policy** in the left navigation menu.

2.1 Creating and Modifying Policy Projects

To create a new policy project and modify an existing policy project:

1. From the navigation menu, under **Policy**, then under **Policy Management**, click **Policy Projects**. Existing policy projects appear in the **Policy Projects** area.
2. To create a new policy project, click **Create**.

> **Note**
>
> To create a policy project under PDS, you must add the PDS service on Policy Engine screen. For more information, see *Oracle Communications Cloud Native Core, Converged Policy User's Guide.*

3. In the **Create Project** dialog box, provide inputs for the following fields:
   a. **Name**: Name for the policy.
   b. **Description**: A description for the policy.
4. Click **Save**.

   The newly created policy project is added to the **Policy Projects** area.
   The **State Transition** for a newly created policy project is set to **Dev** by default and enables policy writers to create policies by dragging blocks to the work area.
5. Change the state of the policy project to **Prod**, by clicking the **Prod** button, after all changes are saved and you want to evaluate the policy.

> **Note**
>
> When the state for a policy project is set to Prod, user cannot add blocks to the work area. To make any changes to your policy project, make sure that it is in **Dev** state.

6. **(Optional)** If you want to modify an existing policy project, select the required policy project, and then click one of the following buttons:
   a. **Edit**: To edit the name and description of the policy project.
   b. **Delete**: To delete the policy project.
   c. **Open**: To open the policy project and create a policy using blocks. For more information, see Creating Policies.
   d. **Clone:** To create a clone of an existing policy project, use this option. Enter name and description, and click the **Save** button.
   e. **Refresh**: To update the changes made to the Policy Projects area.

3
About Policies

You can create policies for Session Management, Access and Mobility Management, UE Management, pcrf-core and pds services. For each policy project, multiple interlocking, graphical blocks are predefined and divided into categories. You can combine these blocks in the work area to create policies.

The side menu, called the Toobox, contains blocks that are organized in categories. Policy writers can click on any of the categories in the toolbox, and select blocks to create policies. The following screen capture shows the toolbox when a user creates policy project in PCF-SM category:

Figure 3-1 Toolbox

Work area allows you to create, edit, save, and delete policies. A policy project execution starts with the main policy. If you want to add more policies to the execution thread, you have to refer to them from the main policy. After the blocks are added to the work area, you can modify them using the context menu available for each block. To view the context menu, right-click the respective block. For more information about the context menu options, see Context Menu Options for All Blocks.

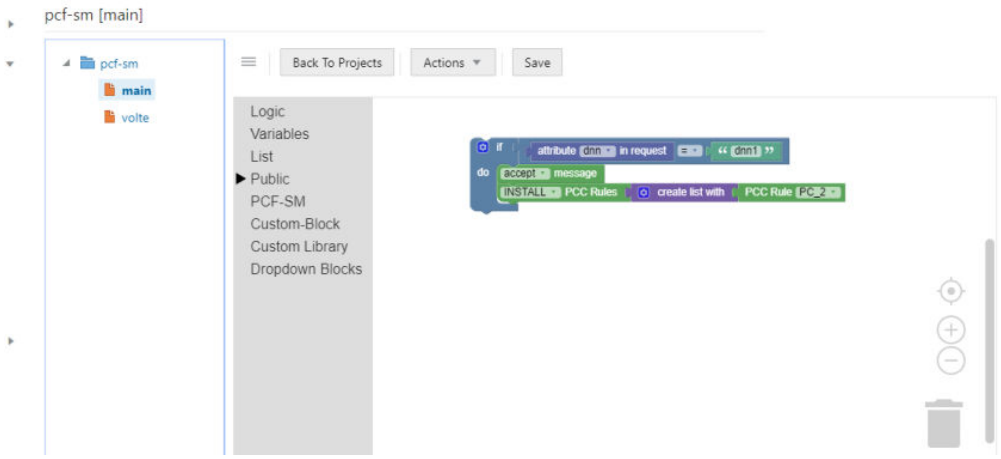
3.1 Creating Policies

You can create new policies using the blocks available for each block category. You can drag blocks to the work area and interconnect them to create policies. These policies can be edited further in the work area.

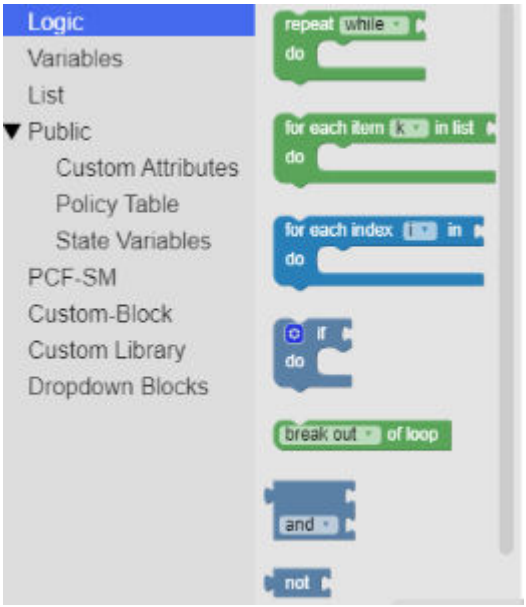
You must have created policy projects in the Policy Projects area as described in Creating and Modifying Policy Projects.

1. From the left navigation menu, under **Policy**, then under **Policy Management**, click **Policy Projects**. Existing policy projects appears in the **Policy Projects** area.
2. In the Policy Projects area, select a policy project and click **Open**.

The toolbox and work area appear.



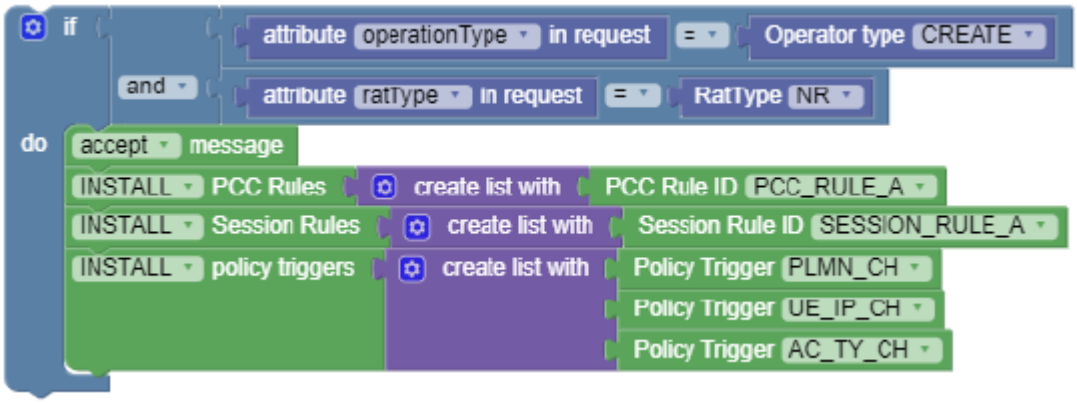
3. From the toolbox, click a category to view the blocks in an adjacent pane. The following screen capture shows the blocks available for **Logic** category:



4. To create a policy, do the following:
   a. From the adjacent pane of the toolbox, click the required block to add into the work area. You can also add the blocks using drag-drop functionality.
   b. After adding the required blocks in the work area, interconnect these blocks in a logical manner to create a policy.
5. Click **Save**.

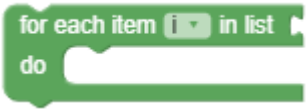
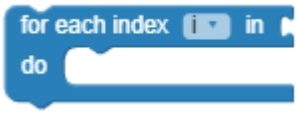
   A new policy is created.

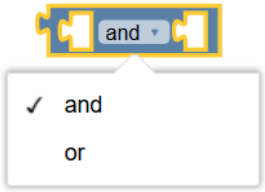
The following image shows an example of a policy for the Session Management policy service:

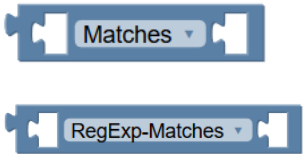


3.2 Logic Category

Using blocks under this category, user can create and terminate loops, compare value of variables, and apply conditionals while writing policies.

Block Icon	Block Name	Description
	repeat	Runs a code in the block body for the specified number of times. This block provides loop options. You can alter between the following options by clicking the existing option: • **while**: Repeats a code in the block body while some conditions are achieved. • **until**: Repeats a code in the block body until some conditions are achieved.
	for each item	Renders loop variable values from a list, not in a numeric sequence. **i** indicates a variable that can be set for each item in the list. To change the value of **i**, or to rename or delete it, click **i** and choose an appropriate option.
	for each index	Loops through list provided using an index **i**. This loop is created to loop custom attributes list using an index value. **i** indicates a variable that can be set for each index. To change the value of **i**, or to rename or delete it, click **i** and choose an appropriate option.

Block Icon	Block Name	Description
	if	Compares the values of two variables available in another block that is interconnected to it. This block provides options to add appropriate clauses to a condition. You can click the gear icon () to add following options to the **if** clause: • **else if** • **else**
	break out of loop	Terminates the loop from moving from one phase or iteration to another. If you want to continue the looping from next phase or iteration, then click **break out** and select the **continue with next iteration** option from the context menu. Note: This block can be used with the following blocks only: • repeat block • for each item block
	and/or	Returns or produces the **true** value when the following options are set: • **and:** Both the inputs are also true. • **or:** Either of its inputs are true. You can alter between the aforementioned options by clicking the existing option.
	not	Converts the input value of its interconnected block to its opposite value. For example, if this block is interconnected to a block with the input values as true, then the output is false. If no input is provided to this block, then it accepts a true value by default and produces an output with value as false.
	inequality	Performs a non-equal comparison between two values using the available inequality options. You can select an appropriate inequality option from the context menu by clicking the existing option.

Block Icon	Block Name	Description
	comparison	Performs simple wildcard matching for character * and ? when the policy writer selects **Matches** from the drop-down value. To perform full regular expression matching, select **RegExp-Matches** from the drop-down list.

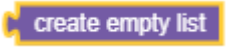
3.3 Variables Category

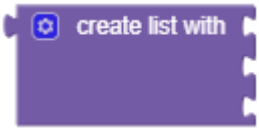
Using this block category, you can assign values to variables.

Block Icon	Block Name	Description
	set	Assigns a value to the variable that matches the value of the input. Also, creates a variable if it does not exist. **i** indicates a variable that can be set for this block. To rename or delete this variable, click **i** and choose an appropriate option from the context menu.
	change	Adds a number to a variable. **i** indicates a variable that can be set for this block. To rename or delete this variable, click **i** and choose an appropriate option from the context menu.
	variable	Returns or produces the value of this variable. **i** indicates a variable. To rename or delete this variable, click **i** and choose an appropriate option from the context menu.

3.4 List Category

Using blocks under this category, you can create lists.

Block Icon	Block Name	Description
	create empty list	Returns or produces a list of length 0 without any data record.
	Concat list	Creates lists in loop. See Use case.

Block Icon	Block Name	Description
	create list with	Creates a list with any number of items. You can click the gear icon () to add items to the list from the context menu.
	contains	This block takes two lists as an input and check if the contents of the list on the right hand side are present in the list on the left hand side based on the option selected in the drop-down list. **Return Type** : returns true/false based on match of drop-down option(**any**,**all**,**none**) Drop-down list Options : 1. **all** : returns true if all the contents of the list on the right hand side are present in the list on the left hand side. 2. **any**: returns true if any one of the contents of the list on the right hand side are present in the list on the left hand side. 3. **none**: returns true if none of the contents of the list on the right hand side are present in the list on the left hand side.
	find	It has two parameters. • Param1 – accepts array of items given by user. • Param2 – takes the json path which has key-value pair -> fetches keys from JSON **Return Type** : array of matched items based on drop-down list (**one**/**any**) Drop-down list options : 1. **any**: Returns the array of matched items. 2. **one**: Returns the first matched item in array.

Block Icon	Block Name	Description
	valuelist	This block matches two value lists as an input and matches the contents of the list on the right hand side with the list on the left hand side based on the option selected in the drop-down list.

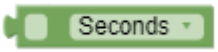
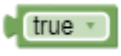
3.5 Public Category

Under the **Public** category, you can find the most commonly used blocks. This category further consists of the following sub-categories:

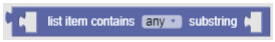
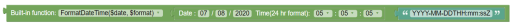
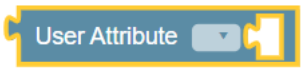
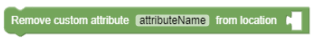
- Customer Attributes
- Policy Table
- State Variables
- Policy Counters (PCF-SM, PCF-AM, PCF-UE, PCRF)
- Operator Specific Data
- User Attributes (PCF-SM, PCF-AM, PCF-UE, PCRF)
- Subscriber Notification (PCF-SM and PCRF only)
- Analytics Data
- Usage Monitoring (PCRF only)

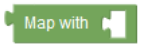
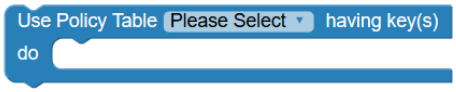
Block Icon	Block Name	Description
	number	Represents a numerical value. To replace the existing value, click the value and type a new value.
	string	Represents a series of characters and numbers. To add one or a series of characters, click the square symbol embedded between quotation mark and type a character for the string.
	message	Accepts or rejects a message when interconnected with another block. You can alter between accept and reject options by clicking the existing option.
	End	This block is actually a return statement.
	End with	This block is used to return with a value.
	request	

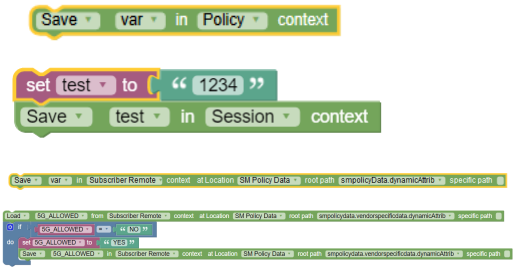
Block Icon	Block Name	Description
	response	
	String Operations	It has two parameters and performs (**contains**, **append**) between two strings. Both the parameters are strings. Drop-down operators : 1. **contains**: returns true if the param1 has substring param2. 2. **appends**: returns the string by appending param1 with param2.
	Call function	This block executes a function from the policy library with zero or more arguments. Please see the Policy Library section for help with defining functions. A function call with zero arguments can be done like this: 
	Call policy	This block is used to call a policy inside another. Click the drop-down option next to the **Policy** block to choose an appropriate option to set the policy.
	Key Value	This block allows policy writers to create {key:"key",value:"value"} pair. You may use this block along with map block to create a {key:value} attribute pair.
	Object expression	This block helps the operator to write a JavaScript statement. This block can return a value or expression. For Example: request.request.appSessionContextReqData.ascReqData.medComponents
	Statement expression	This block helps the operator to write a JavaScript statement. This block does not return anything. For Example: logger.log("ALWAYS",JSON.stringify(response))

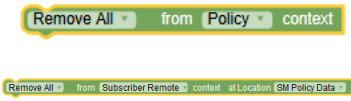
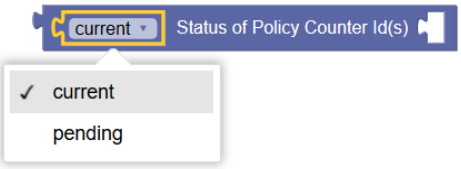
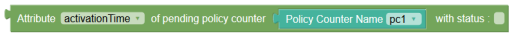
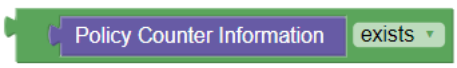
Block Icon	Block Name	Description
	Log level	This block can be used to set the log level for Policy services. Users can select any of the following valid values using the drop-down menu: • ALWAYS • ERROR • WARN • INFO • DEBUG • TRACE The Log level condition block can be used to design policies for PCF-SM, UE, AM, PDS, and PCRF-Core policy projects.
	Arithmetic	Performs arithmetic operations on two variables. This block provides multiple arithmetic operations. Click the drop-down option to choose an appropriate option.
	Date Arithmetic Helper	Performs date arithmetic operations. This block provides multiple units of time. Click the drop-down option to choose an appropriate option.
	built-in function	Performs built-in functions and produces outputs in predefined formats. For example, a date input can produce outputs in different formats, such as hour, minute, seconds, and so on. This block provides multiple options to set a value of the function. Click the drop-down option to choose an appropriate option.
	Date and time format	Produces a selected date in date and time formats. To set a date and time, click the required option and type a value.
	boolean	Sets a variable value to **true** or **false**. To set this block to **true** or **false**, click the drop-down option and choose the required option.

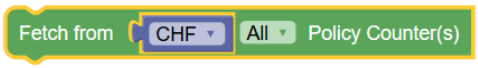
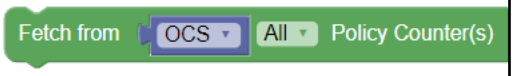
Block Icon	Block Name	Description
	Exist/is null check	Determines the value of the block at the placeholder. You can set this block to one of the following options: • **exists**: Checks whether the value of block at the placeholder is "undefined". If yes, it produces true, otherwise false. • **is null**: Checks whether the value of block at the placeholder is "null". If yes, it produces true, otherwise false. To set this block to **exists** or **is null**, click the drop-down option and choose the required option.
	contains in matchlist	This block takes matchlist items in right side and any block can be attached in list in left side. There are three options: • **any** - If any attribute value from left side is present in matchList - condition will return true, otherwise false. • **all** - If all attribute values from left side are present in matchList - condition will return true, otherwise false. • **none** - If none of the attribute value from left side is present in matchList - condition will return true, otherwise false.
	list includes variable	This block can be used to find whether a variable is present in the list or not. Left hand side contains List and right hand side is variable which is to be validated for its presence or absence. There are two options: • **includes** • **doesnt_include**

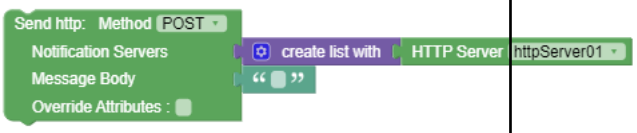
Block Icon	Block Name	Description
	list items contain substring	This block can be used to find whether all, any, or no substring is present in list items. Left hand side contains List and right hand side is variable/list which is to be validated for its presence or absence. There are three options: • **any** • **all** • **none**
	Convert epoch time to date format	This block can be used to convert epoch time to specified date format.
User Attributes		
	User Attributes	This block allows operators to access custom yaml schemas for suscribers that were imported and tagged as "user" during the import on the **Yaml Schema** screen on CNC Console. The drop-down values in the block are auto-populated depending on the attribute selected by the operator. The User Attributes can be used for PCF-SM, PCF-AM, PCF-UE, and PCRF Core policy projects.
Customer Attributes		
	root	Creates attributes at the root level.
	default	Configures the default path of a policy.
	custom attributes validation	Produces the value of a selected attribute present in the path provided by the default block.
	set custom attributes	Creates custom attributes with the "attributeName" name at the "root" location with a value provided by the Create node block.
	remove custom attributes	Removes custom attributes and the attribute name from the root location.
	create node	Creates JSON objects. When an attribute is selected, all the fields of that attribute are populated. You must provide values to these attributes by clicking the drop-down options.

Block Icon	Block Name	Description
	Create map with	Creates Map object with key value pairs when combined Key Value block.
Policy Table		
	Fetch Policy Table Row	Fetches "policy Table Row" based on the match with the key Columns values provided. This block can be used to configure Charging Servers. To configure a changing server: 1. Select **ChargingServers** from the Use Policy Table drop-down list. 2. Provide value for the **Charging_Server_row**.
	Fetch Policy Table Column	Fetches "Policy Table Column value" based on the row selected in the "Fetch Policy Table Row" Block.
	Fetch Policy Table Row Loop	This block returns multiple matched rows. It supports sort option, and can be used with multiple operators such as, "=", "!=", Ignore, matches for, and more.
	break out of loop	Terminates the loop from moving from one phase or iteration to another. If you want to continue the looping from next phase or iteration, then click break out and select the continue with next iteration option from the contex menu. **Note:** This block can only be used with the blocks listed under the **Policy Table** category.
State Variables		

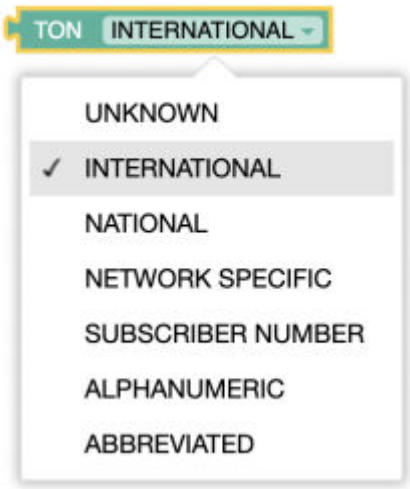
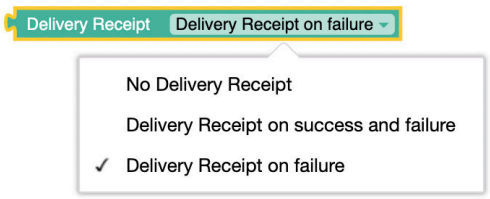
Block Icon	Block Name	Description
 **Figure 3-2 Example: Remote SSV for UE Policy**  	save/load/remove state variable(s)	When you use the context as **Policy**, **Session**, or **Subscriber**, this block can be used to save in, load, or remove from the specified state variable `var` and the value assigned to it inside the selected context. When you select the context as **Subscriber Remote**, the block is automatically populated with the following new fields: • **at Location**: This drop-down list provides the list of root path types that are pre-configured under **Policy**, and then **Service Configurations**, and then **PDS**. • **root path**: After you select the required root path type, this field shows the list of configured paths as a drop-down list. You may select any one from the list. **Note**: The specific path check box can be used to modify a particular attribute or variable in JSON. In the given policy example, SM receives SMPolicyData and SubscriberStateVariables from PDS. Then, PRE evaluates subscriberStateVariables (5G_ALLOWED), and SM_PRE sends updated information to PDS. It is important to note that both PRE and SM-PRE refers to `subscribervariable.remote.smpolicydata.dynamicattribute` and not `smpolicydata.dynamicAttrib`. **Note**:The context list includes the Remote option to create Subscriber Remote State Variables only for SM and UE Services. This option is not available for AM Service.

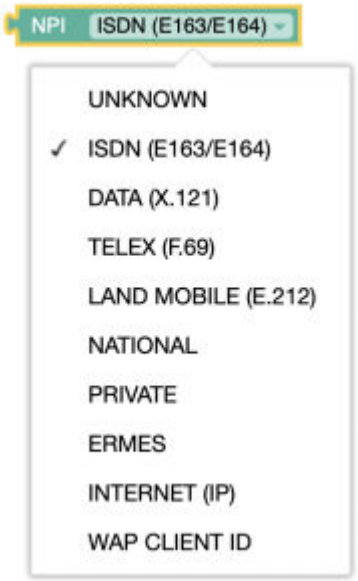
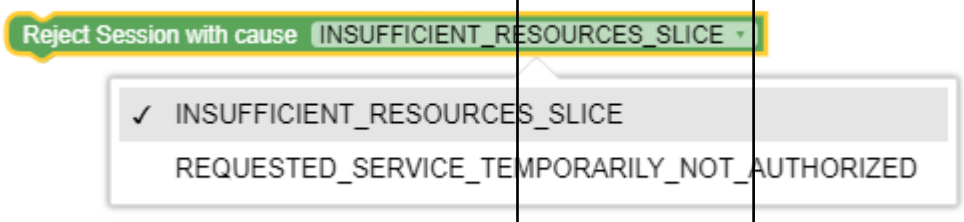
Block Icon	Block Name	Description
	remove all variables	Removes all the variables from specified context. The available options for context drop-down are: • **Policy** • **Session** • **Subscriber** • **Subscriber Remote**
Figure 3-3 Operator Specific Data 	Operator Specific Data	Retrieves the values from the schema.yaml files uploaded on the Yaml Schema page on CNC Console for Policy. For more information on how to use Yaml Schema page, see *Oracle Communications Cloud Native Core, Converged Policy User's Guide*.
Policy Counters		
	Policy Counter Name	Retrieves policy counter names, configured using Policy Data configurations (**Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Policy Counter Id** on the Cloud Native Configuration Console.
	Status of Policy Counter ID(s)	Retrieves the current or pending status of specified policy counter IDs. Operators can specify policy counter IDs by using either **Policy Counter Name** block or **string** block.
	Attribute of pending policy counter with status	Selects activationTime attribute of pending policy counter IDs, specified by the operator. The status here is optional. Select the check box for **status**, and provide its value using a string block.
	Policy Counter IDs	Retrieves all the available policy counter IDs. It is available only in the Public category of PCRF Core policy projects.
	Policy Counter Information	Checks if Policy Counter Information exists or not. It is available only in the Public category of PCRF Core policy projects.

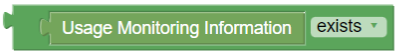
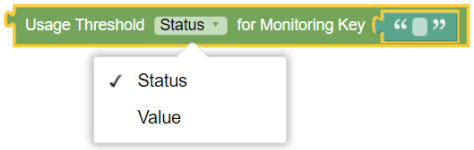
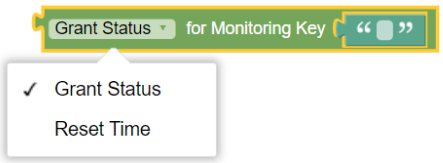
Block Icon	Block Name	Description
	Fetch Policy Counters	Retrieves the status of all or specific policy counters from the CHF or OCS through session management service. If you want to fetch specific policy counters from CHF or OCS, use either of the following blocks: • policy counter name block and select policy counter ID from the drop-down list. • string block with comma separated values (policy counter IDs). **Note**: To use this block, make sure that **Enable Async CHF Query** or **Enable Async OCS Query** button is enabled on service configurations page on CNC console. (Policy > Service Configurations > PCF Session Management) This block is available under the **Public** category of **PCF Session Management** policy projects.
	Fetch Policy Counters from OCS	Retrieves the status of all or specific policy counters from the OCS. If operators wish to fetch specific policy counters from OCS, either of the following can be used: • policy counter name block and select policy counter ID from the drop-down list • string block with comma separated values (policy counter IDs) **Note**: To use this block, make sure that **Async Query** switch is enabled on service configurations page on CNC console. (Policy > Service Configurations > PCRF Core > Settings) This block is available under the **Public** category of **PCRF Core** policy projects.

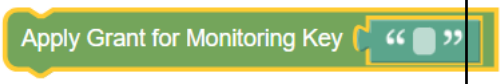
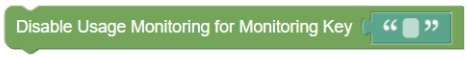
Block Icon	Block Name	Description
	End All	You can exit the policy evaluation at any point in time using the **End All** blockly. This blockly has been added in the Public section for all the services such as PCRF CORE, SM, PDS, and so on. If the **End All** blockly is used, the policy evaluation exits from that point and whatever evaluation has been done till then returns from PRE (policy runtime). It is used in case the user wants to perform a certain set of actions and exit from there in some condition without going and evaluating an entire policy. The following log message is printed in the policy runtime indicating that policy evaluation has exited: `Exit requested from Policy evaluation, hence Exiting from policy!!`
Subscriber Notification		
Figure 3-4 Send HTTP Notification 	Send HTTP Notification	This block can be used to send HTTP messages to pre-defined HTTP servers with HTTP header and message body. The HTTP methods supported for sending messages are POST, PUT, GET, and PATCH.

Block Icon	Block Name	Description
Figure 3-5 Send SMS 	Send SMS using SMPP protocol	This action is used to send short text messages as SMS using SMPP Protocol. You must include the MessageBody and the Destination address with User IDs. **Note** Currently, this action is supported only for PCRF-Core call flows. For more details on Send SMS action, see Subscriber Notification Use Cases.

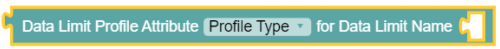
Block Icon	Block Name	Description
Figure 3-6 Type of Number 	Type of Number	Type of Number can be: • UNKNOWN • INTERNATIONAL • NATIONAL • NETWORK SPECIFIC • SUBSCRIBER NUMBER • ALPHANUMERIC • ABBREVIATED
Figure 3-7 SMS Gateway Group 	SMS Gateway Group	This blockly is used to display the list of SMS Gateways configured in CNC Console.
Figure 3-8 Delivery Receipt 	Delivery Receipt	The Delivery Receipt can be: • No Delivery Receipt • Delivery Receipt on Success and Failure • Delivery Receipt on Failure

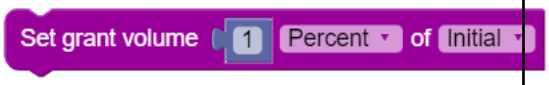
Block Icon	Block Name	Description
Figure 3-9 Number Plan Indicator 	Number Plan Indicator	Number Plan Indicator blockly is used to select the type of plan such as: • UNKNOWN • ISDN (E163/E164) • DATA (X, 121) • TELEX • LAND MOBILE • NATIONAL • PRIVATE • ERMES • INTERNET (IP) • WAP CLIENT ID
Analytics Data		
Figure 3-10 Analytics Data 	Analytics Data	This block can be used to select analytic data attributes related to Slice Load Level.
Figure 3-11 Reject Session with Cause 	Reject Session with Cause	This block can be used to reject a session due to insufficient resources or unauthorized scenario.
Usage Monitoring		

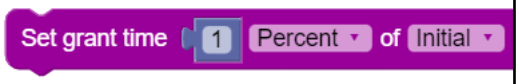
Block Icon	Block Name	Description
Figure 3-12 Usage Monitoring exists 	Usage Monitoring Information exists	Checks if Usage Monitoring Information exists or not.
Figure 3-13 Monitoring Key for Usage Monitoring Level 	Monitoring Key for Usage Monitoring Level	This block can be used to retrieve monitoring key when Usage Monitoring is at session level.
Figure 3-14 Usage Threshold Status for Monitoring Key 	Usage Threshold Status for Monitoring Key	This block can be used to retrieve usage threshold status or value for the specified Monitoring Key.
Figure 3-15 Grant Status for Monitoring Key 	Grant Status for Monitoring Key	This block is used to retrieve the grant status or reset time for the specified Monitoring Key.

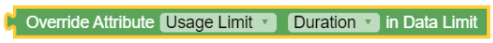
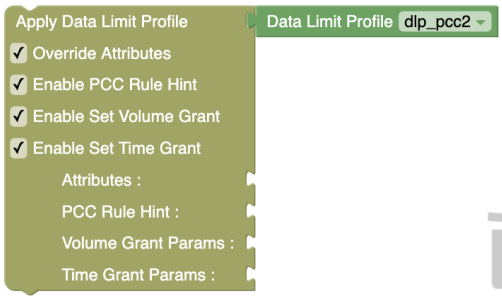
Block Icon	Block Name	Description
Figure 3-16 Apply Grant for Monitoring Key 	Apply Grant for Monitoring Key	This action block can be used to apply Grant for the specified Monitoring Key.
Figure 3-17 Disable Usage Monitoring for Monitoring Key 	Disable Usage Monitoring for Monitoring Key	This action block can be used to disable Grant for the specified Monitoring Key.
Figure 3-18 Usage Monitoring Level 	Usage Monitoring Level	This util can be used for specifying that the Usage Monitoring is at session level.
Figure 3-19 Grant Status Approved 	Grant status	This util can be used for specifying whether Grant status is approved or denied.

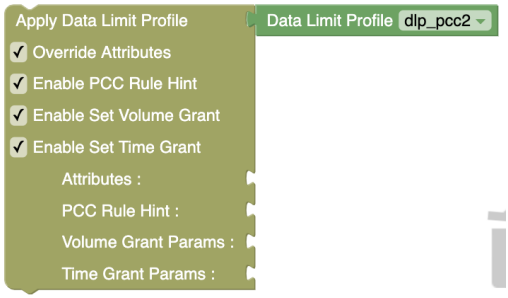
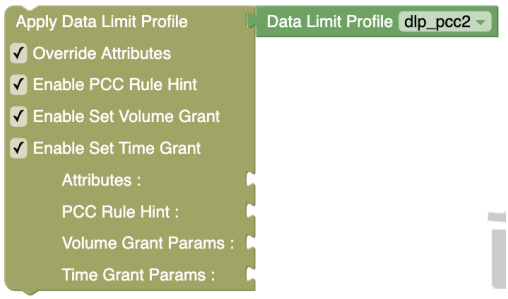
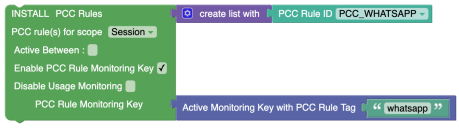
Block Icon	Block Name	Description
Figure 3-20 Usage Monitoring Information 	Usage Monitoring Information	This util can be used for retrieving Usage Monitoring Information.
	Forwarded Attribute	Used to access the value of an attribute forwarded by the core service to Usage Monitoring service.
	Reported Usage Data Limits	Used to access the Data Limit Profile names for which usage was reported by the core (such as PGW) in the Session Update (such as CCR-UPDATE) message.
	Attribute in UM Request	Provides the following options: • dnn • operationType • UDR indicated Limit Ids

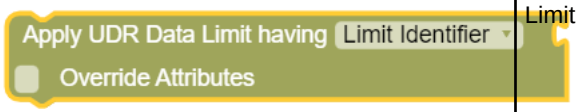
Block Icon	Block Name	Description
	Data Limit Profile Attribute	Used to access the properties of a Usage Monitoring Data Limit Profile configured on the Policy. The Data Limit Profile Attribute provides the following options: • Profile Type • Plan Type • Priority • UM Level • Usage Limit / Duration • Usage Limit / Volume Total • Usage Limit / Volume Uplink • Usage Limit / Volume Downlink • Reset Period / Periodicity • Reset Period / Max No. of Periods • Billing Day / Type • Billing Day / Day • Billing Day / Time • Data Rollover Profile • Inactivity Time • Allow Excess Usage • Excess Usage Limit / Percentage • Excess Usage Limit / Duration • Excess Usage Limit / Volume Total • Excess Usage Limit / Volume Uplink • Excess Usage Limit / Volume Downlink
	UDR Data Limit Attribute	Used to access the properties of a Usage Monitoring Data Limit provided by UDR. The UDR Data Limit Attribute provides the following options: • UM Level • Start Date • End Date • Usage Limit / Duration • Usage Limit / Volume Total • Usage Limit / Volume Uplink • Usage Limit / Volume Downlink • Reset Period / Periodicity • Reset Period / Max No. of Periods • Custom Attribute / <name>

Block Icon	Block Name	Description
	Usage Data Attribute	Used to access the properties of a Usage Monitoring Data object. The Usage Data Attribute block provides the following options: • UM Level • Allowed Usage / Duration • Allowed Usage / Volume Total • Allowed Usage / Volume Uplink • Allowed Usage / Volume Downlink • Consumed Usage / Duration • Consumed Usage / Volume Total • Consumed Usage / Volume Uplink • Consumed Usage / Volume Downlink • Consumed Usage Percentage / Duration • Consumed Usage Percentage / Volume Total • Consumed Usage Percentage / Volume Uplink • Consumed Usage Percentage / Volume Downlink • Reset Time • Activation Time • Last Reset Time • Reset Count • Custom Attribute / <name>
	Policy Tag	Used to access the Policy Decision Tags provided by Usage Monitoring service to Core Service.
	Set Grant Volume	Used to indicate a volume grant value. Units has the following options: • Percent • Bytes Source options: • Initial • Used • Remaining

Block Icon	Block Name	Description
	Set Grant Time	Used to indicate a time grant value. Units has the following options: • Percent • Seconds Source options: • Initial • Used • Remaining
	Apply Data Limit Profile	Selects a Data Limit Profile from the configured Data Limit Profiles. This blockly also presents the option to use any Data Limits provisioned on the UDR for the subscriber. The provisioned Data Limits can be any top-ups and/or passes. Those data limits can have an option to preempt the currently running data limit.

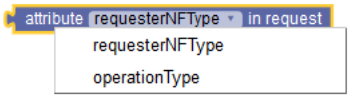
Block Icon	Block Name	Description
	Override Attribute	The Data Limit block represents the attributes inside the UM Data Limit. This block can be used along with Action blocks like "Override Attributes" to indicate which attributes to override. The value selected for this blockly is sent in the PRE response: • Usage Limit / Duration • Usage Limit / Total Volume • Usage Limit / Downlink Volume • Usage Limit / Uplink Volume • Priority • Start Date • End Date • Reset Period / Periodicity • Reset Period / Max No. of Periods • Billing Day / Type • Billing Day / Day • Billing Day / Time • Custom Attribute / <var> • Data Rollover Profile • Excess Usage Limit / Percentage • Excess Usage Limit / Duration • Excess Usage Limit / Total Volume • Excess Usage Limit / Downlink Volume • Excess Usage Limit / Uplink Volume
Figure 3-21 PCC Rule Hint 	PCC Rule Hint	This attribute is used with the Data Limit Profile block. It allows to access the value of PCCRuleHint from Data limit profile and apply the same in UMPolicyDecision in monitoring key.

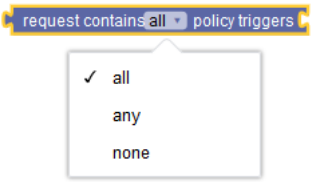
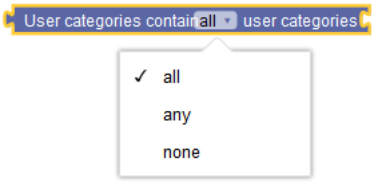
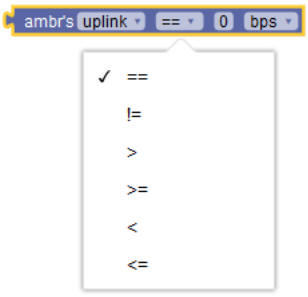
Block Icon	Block Name	Description
Figure 3-22 Volume Grant Params 	Volume Grant Parameters	Used to configure volume grants at PCC rule level.
Figure 3-23 Time Grant Params 	Time Grant Parameters	Used to configure time grants at PCC rule level.
Figure 3-24 Active Monitoring Key with PCCRuleHint 	Active Monitoring Key with PCCRuleHint	Selects a Monitoring key for the configured PCCRule from usage monitoring policy decision which fulfills the value from active monitoring with PccRuleHint attribute.

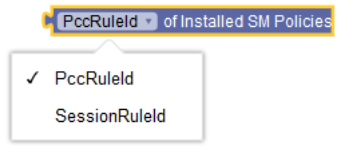
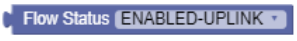
Block Icon	Block Name	Description
	Select Data Limit - Using Data Limit Selection Profile	Selects a Data Limit from the List of Data Limits provided by the UDR using a Selection Profile. The Override Attributes option allows to override: • Start Date • End Date • Usage Limit / Duration • Usage Limit / Total Volume • Usage Limit / Downlink Volume • Usage Limit / Uplink Volume • Priority • Excess Usage Limit / Percentage • Excess Usage Limit / Duration • Excess Usage Limit / Total Volume • Excess Usage Limit / Downlink Volume • Excess Usage Limit / Uplink Volume
	Sort Data Limits using Data Limit Sorting Profile	Sorts the selected Data Limits using the given sorting profile..
	Apply UDR Data Limit having	Selects a Data Limit from the List of Data Limits provided by the UDR using either a plan name. This blockly provides the following options: • Limit Identifier • Name • Custom Attribute
	Apply Tag with name and value	Used to indicate to the core service one or more identifiers (key value pair(s)) to take further actions such as QoS or Charging related decisions.
	Reset Usage Data	Instructs the Usage Monitoring service to reset the Usage Data for the Profile / Data Limit name mentioned.
	Disable Usage Monitoring	Disable usage monitoring for all or a specific data limit.

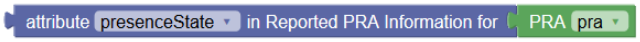
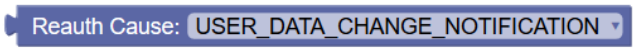
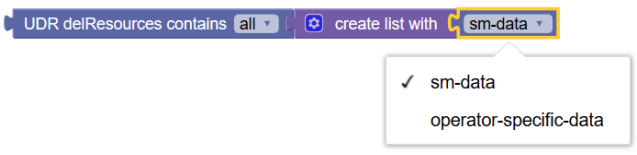
3.6 PCF-SM Category

The blocks for this category is available only when you select SM service while configuring the policy project.

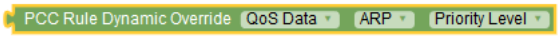
Block Icon	Block Name	Description
Constructs		
	For Each AF Flow Request	It loops through the Media Component and SubComponent Blocks comparing with Media Type Block.
Conditions		
	Request attributes	Sets the value to one of the JSON paths of drop-down list options. **Drop-down list options:** requesterNFType operationType
	Request Attributes in SMF	Sets the value to one of the JSON paths of drop-down list options. **Drop-down list options** : requesterNFType, operationType, gpsi, supi, accessType, ratType, pei, subsDefQos.5qi, subsDefQos.arp.priorityLevel, subsDefQos.arp.preemptCap, subsDefQos.arp.preemptVuln, subsDefQos.priorityLevel, dnn. **Note**: It is recommended to use Request attributes block, described in the next row, if you are selecting **requesterNFType** or **operationType** from the drop-down list.
	Rat Type	Sets the value to one of the drop-down list options of Rat Type. **Drop-down list options** : NR, NR_REDCAP, EUTRA, WLAN, VIRTUAL.
	app ID	

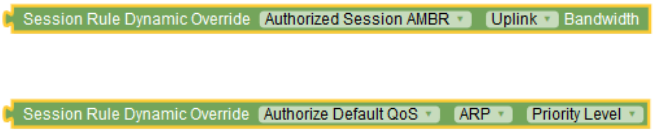
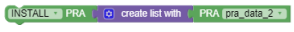
	Operation Type	Sets the value to one of the drop-down list options of Operation Type. **Drop-down list options** : CREATE, MODIFY, TERMINATE, REAUTH.
	PLMN Id	Compares the plmnId in the User Location Info received in SM Policy Create or Update request.
	Contains session rules	Compares the given list with the list of session rules previously delivered to the SMF and stored in the SM Policy Association.
	Contains policy triggers	Compares the policy triggers received in the SM Policy Update request with the given list of triggers.
	Contain user categories	Compares User Categories attribute fetched from UDR with a list of provided User Categories.
	sliceInfo	Compares the Slice Information received in SM Policy request.
	AMBR	Compares the AMBR received in the "subsSessAmbr" attribute in SM Policy request from SMF.

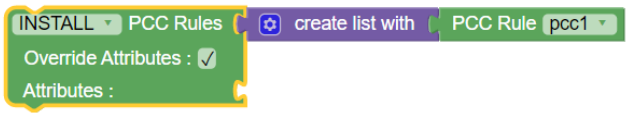
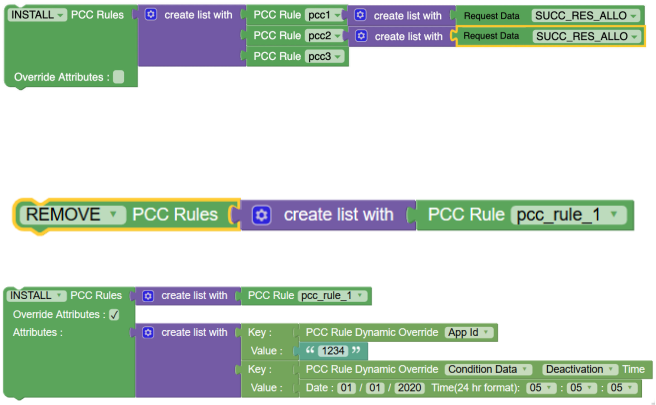
	Installed SM Policies	Retrieves the list of PCC Rules previously delivered to the SMF and stored in the SM Policy Association.
	Attribute in SM Policy Data	Retrieves data from the SM Policy Data (Subscriber Profile) fetched from UDR for a given S-NSSAI and DNN.
	Media Componet	Sets the value to one of the JSON path of drop-down list options. **Drop-down list options** : AF Application Id, Media Type, Media Component Number, Flow Status.
	Media Sub-Component	Sets the value to one of the JSON path of drop-down list options. **Drop-down list options** : Flow Usage, Flow Number, Flow Description, Flow Status, ToS Traffic Class.
	Media Type	Sets the value to one of the drop-down list options of Media Type. **Drop-down list options** : AUDIO, DATA, VIDEO, TEXT,CONTROL, APPLICATION, MESSAGE,OTHERS.
	Flow Usage	Sets the value to one of the drop-down list options of Flow Usage. **Drop-down list options:** RTCP, NO_INFO.
	Flow Status	Sets the value to one of the drop-down list options of Flow Status. **Drop-down list options:** ENABLED-UPLINK, ENABLED, ENABLED-DOWNLINK, DISABLED, REMOVED.

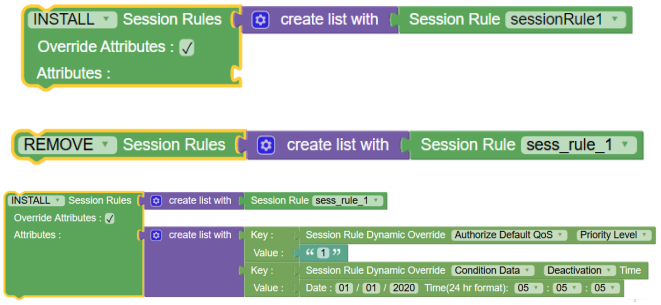
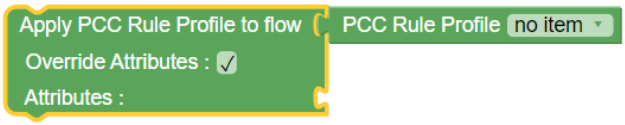
	Attribute in Reported PRA Information	Retrieves the value of `presenceState` attribute in Reported PRA information for specified PRAs. **Note**: Before accessing the `presenceState` attribute, it verifies the availability of the specified PRA and its Reported PRA information. If either of the two is missing, this block returns null value.
	NF Type	Allows operators to specify the type of network function. The following are the available drop-down list values: • SMF • AMF • BSF • NEF • AF • UDR • CHF
	Communication Mode	Allows operators to specify mode of communication. The available drop-down values are: • Synchronous • Asynchronous
	Presence State	Allows operators to specify the value for presence state. The supported values are: • IN_AREA • OUT_OF_AREA • UNKNOWN • INACTIVE
	Reauthorization Cause	Checks the value of the attribute - `reauthCause` of the policy request. The supported value is "USER_DATA_CHANGE_NOTIFICATION".
	UDR delete Resources	Checks the value of the attribute - `policyDataChangeNotification.delResources` of the policy request. The supported values are "sm-data" and "operator-specific-data".

Actions

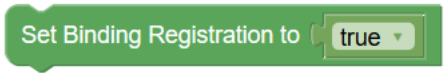
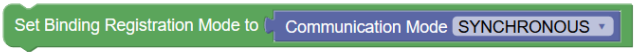
 	PCC Rule Dyanamic Override	This block is used as a key to create a pair of {attribute: value}to override PCC rule attributes in real-time. This block is used with the **Key Value** block. The drop-down list values, auto-populated in the block, are taken from the PCC Rule configuration Page.**Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **PCC Rule** Currently, operators can use this block to override the values for the following parameters: • App Id • Content Version • Precedence **Note**: This attribute specifies the precedence of the PCC rule among all PCC rules associated with the PDU session. • AF Signalling Protocol • Application Relocation • QoS Data • Traffic Control Data • Charging Data • Condition Data **Important**: If SM service does not override attributes provided in the policy: • Verify if the response from PRE contains all parameters specified in the policy. • Verify if SM service logs contain the following: `Invalid format of OverriddenAttr received from PRE.`

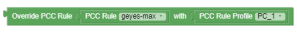
		It indicates a problem parsing PRE response for overridden attributes.
 	Session Rule Dynamic Override	This block is used as a key to create a pair of {attribute: value}to override session rule attributes in real-time. This block is used with **Key Value** block. The drop-down list values, auto-populated in the block, are taken from the Session Rule configuration Page.**Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Session Rule** Currently, operators can use this block to override the values for the following parameters: • Authorized Session AMBR • Condition Data • Authorize Default QoS
	Apply Session Rule	It modifies the session Rule that is atttached after the "Create list with" Block.
	Install/ Remove Policy Trigger	This block performs **Install / Remove** of the Policy Trigger. The Policy Trigger item to install/remove is picked from the set of hardcoded drop-down list values of Policy Trigger Block.
	Install/ Remove PRA	This block performs **Install / Remove** of the PRA. The PRA item to install/ remove is picked from the configuration Page. (PCF→ Policy Configurations → Common → Presence Reporting Area)

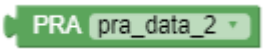
 **Figure 3-25 Install PCC Rule with SRA** 	Install/ Update/ Remove PCC Rules with Override Attributes	This block can be used to create, modify, or remove specific PCC Rules. To update or override PCC rule attributes dynamically, you can drag and add **create list with** block to create pairs of {key:value} attributes using the **Key Value** block. The PCC rule attributes that you can update dynamically can be selected from the drop-down. You can select **SUCC_RES_ALLO** for **Request Data** to install PCC rules with Successful Resource Allocation (SRA) attribute. **Note**: Override Attributes checkbox is disabled if you select the **Remove** option from the drop-down. **Important**: When the PCC rule is initially provisioned, PCF must supply **flowInfos** or **appId** attribute. If it supplies appId, then PCF does not update **appId** attribute later provided by the user.

	Install/ Update/ Remove Session Rules with Override Attributes	This block can be used to create, update, and remove specific session rules. To update or override session rule attributes dynamically, you can drag and add **create list with** block to create pairs of {key:value} attributes using the **Key Value** block. **Note**: Override Attributes checkbox is disabled if you select **Remove** option from the drop-down. The Session rule attributes that you can update dynamically can be selected from the drop-down.
	Apply PCC Rule Profile to flow with Override Attributes	It applies PCC rule with specified PCC Rule Profile. To update or override attributes dynamically, you can drag and add **create list with** block to create pairs of key:value attributes using the **Key** block.

	Remove PCC Rules	This block removes PCC Rules as per the option selected in drop-down list by the user. **Drop-down list options:** ALL DYNAMIC PRE_DEFINED NON_CONDITIONED CONDITIONED If you select **DYNAMIC** from the drop-down value, SM service removes the following Dynamic PCC rules: • Defined on CM for SM policy data and installed by previous policy decisions for the specified SM Policy association • Derived and installed for AF flow If you select **PRE_DEFINED** from the drop-down value, SM service removes the pre-defined PCC rules defined on CM for SM policy data, and installed by previous policy decisions for the specified SM policy association. When removing PCC Rules in bulk, the policy also removes reference data only if the data is not referred by any PCC rule except the ones being deleted. To view all the PCC rules removed as part of a policy action, you can refer to the Info level policy logs. **Important**: If you are importing policies from older versions (previous to 1.8.0), delete the existing **Remove PCC Rules** blocks, and drag it from blockly library again after upgrade.

	Remove Session Rules	This block performs Remove of Session Rules as per condition in drop-down list. **Drop-down list options:** REMOVE_ALL, REMOVE_NON_CONDITIONED, REMOVE_ALL_CONDITIONED.
	Set Binding Registration	Specifies whether to enable or disable the binding operation. The supported values are **True** and **False**. **Note**: This policy action can read values from a policy table. **Note**: If **Binding Operation** flag is disabled on the service configurations page on CNC Console (Policy > Service Configurations > PCF Session Management), no binding operation is performed, irrespective of the value of policy decision.
	Set Binding Registration Mode	Specifies whether to set binding registration mode as synchronous or asynchronous. Note: This policy action can read values from a policy table.

	Policy Trigger	Sets the value to one of the drop-down list options of Policy Trigger. **Drop-down list options:** PLMN_CH, RES_MO_RE, AC_TY_CH, UE_IP_CH, UE_MAC_CH, AN_CH_COR, US_RE, APP_STA, APP_STO, AN_INFO, CM_SES_FAIL, PS_DA_OFF, DEF_QOS_CH, SE_AMBR_CH, QOS_NOTIF, NO_CREDIT, PRA_CH, SAREA_CH, SCNN_CH, RE_TIMEOUT, RES_RELEASE, SUCC_RES_ALLO, RAT_TY_CH, REF_QOS_IND_CH, NUM_OF_PACKET_FILTER, UE_STATUS_RESUME, UE_TZ_CH, SCELL_CH.
	PCC Rule	sets the value to one of the drop-down list options of PCC Rule. The drop-down list Values is picked from configuration Page. (PCF→ Policy Configurations → SM Policy → PCC Rule)
	PCC Rule Profile	sets the value to one of the drop-down list options of PCC Rule Profile. The drop-down list Values is picked from configuration Page. (PCF→ Policy Configurations → SM Policy → PCC Rule Profile)
	Override PCC Rule	It appends the "PCC Rule" and "PCC Rule Profile" Block and creates an Object {"pccRuleId": ('geyes-max'), "id":('pc_1')} and returns it.

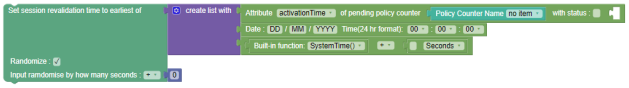
	Session Rule	sets the value to one of the drop-down list options of Session Rule. The drop-down list Values is picked from configuration Page. (PCF→ Policy Configurations → SM Policy → Session Rule)
	Ovverride Session Rule	It appends the "Session Rule" and "Session Rule Profile" Block and creates an Object {"sessRuleId": 'sm-data', "sessRuleProfileId": ('session_rule_profile_2')} and returns it.
	Session Rule Profile	Sets the value to one of the drop-down list options of Session Rule profile. The drop-down list Values is picked from configuration Page. (PCF→ Policy Configurations → SM Policy → Session Rule Profile)
	Presence Reporting Area	Sets the value to one of the drop-down list options of PRA. The drop-down list Values is picked from configuration Page. (PCF→ Policy Configurations → Common → Presence Reporting Area)

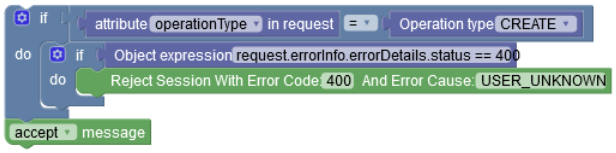
	Release Session	Directs the SM service to trigger session termination notification and thus releasing a policy association. When SM service receives this action, it ignores all other actions. **Note**: SM Service only releases a policy association triggered by `UserDataChangeNotification`. That is, session terminate notification is triggered based on: • change notification on CHF counters. • policies in PCF in response to an UPDATE from SMF. • any upate notification from UDR.

Figure 3-26 Set Revalidation Time

	Set Revalidation Time	Revalidation time defines the period within which the Session Management Function (SMF) triggers the PCC rule request towards PCF for an established PDU Session. You can use this action block to set the session revalidation time to a specific year, month, day, or time. In addition, you can check the Randomize checkbox to select a random revalidation time from the defined range. When you select the Randomize checkbox, you need to define the range for revalidation time. You can define the range by using the number block (under Public category) for specifying the seconds and selecting any of the following values from the dropdown list: • "**+**": It adds the specified seconds to the time entered. • "**-**": It subtracts the specified seconds from the time entered. • "**+/-**": The range is defined by [Time entered - specified seconds] to [Time entered + specified seconds]. If you select the Randomize option, the following message is printed in the Policy runtime logs: {"messageTimestamp":"2022-01-28T10:56:33.148Z","logLevel":"WARN","pid":9700,"workerId":1,"fileName":"..\\..\\engine\\policies\\pcf-sm\\test1\\main.js","lineNo":"46","message":"Randomization of revalidation

		time choosen by seconds"} If you input anything other than a number for randomization, the following error is printed in the logs: "message":"Error!! Entered seconds is not a number for randomization !! Please enter number in seconds field." **Note**: On upgrading to Policy 22.1.0 or higher, the **Set revalidation time** block is upgraded automatically in the existing policies.

Figure 3-27 Set session revalidation time to earliest of 	Set Session Revalidation time to earliest of	Set session revalidation time to the earliest of returns the earliest time from the following list: • Time in the specified policy counter ID or IDs • Time defined in the `Seconds/ Minutes/ Hours/Days` format from the time when a policy is executed • Specific time in `hh:mm` format (limited to 15-minute intervals) on a specific day of the week using either *SYSTEM TIME* or *UTC TIME* time-zone. • Random time between a time range This action block is Policy table compliant. In addition, you can check the Randomize checkbox to select a random revalidation time from the time range. You can define the range by using the number block (under Public category) for specifying the seconds and selecting any of the following values from the dropdown list: • "**+**": It adds the specified seconds to the time entered. • "**-**": It subtracts the specified seconds from the time entered. • "**+/-**": The range is defined by [Time entered - specified seconds] to [Time entered + specified seconds]. If you select the Randomize option, the following message is printed in the Policy runtime logs:

		{"messageTimestamp":"2022-01-25T08:10:41.698Z","logLevel":"WARN","pid":14692,"workerId":2,"fileName":"lib\\services\\sm_core-service.js","lineNo":"25","message":"**Applying randomization on earliest time**} If you input anything other than a number for randomization, the following error is printed in the logs: "message":"Error!! Entered seconds is not a number for randomization !! Please enter number in seconds field." **Note:** Configuring a session revalidation time using 'Set session revalidation time to earliest of' action results in the installation of the RE_TIMEOUT trigger.
Figure 3-28 Reject Session with Error Code and Error Cause  **Figure 3-29 Example**  	Reject Session with Error Code and Error Cause	Allow to reject the session with a custom error code and a custom error cause. **Note:** If the **Error Cause** field is empty, only the **Error Code** will be sent back.

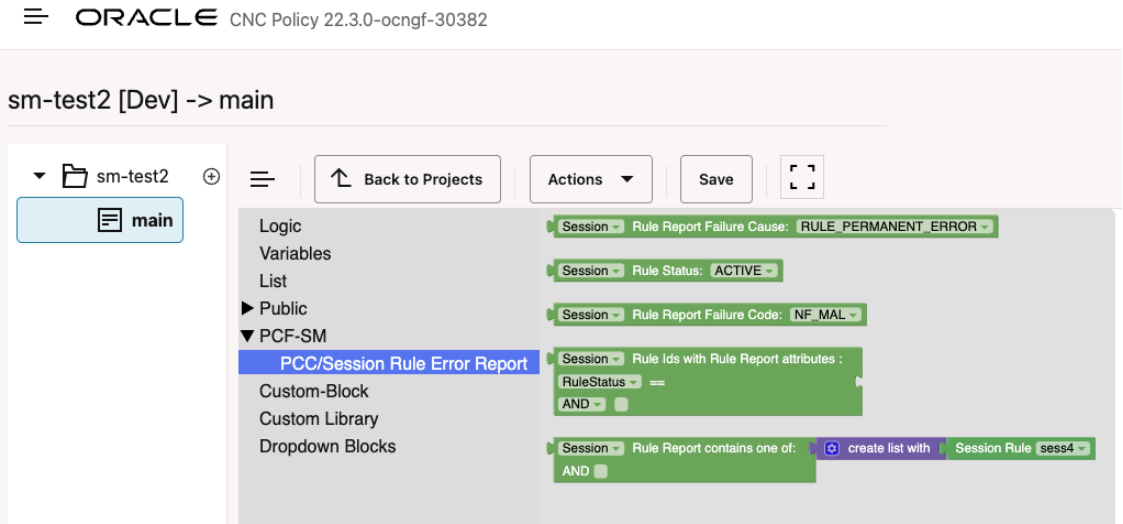
3.6.1 PCC/Session Rule Error Report

The blocks for this category is available only when you select PCC/Session Rule Error Report under PCF-SM service while configuring the policy project.

Block Icon	Block Name	Description
Constructs		
	PCC/Session Rule Status	The rule status can be combined with policy conditions "RuleIds" and "Rulereports" to specify rule status "Active" or "Inactive"
	PCC/Session Rule Failure Code	sessRuleFailureCode can be combined with policy conditions "RuleIds" and "Rulereports" to check the failure code values
	PCC/Session Failure Cause	Returns Failure Cause values ["RULE_PERMANENT_ERROR", "RULE_TEMPORARY_ERROR"] used along with two condition blocks "PCC/Session Rule Ids" and PCC/Session Rule report". Checks the cause/ failureCause attribute received in errorReport or partialSuccessReport. Checks the sessRuleFailureCode attribute received in sessRuleReports.
	PCC/Session RuleIds from rulereport	Used to get the ruleIds received in ruleReports or sessRuleReports with condition matching for ruleStatus, ruleFailureCode or sessRuleFailureCode and failureCause.
	PCC/Session Rule Report	This condition blockly matches with configured ruleIds, ruleStatus, sessRuleFailureCode and failureCause and returns true or false.

Sample block for PCC/Session Rule Error Report:

Figure 3-30 Sample block for PCC/Session Rule Error Report



3.7 PCF UE Policy

This section describes the blocks that operators can access while configuring PCF UE Policy projects.

Table 3-1 UE Policy Blocks

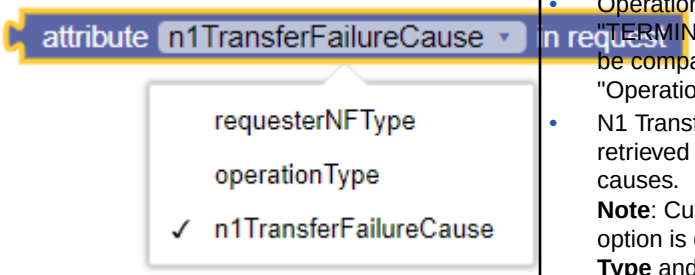
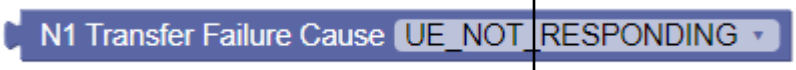
Block	Description
Figure 3-31 Attribute in Request Type 	Allows the policy writer to retrieve the following: • Requester NF Type (e.g. AMF etc.) - The value retrieved can be compared to the enumeration block "NF Type". • Operation Type (e.g. "CREATE", "UPDATE", "TERMINATE" etc.) - The value retrieved can be compared to the enumeration block "Operation Type". • N1 Transfer Failure Cause - The value retrieved can be compared to the failure causes. **Note**: Currently, N1 Transfer Failure Cause option is deprecated for **Attribute in Request Type** and is available under **Attribute in AMF Request**.
Figure 3-32 N1 Transfer Failure Cause 	This blockly allows the policy writer to identify the N1 transfer failure causes such as `UE_NOT_RESPONDING` in the messages.

Table 3-1 (Cont.) UE Policy Blocks

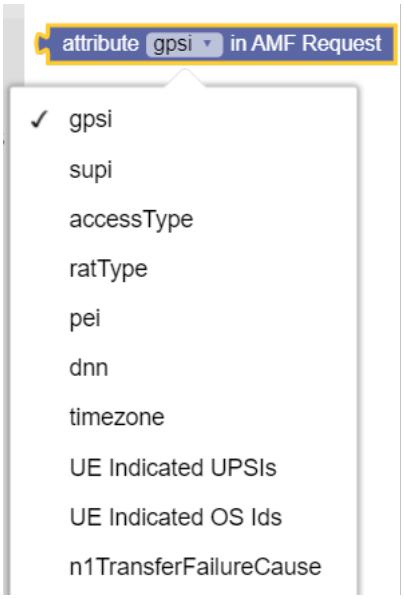
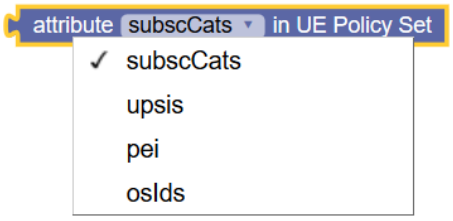
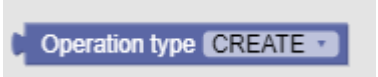
Block	Description
Figure 3-33 Attribute in AMF Request 	Retrieves the specified attribute value from the incoming request message. The available options are: • gpsi • supi • accessType • ratType • pei • dnn • timezone • UE Indicated UPSIs • UE Indicated OS Ids • n1TransferFailureCause
Figure 3-34 Attributes in UE Policy Set 	Retrieves the specified attribute value from the UE Policy Set (as obtained from UDR). The available options are: • subsCats • upsis • pei • osIds
Figure 3-35 Operation Type 	Allows operators to specify the Operation Type. The supported values are CREATE, UPDATE, TERMINATE, and NOTIFICATION.

Table 3-1 (Cont.) UE Policy Blocks

Block	Description
Figure 3-36 RatType 	Allows operators to specify the value of RAT Type. The supported values are : • NR • WLAN • EUTRA • VIRTUAL • NR_REDCAP
Figure 3-37 AccessType 	Allows operators to specify the Access Type. The supported values are 3GPP Access and Non 3GPP Access.
Figure 3-38 PLMN ID 	Allows operators to specify MCC or MNC of plmnid in the following supported values: Serving PLMN Id, EUTRACelld, EUTRA tracking Area Code, NR Celld, NR tracking Area Code, eutraLocation.tai, ecgi, globalNgenbld, nrLocation.tai, ncgi, and globalGnbld.
Figure 3-39 UPSI Values 	Allows the operators to specify the value of the UPSI.
Figure 3-40 UPSI 	This block allows the policy writer to select a UPSI configured using the **Policy > Policy Data Configurations > PCF UE Policy > UPSI** screen.

Table 3-1 (Cont.) UE Policy Blocks

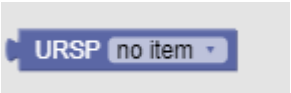
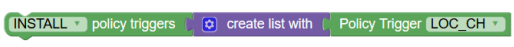
Block	Description
Figure 3-41 URSP 	This block allows the policy writer to select a URSP configured using the **Policy > Policy Data Configurations > PCF UE Policy > URSP Rule** screen.
Actions	
Figure 3-42 Install/Remove UPSI 	Allows the policy writer to install or remove UPSIs that are already configured in GUI on the UPSI screen (**Policy > Policy Data Configurations > PCF UE Policy > UPSI**). Click the drop-down menu of **UPSI** block to select desired UPSI Ids.
Figure 3-43 Install/Remove UPSIs from UE Policy Set 	Allows the policy writer to install or remove UPSIs retrieved from the UDR in the UE Policy Set (upsis attribute). **Notes**: • The UPSIs in the UePolicySet.upsis attribute MUST be represented in string format "<mcc>-<mnc>-<upsc>" where mcc is an integer containing the Mobile Country Code, mnc is an integer containing the Mobile Network Code and upsc is an integer containing the Ue Policy Section Code. E.g. "401-301-1234" • A corresponding UPSI must be configured using the **Policy > Policy Data Configurations > PCF UE Policy > UPSI** screen having the same MCC, MNC and UPSC as that received from UDR. The name of the UPSI in the PCF configuration can be anything convenient. • PCF shall use the upsis received from UDR to pick the URSP rules from the PCF configuration and deliver the same to the UE.
Figure 3-44 Install Policy Trigger 	This action block allows the policy writer to install or remove policy triggers. The Policy Trigger value to install/remove is automatically populated in the form of drop-down with the **Policy Trigger** block. **Note**: Currently, the only supported policy trigger value is **LOC_CH** (change in location).

Table 3-1 (Cont.) UE Policy Blocks

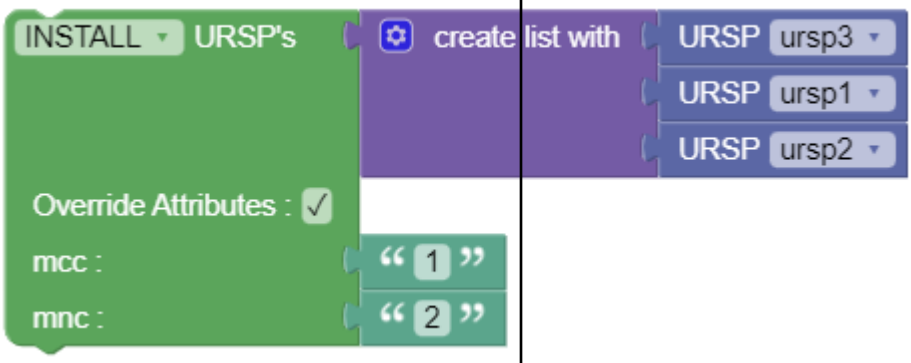
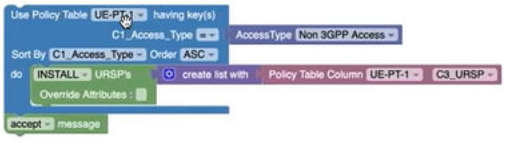
Block	Description
Figure 3-45 Install/Remove URSP's 	Allows the policy writer to install or delete URSP rules for delivery using the fragmentation feature.
Figure 3-46 Remove UPSIs 	Allows the policy writer to remove UPSI from the UDR in the UE Policy Set.
Single URSP **Figure 3-47 Policy Table Column Blockly**  **Figure 3-48 Example: Policy Table Column, an URSP** 	This block allows the policy writer to create an Policy URSP data type column, while configuring the policy project using the policy table. For example: Use Policy Table UE-PT1 whose access type is Non-3GPP Access and Install URSPs with Policy Table UE-PT1 with column c3_URSP (single URSP).

Table 3-1 (Cont.) UE Policy Blocks

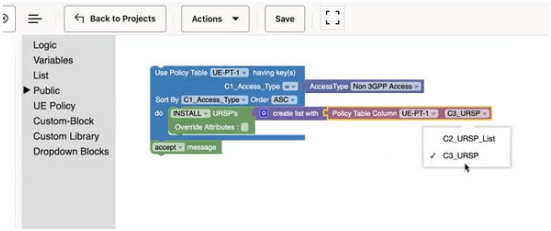
Block	Description
URSP List **Figure 3-49 Example: Policy Table Column, URSP List** 	This block allows the policy writer to create an Policy URSP `List` data type column, while configuring the policy project using the policy table. For example: Use Policy Table UE-PT1 whose access type is Non-3GPP Access and Install URSPs with Policy Table UE-PT1 with column c3_URSP_List (an URSP List).
Figure 3-50 Retransmit UPSI 	This blockly allows the policy writer to either re-transmit some of the rejected UPSI or to abort the transmission entirely.
Figure 3-51 Skip current fragment 	This blockly allows the policy writer to skip the current fragment transmission, immediately starting the next fragment transmission or ending the transaction in case there is no next fragment.
Figure 3-52 Abort N1 Notify Transmission 	This blockly immediately ends the transaction and won't continue the N1 transmission.

Table 3-1 (Cont.) UE Policy Blocks

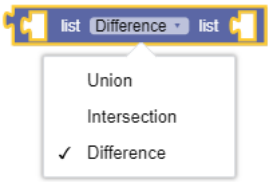
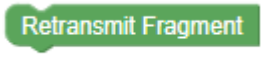
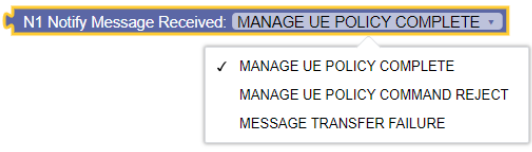
Block	Description
Figure 3-53 UPSI List 	**Note** The List blockly is used for setting operation on two lists. It can be used for general cases in addition to the operation on UPSI lists. The List operation is used while finding the delta between the UPSI's ID list that is currently configured in PCF, the UPSI's that are sent on UE Policy Registration and the UPSIs that are on UDR. Allowed values: • Union: Displays the list of all the UPSI IDs that are present in two separate lists. • Intersection: Displays the list of UPSI IDs that are common (intersection) in two separate lists. • Difference: Displays the list of UPSI IDs that contain the difference of the two separate lists.
Figure 3-54 Retransmit Fragment 	This blockly allows the policy writer to retransmit the whole n1 fragment.
Condition Blocks	
Figure 3-55 N1 Notify Message Received 	This blockly allows the policy writer to identify the following N1Notify messages: • MANAGE UE POLICY COMPLETE • MANAGE UE POLICY COMMAND REJECT • MESSAGE TRANSFER FAILURE

Table 3-1 (Cont.) UE Policy Blocks

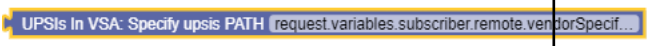
Block	Description
Figure 3-56 UPSIs attribute path 	**UPSI's in VSA: Specify upsi PATH** condition returns the UPSIs attribute path in the request. **Figure 3-57 UPSI's attribute path in VSA - Example**  The above example returns the UPSIs attribute path in VSA as: `request['variables']['subscriber']['remote']['vendorSpecific-012591']['consumerAttrs']['blobValue']['upsis']` **Note**: The PATH text must be either the dotted notation or the array notation and must not mix these two together.

Table 3-1 (Cont.) UE Policy Blocks

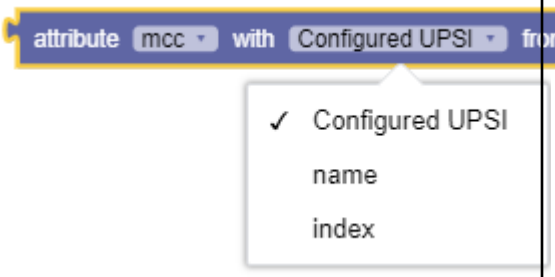
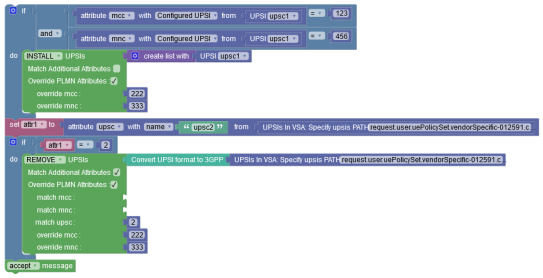
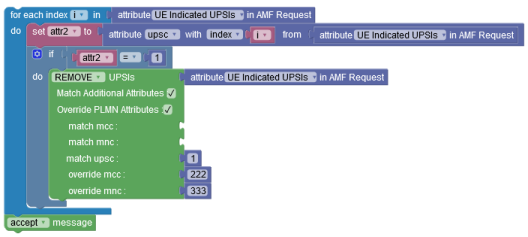
Block	Description
Figure 3-58 Get Configured UPSIs/ UPSI Name/ UPSI Index 	**with** condition allows to retrieve configured UPSI from PCF, or UPSI name, or UPSI index for the specified attribute (mcc/mnc/upsc/ursp) from the list of UPSIs or individual UPSI plugged in the last section of the blockly. **Example for Configured UPSIs and UPSI Name**:  In this example, the first part of the blockly will install the "upsc1" upsi if its mcc equals to 123 and mnc equals to 456 and override its PLMN to be 222-333. Similar for the second part, it will assign a variable called attr1 with the attribute of upsc from the UPSI which has the name "upsc2" on the VSA UPSIs list, and if this value is equal to 2, it will remove this UPSI and will override its PLMN to be 222-333. **NOTE:** In this case, when searching by name, we will check of the list that are on VSA request and if it exist on the PCF Configured UPSIs, it will return the given attribute, so here we check for the UPSI with name "upsc2" which is in the list of the VSA UPSIs and it exists also as a configured UPSI in PCF, then we procced with the validation. **Example for UPSI Index**:  This example loops on all the UPSIs that are located on AMF request. It allows to access an attribute from specific UPSI on AMF request. This Policy checks if any of the UPSIs on the list has its UPSC as 2.

Table 3-1 (Cont.) UE Policy Blocks

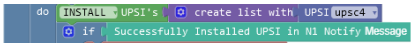
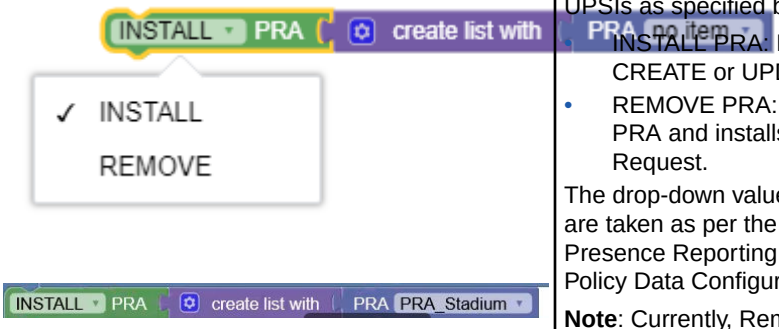
Block	Description
	If found, it removes the corresponding UPSI and overrides its PLMN to be 222-333.
Util Blocks	
Figure 3-59 Successfully Installed UPSI in N1 Notify Message 	This blockly allows to notify the successfully installed UPSI received in N1N2 notification. The successfully installed UPSI will only be available in the blockly when they are installed using the install UPSIs blockly.
Figure 3-60 Rejected UPSI in N1 Notify Message 	This blockly allows the policy writer to iterate over the rejected UPSI when the N1 Notify message comes as MANAGE UE POLICY COMMAND REJECT.
Figure 3-61 Retransmit count for UPSI 	This blockly allows the policy writer to get the current retransmission count for a specific UPSI, allowing the policy writer to control how many times the retransmission has happened.
	Installs or removes elements such as PRAs or UPSIs as specified by the operator. • INSTALL PRA: Installs the specified PRA on CREATE or UPDATE request. • REMOVE PRA: Removes previously installed PRA and installs different PRA on UPDATE Request. The drop-down values, auto-populated in the block, are taken as per the configuration on PCF Presence Reporting Area page under Common Policy Data Configurations. **Note**: Currently, Remove all request triggers functionality is not yet supported.

Table 3-1 (Cont.) UE Policy Blocks

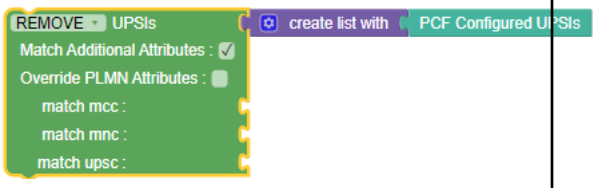
Block	Description
Figure 3-62 Install UPSIs  **Figure 3-63 Remove UPSIs** 	Install/Remove UPSIs with/without matching specific attribute of mcc, mnc and upsc. It also supports the checkbox to override PLMN for INSTALL/REMOVE.
Figure 3-64 Retransmit count for URSP 	This blockly allows the policy writer to get the current re-transmission count for a specific URSP, allowing the policy writer to control how many times the re-transmission has happened.
Figure 3-65 Rejected URSP in N1 Notify Message 	This blockly allows the policy writer to iterate over the rejected URSP when the N1 Notify message comes as MANAGE UE POLICY COMMAND REJECT.
Figure 3-66 N1 fragement retransmit count 	This blockly allows the policy writer to get the current re-transmission count of the whole N1 fragment. Using this the policy writer supervises number of retransmission occurrences.

Table 3-1 (Cont.) UE Policy Blocks

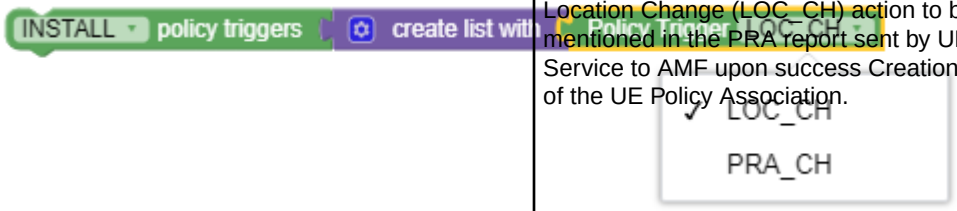
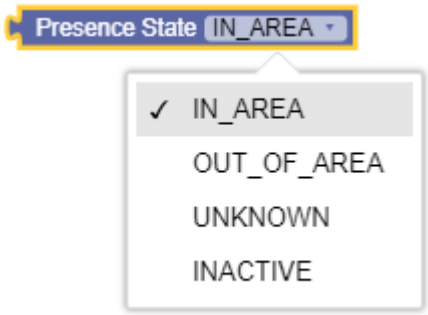
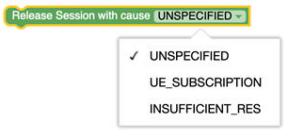
Block	Description
	Specifies if it is the PRA Change (PRA_CH) or the Location Change (LOC_CH) action to be mentioned in the PRA report sent by UE Policy Service to AMF upon success Creation or update of the UE Policy Association.
	Indicates the presence state of the UE: • IN_AREA: UE is present in the specified Presence Reporting Area. • OUT_OF_AREA: UE is not present in the specified Presence Reporting Area. • UNKNOWN: The presence status of the UE in the specified Presence Reporting Area is unknown or not available. • INACTIVE: The Presence Reporting Area is unavailable or not supported.
	Sets the value to one of the drop-down list options of PRA. The drop-down list Values is picked from configuration Page. (PCF→ Policy Configurations → Common → Presence Reporting Area)
	Indicates current presence status of the UE in a Presence Reporting Area, and notifies that the UE enters/leaves the Presence Reporting Area.
Figure 3-67 PCF Configured UPSIs 	**PCF Configured UPSIs** utility used with **create list with** block to generate a list of all configured UPSIs in PCF.
Figure 3-68 Convert UPSI Format to 3GPP 	Converts UPSI in format "mcc-mnc-upsc" or UPSI configuration name in PCF such as "upsi01" to 3GPP format. This utility is used with **UPSIs in VSA** block. For example: 

Table 3-1 (Cont.) UE Policy Blocks

Block	Description
Figure 3-69 UDR delResources contains 	Checks the value of the attribute - `policyDataChangeNotification.delResources` of the policy request. The supported values are: • am-data • sm-data • ue-policy-set • operator-specific-data For example: **Figure 3-70 Example usage of UDR delResources contains** 
Figure 3-71 Release Session with cause 	PolicyAssociationReleaseCause can have: **Table 3-2 PolicyAssociationReleaseCause** Enumeration value: UNSPECIFIED — Description: This value is used for unspecified reasons. Enumeration value: UE_SUBSCRIPTION — Description: This value indicates that the policy association needs to be terminated as the subscription of UE has changed. Enumeration value: INSUFFICIENT_RES — Description: This value indicates that the server is overloaded and needs to abort the policy association.
Figure 3-72 Release Session without cause 	Directs the AM/UE service to trigger session termination notification and thus releasing a policy association. When AM/UE service receives this action, it ignores all other actions.

3.8 PCF-AM Blocks

This section describes the blocks that operators can access while configuring PCF AM Policy projects.

Table 3-3 AM Policy Blocks

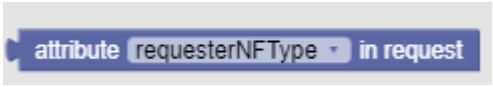
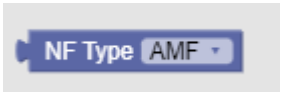
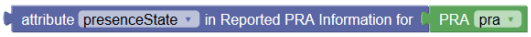
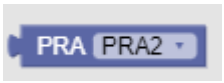
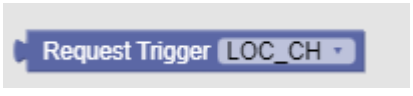
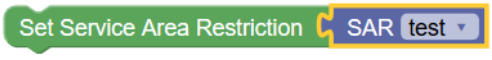
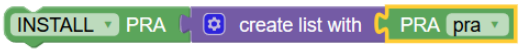
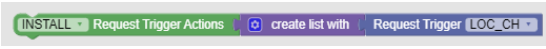
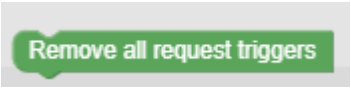
Block	Description
	Retrieves the value of requester NFType attribute in request.
	Retrieves the value of SUPI attribute in AMF request.
	Allows operators to specify the value of RAT Type. The supported values are NR, NR_REDCAP, WLAN, EUTRA, and VIRTUAL.
	Allows operators to specify the NF Type. The supported values are AMF, SMF, BSF, NEF, AF, UDR, and CHF.
	Allows operators to specify the Operation Type. The supported values are CREATE, UPDATE, DELETE, NOTIFICATION, UPDATE_NOTIFY, and TERMINATE_NOTIFY.
	Allows operators to specify MCC or MNC of plmnid in the following supported values: eutraLocation.tai, ecgi, globalNgenbld, nrLocation.tai, ncgi, globalGnbld, and negaLocation.n3gppTai.
	Allows operators to specify Restriction Type as ALLOWED_AREAS or NOT_ALLOWED_AREAS.
	Retrieves the service area restriction values, created through **Service Area Restriction** screen on CNC Console.
	Retrieves the value of `presenceState` attribute in Reported PRA information for specified PRAs. **Note**: Before accessing `presenceState` attribute, it verifies the availability of the specified PRA and its Reported PRA information. If either of the two is missing, this block returns null value.
	Retrieves the PRA values. The supported values are PRA1 and PRA2.
	Retrieves the Request Trigger values. The supported values are LOC_CH, PRA_CH, SERV_AREA_CH, and RFSP_CH.
Actions	
	Installs Service Area Restriction, specified by the operator.
	Sets a value for RFSP Index.

Table 3-3 (Cont.) AM Policy Blocks

Block	Description
	Installs or removes list of PRAs, specified by the operator. The drop-down values, auto-populated in the block, are taken from the PCF Presence Reporting Area configuration Page (**Policy** > **Policy Data Configurations** > **Common** > **PCF Presence Reporting Area**).
	Installs or removes list Request Trigger Actions, specified by the operator.
	Removes all request triggers.

3.9 PDS Category

This section provides information about blocks that can be used to write policies for Policy Data Source service.

Table 3-4 PDS Blocks

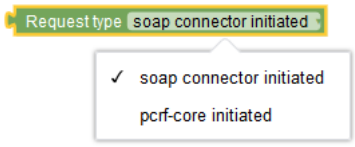
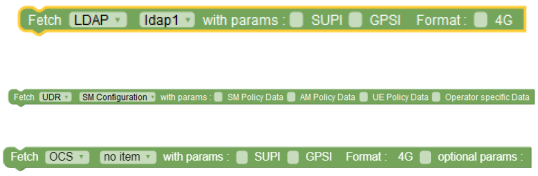
Block Image	Description
Conditions	
	Specifies the first value and the last value of a SUPI range.
	Specifies the first value and the last value of a GPSI range.
	Specifies the pattern representing the set of SUPI's belonging to this range.
	Specifies the pattern representing the set of GPSI's belonging to this range.
	Specifies whether the incoming request message is coming from soap connector or PCRF core.
Actions	

Table 3-4 (Cont.) PDS Blocks

Block Image	Description
	This blockly action allows policy writers to retrieve resourceTypes from specified datasource. When the user selects LDAP from the drop-down menu, retrieval takes place through LDAP datasource. Use the drop-down menu to select LDAP ID configured using the **Policy**, and then **Service Configurations**, and then **PDS Settings** screen in CNC Console. In addition, user can select parameters - SUPI or GPSI to perform the lookup. When the 4G checkbox is selected, the lookup is done using IMSI or MSISDN. When UDR is selected from the drop-down menu, the policy retrieves UDR datasource and the default configurations, configured using **Policy**, and then **Service Configurations**, and then **PCF User Connector** screen. In addition, user can use the checkboxes to retrieve multiple resourceTypes at once. When CHF is selected from the drop-down menu, the policy retrieves CHF datasource and the default configurations, configured using **Policy**, and then **Service Configurations**, and then **PCF User Connector** screen. When OCS is selected from the drop-down menu, the policy retrieves OCS datasource and the default configurations, configured using **Policy** > **Diameter Configurations** > Peer Nodes page. By default, OCS supports 4G format.

3.10 PCRF-Core

The policy wizard supports a large number of conditions that can be used for constructing policy rules. To help you find the conditions you want, the conditions are organized into different categories.

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

3.10.1 Conditions

This section provides information on policy conditions available for PCRF Core service.

The enforcement session is one of *an IP-CAN session*

This policy condition, as shown in the following image, triggers a policy that evaluates the type of the enforcement session.

The following are the valid values that can be selected from the drop-down field:

- **an IP-CAN session** (default)
- **a gateway control session**
- **a DPI enforcement session**
- **an S9 sub-session**
- **an S9 session**

Mobile session includes Sponsored Connectivity

The Mobile session *includes* or *does not include* Sponsored Connectivity policy condition, as shown in the following image, triggers a policy that evaluates whether or not the mobile session supports sponsored data connectivity. This condition supports sponsored data connectivity for both Gx and Rx requests.

Reauthorization Reason

The **Reauthorization Reason** policy condition, as shown in the following image, compares reauthorization reason in request received by PRE with the value specified in the policy condition.

User can select any of the following valid values from the Reauthorization drop-down field:

- REASON_DEFAULT
- REASON_AUDIT
- REASON_TOD
- REASON_LI
- REASON_RELEASE_SESSION
- REASON_POLICY
- REASON_NOTIFICATION
- REASON_RETRY
- REASON_AF
- REASON_OCS_NOTIFICATION
- REASON_RECONCILE
- REASON_USER_SCHEDULED_TASK
- REASON_REVALIDATION_TIMEOUT
- REASON_SY_SESSION_TERMINATION_BY_OCS

request *supports* feature *name*

The **request *supports or does not support* feature *name*** policy condition, as shown in the following image, determines whether the request supports or does not support a specified feature respectively.

For the name of the feature, this policy condition supports a comma-delimited list of values.

where the event trigger is one of

This policy condition, as shown in the following image, triggers a policy that is only evaluated for a specific event trigger type.

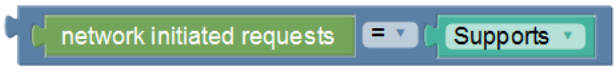
User can select any one of the following valid values from **event trigger** drop-down field:

- SGSN_CHANGE
- QOS_CHANGE
- RAT_CHANGE
- TFT_CHANGE
- PLMN_CHANGE
- LOSS_OF_BEARER
- RECOVERY_OF_BEARER
- IP_CAN_CHANGE
- GW_PCEF_MALFUNCTION
- RESOURCES_LIMITATION
- MAX_NR_BEARERS_REACHED
- QOS_CHANGE_EXCEEDING_AUTHORIZATION
- RAI_CHANGE
- USER_LOCATION_CHANGE
- NO_EVENT_TRIGGERS
- OUT_OF_CREDIT
- REALLOCATION_OF_CREDIT
- REVALIDATION_TIMEOUT
- UE_IP_ADDRESS_ALLOCATE
- UE_IP_ADDRESS_RELEASE
- DEFAULT_EPS_BEARER_QOS_CHANGE
- AN_GW_CHANGE
- SUCCESSFUL_RESOURCE_ALLOCATION

- RESOURCE_MODIFICATION_REQUEST
- UE_TIME_ZONE_CHANGE
- TAI_CHANGE
- ECGI_CHANGE
- CHARGING_CORRELATION_EXCHANGE
- APN_AMBR_MODIFICATION_FAILURE
- USER_CSG_INFORMATION_CHANGE
- USAGE_REPORT
- DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE
- USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE
- USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE
- APPLICATION_START
- APPLICATION_STOP
- ADC_REVALIDATION_TIMEOUT
- ACCESS_NETWORK_INFO_REPORT
- CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT
- HOTSPOT_SHARE_START
- USAGE_THRESHOLD_REACHED
- SERVICE_FLOW_DETECTION
- CELL_CONGESTED
- CELL_CLEAR
- RAN_NAS_Cause
- SESSION_RECOVERY_VZW
- SESSION_SYNC_VZW
- CREDIT_MANAGEMENT_SESSION_FAILURE

network initiated requests are *supported*

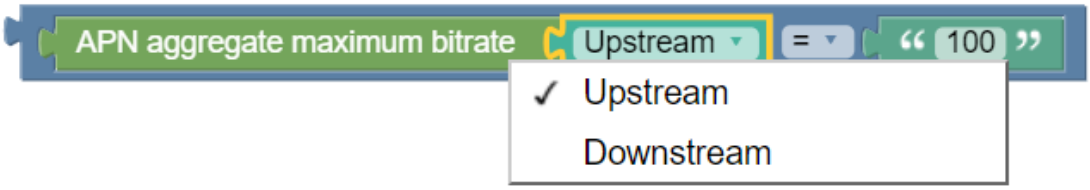
The network initiated requests policy condition, as shown in the following image, triggers a policy that is only evaluated when network initiated requests are supported. On selecting **does not Support** from the drop-down field, this condition block triggers a policy that is only evaluated when network initiated requests are not supported.



APN aggregate maximum bitrate

The **APN aggregate maximum bitrate** condition block, as shown in the following image, selects protocol messages based on the maximum bitrate being requested for an access point name (APN) in a specific direction relative to a numeric value - specified in the **string** block.

The unit of bandwidth is compatible with the Credit Control Request (CCR) message. The APN aggregate maximum bitrate condition block is Policy Table compliant.



From the drop-down field, user can choose the *flow direction* as **Upstream** or **Downstream**. The default operator for this condition is **=**. Select any one of the following operators from the drop-down field:

- =
- !=
- <
- <=
- >
- >=
- Matches
- RegExp-Matches

IP-CAN type

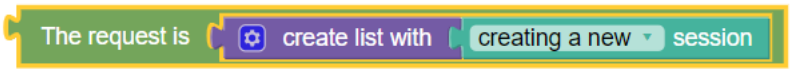
The **IP-CAN type** policy condition, as shown in the following image, triggers a policy that is only evaluated for a protocol message with a specific IP-CAN type.

The user can select any one of the following supported values using the **IP-CAN Type** drop-down field:

- **3GPP_GPRS**
- **3GPP_EPS**
- **NON_3GPP EPS**
- **3GPP2**
- **WiMAX**
- **DOCSIS**
- **xDSL**

The request is

The **request is** policy condition, as shown in the following image, evaluates whether the request type matches with the specified request.



The user can select any one of the following supported values using the drop-down field:

- **creating a new** session (default)
- **modifying an existing** session
- **re-authorizing an existing** session
- **terminating an existing** session

The RAT type is

The **The RAT type is** policy condition, as shown in the following image, triggers a policy that is only evaluated for a protocol message with a specific Radio Access Technology (RAT) type.

The user can select any one of the following valid values from **RATType** drop-down field:

- GERAN
- UTRAN
- HSPA Evolution
- UMA/GAN
- EUTRAN
- EUTRAN NB IoT
- WLAN
- CDMA2000 1x
- HRPD
- UMB
- eHRPD
- NR_REDCAP

QoS Upgrade

The **QoS Upgrade** policy condition, as shown in the following image, evaluates if QoS upgrade is supported (`supports`) or not (`does not support`).

The session is an enforcement session

The **The session is *an enforcement* session** condition block, as shown in the following image, distinguishes between protocol messages that are operating on different sessions.

The user can select any one of the values for the session type using the drop-down field:

- **an enforcement session** (default)
- **an application session**
- **a credit control session**
- **a radius authorization session**

tier

The **tier** condition block, as shown in the following image, triggers a policy that is evaluated for one or more specific tiers.

cell state is *congested*

The **cell state is congested** policy condition block, as shown in the following image, triggers a policy that is evaluated based on the level of congestion in the cell. The supported values are **congested** and **not congested**.

3.10.2 Actions

This section describes the policy actions that can be used to construct policy rules for PCRF Core service.

set Alert with severity level, ID and message

This policy action, as shown in the following image, sends an alert to the system containing the specified severity level and message text. This alert appears in the Active Alerts display for one hour, until cleared, or unless the server fails over, whichever comes first. Alerts generated by policy actions do not affect the HA score of a server, and will not cause a failover. On choosing clear from the drop-down field, the alert containing the specified severity level and message text is cleared from the system.

The following are the valid values that can be selected from the severity drop-down field:

- **Critical** (default)
- **Major**

- **Minor**

The **ID** field specifies the alert ID. On selecting Evaluate as expression, the text in the field is evaluated as an arithmetic expression, and the result is used.

The **message** accepts string value. This text may contain policy parameters to perform parameter substitution within the message text. If you select Evaluate as expression, the text in the field is evaluated as an arithmetic expression, and the result is used.

> **Note**
>
> The "set Alert with severity level, ID and message" has been deprecated in 23.4.0. It should not be used.

reset all subscriber data

The **reset all subscriber data** policy action, as shown in the following image, resets all data for the subscriber.

set policy context property name to value

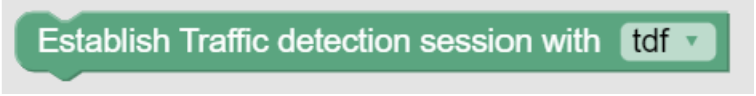
This policy action block, as shown in the following image, sets a subscriber property. The property-name and value accept strings as value.

remove all policy context properties

The **remove all policy context properties** policy action, as shown in the following image, removes all policy context properties.

Establish Traffic Detection Session for a Peer Node

The **Establish Traffic detection session with** policy action, as shown in the following image, establishes a traffic detection session with the selected network element identity.



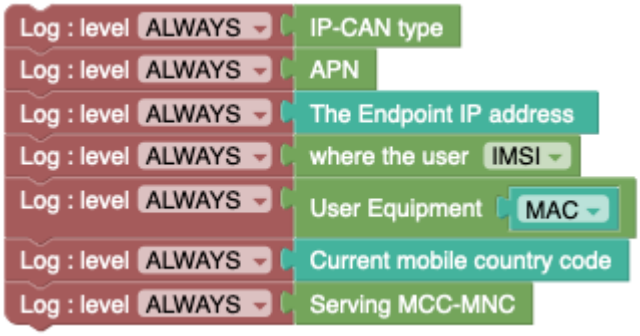
Establish Traffic Detection Session for Peer Node Set

The **Establish Traffic detection session with** policy action, as shown in the following image, establishes a traffic detection session with the selected network element identity.

Enable Logging with log levels

The public **Log: Level** block is enabled **ALWAYS** in the event of various actions, as shown in the following image.

Figure 3-73 Log: level



3.10.3 AF

This section describes the blocks and conditions specific to flows.

3.10.3.1 Conditions

This section describes the conditions specific to flows.

Required-Access-Info

The **Required-Access-Info** policy condition, as shown in the following image, triggers a policy when the returned access network information, populated in Rx call flow, for that AF session matches the specified value.

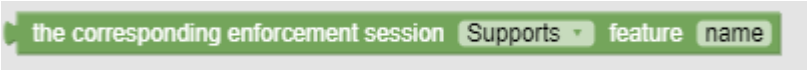
Figure 3-74 Policy Condition for Required-Access-Info

The user can select any one of the following valid values from the drop-down field:

- **USER_LOCATION** (default)
- **MS_TIME_ZONE**
- **USER_LOCATION_AND_MS_TIME_ZONE**

the corresponding enforcement session *supports* feature

The **the corresponding enforcement session *supports* feature *name*** policy condition, as shown in the following image, evaluates the feature name in the enforcement session that correlates to the corresponding application (Rx) request.



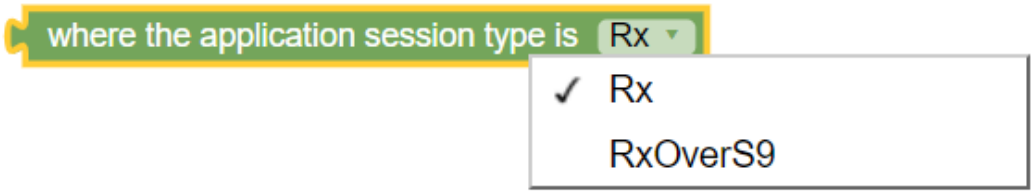
To specify the name of the features, a comma-delimited list of values can be used. This list can contain one or more supported feature. To use a wildcard match pattern, select **RegExp-Matches**. Wildcard match patterns use the following characters:

- * (asterisk) character to match zero or more characters
- ? (question mark) character to match exactly one character

where the application session type is *Rx*

The **where the application session type is *Rx*** policy condition, as shown in the following image, validates whether the application-session is Rx or RxOverS9.

Figure 3-75 Application Session Type Block



> **Note**
>
> If the application session is not Rx, the policy condition returns unknown.

Apply Traffic Profile to Flow(s) whose media type matches one of specified values

This policy condition, as shown in the following image, applies one or more traffic profiles to one or more flows of the specified type media type. It overwrites the corresponding settings in the protocol messages of the specified flows. If multiple traffic profiles are selected, they are applied in the order in which they are specified. If a traffic profile contains settings that are not relevant in the current protocol message, they are ignored. This policy condition is Policy Table compliant.

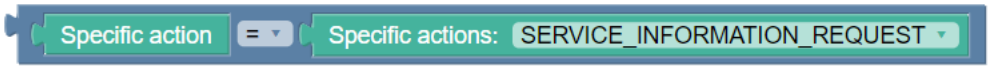
To specify the flow media type, user can select any of the following valid values from the **Type** drop-down field:

- Audio
- Video

- Data
- Application
- Control
- Text
- Message
- Other

Specific action

The **Specific action** policy condition, as shown in the following image, triggers a policy when the value of the Specific-Action AVP field within an Rx RAA message matches the specified value.



The user can select any of the following valid values from the **Specific actions** drop-down field:

- **SERVICE_INFORMATION_REQUEST** (default)
- **CHARGING_CORRELATION_EXCHANGE**
- **INDICATION_OF_LOSS_OF_BEARER**
- **INDICATION_OF_RECOVERY_OF_BEARER**
- **INDICATION_OF_RELEASE_OF_BEARER**
- **INDICATION_OF_ESTABLISHMENT_OF_BEARER**
- **INDICATION_OF_IP_CAN_CHANGE**
- **INDICATION_OF_OUT_OF_CREDIT**
- **INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION**
- **INDICATION_OF_FAILED_RESOURCES_ALLOCATION**
- **INDICATION_OF_LIMITED_PCC_DEPLOYMENT**
- **USAGE_REPORT**
- **ACCESS_NETWORK_INFO_REPORT**
- **INDICATION_OF_RECOVERY_FROM_LIMITED_PCC_DEPLOYMENT**
- **INDICATION_OF_ACCESS_NETWORK_INFO_REPORTING_FAILURE**
- **PLMN_CHANGE**

3.10.3.2 CODEC Conditions

Session Description Protocol (SDP) properties conditions identify any specific SDP attributes and evaluate their value. This includes setting proper bandwidth values on related PCC rules. The following conditions are available.

the *local* specified SDP property matches one of value(s)

This policy condition, as shown in the following image, checks the Codec type (offer or answer) for a subscriber's device (**local**, **remote** or **common**) for specific values (a comma-delimited list).

Users can select any of the following valid values from the drop-down field that specifies where to search for the SDP Property:

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

Specifying SDP Property
A comma-delimited list of SDP properties. Specify the SDP properties using one of the following methods:

- **Generic descriptor**
  Syntax: `sdp.[option]`

  where *option* is any name (for example, i) or any keyword (for example, a=ptime)

  Examples using an SDP generic descriptor:

  - `where the local sdp.[i] matches one of *recvonly*`
  - `where the common sdp.[a=ptime] matches one of 20`
  - `where the common sdp.[a] matches one of ptime: 20`
  - `where the common sdp.[u] matches one of http://www.oracle.com:8080/hr/one.htm`
  - `where the common sdp.[u=http://www.oracle.com] matches one of 8080/hr/one.htm`
  - `where the common sdp.[u=http] matches one of //www.oracle.com:8080/hr/one.htm`
  - `where the remote sdp.[xy] matches one of z`
  - `where the remote sdp.[xy=z] matches one of 80`

- **Media descriptor**
  Syntax: `sdp.[m.option]`

  where *option* can be any of the given values - fmt, port, numberofports, media, and proto.

  Examples using an SDP media descriptor:

  - `where the common sdp.[m.fmt] matches one of 102`
  - `where the common sdp.[m.port] does not match any of 41000,41002`
  - `where the remote sdp.[m.media] matches one of audio,video`
  - `where the local sdp.[m.proto] matches one of RTP/AVP`

- **rtpmap**
  Syntax: `sdp.[codec-name(codec-name).rtpmap.OPTION]`

  where *codec-name* specifies a codec name.

  where *option* can be any of the given values - payloadtype, clockrate, and encodingparameters.

  Examples using rtpmap:

  - `where the common sdp.[ codec-name(AMR-WB).rtpmap] matches one of 104 AMR-WB/160000`
  - `where the common sdp.[ codec-name(AMR-WB).rtpmap.encodingparameters] matches one of 2`
  - `where the common sdp.[ codec-name(AMR-WB).rtpmap.payloadtype] matches one of 104,102`

- **fmtp**
  Syntax: `sdp.[codec-name(`*`codec-name`*`).fmtp.`*`OPTIONS`*`]`

  where *codec-name* specifies a codec name.

  where *option* can be any of the given values - fmt, profile-level-id, mode-set, packetization-mode, or any other parameter to be conveyed.

  Examples using fmtp:

  - `where the common sdp.[codec-name(AMR-WB).fmtp.fmt] matches one of 104,102`
  - `where the common sdp.[codec-name(AMR-WB).fmtp.mode-set] matches one of 2,4`
  - `where the commonsdp.[codec-name(H264).fmtp.profile-level-id] matches one of42e00c`

the *local* specified SDP property *exists*

This policy condition, as shown in the following image, checks for the existence or non-existence of any SDP property for a subscriber's device (**local**, **remote** or **common**).

Users can select any of the following valid values from the drop-down field that specifies where to search for the SDP Property:

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

For information on how to specify the name of SDP property, see Specifying SDP Property.

the *local* specified SDP property is numerically *equal to* specified value

This policy condition, as shown in the following image, compares a numerical SDP property for a subscriber's device (**local**, **remote** or **common**) against a specified number (string).

Users can select any of the following valid values from the drop-down field that specifies where to search for the SDP Property:

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

Users can select any of the following valid values from the drop-down field for the comparison:

- **equal to**

- **not equal to**
- **less than**
- **greater than**
- **less than or equal to**
- **greater than or equal to**

where the *local* codec data is an *offer*

This policy condition, as shown in the following image, checks the Codec type (**offer** or **answer**) for a subscriber's device (**local**, **remote**, or **common**).

Users can select any of the following valid values from the drop-down field that specifies where to search for the SDP Property:

- **Local**—The capabilities of the device for the subscriber.
- **Remote**—The capabilities of the device for the remote party.
- **Common**—The capabilities that the local and remote devices have in common.

3.10.4 AVP Specific

This section describes conditions and actions specific to Attribute Value Pair (AVP).

3.10.4.1 Conditions

This section describes the conditions specific to AVP. The AVP conditions are Policy Table compliant.

AVP Name *exists*

This policy condition, as shown in the following image, checks whether the specified third-party AVP exists or does not exist in an incoming Diameter message. This policy condition supports both loaded base Diameter AVPs and third-party AVPs.

To specify AVP name, select any one of the following formats:

- *name*:*vendorID*
- a full path

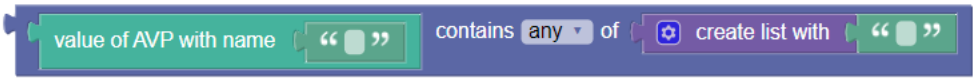
  [*avp_name1*]:*vendorID*.[*avp_name2*]:*vendorID*…

  for the members of the grouped AVPs

value of AVP with name contains one or more of specified values

This policy condition, as shown in the following image, compares the specified value of AVP with name with the values or variables from the specified list. The condition is where the

request AVP name value matches one of the values. The values can be evaluated for equality as well as inequality. To evaluate an AVP value for inequality, the block **contains of** must have the value **none**. This policy condition supports both loaded base Diameter AVPs and third-party AVPs.



To specify AVP name, select any one of the following formats:

- *name*:*vendorID*
- a full path

  [*avp_name1*]:*vendorID*.[*avp_name2*]:*vendorID*…

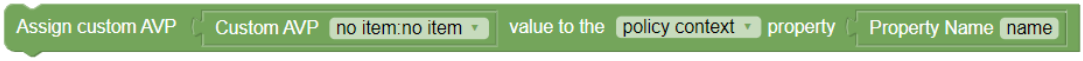
  for the members of the grouped AVPs.

3.10.4.2 Actions

This section describes the policy actions specific to AVP. The AVP actions are Policy Table compliant.

set custom AVP value to the specified property name

This policy action, as shown in the following image, makes the AVP value accessible throughout the policy context so other policies can access this AVP value as a context property. The context property variable will be set only if this AVP exists in the request and its value is not null.



The `property name` is a string that represents the policy context property. The Custom AVP name must be an existing AVP name and Vendor ID.

set value to *existing* or *new* custom AVP

This policy action, as shown in the following image, adds the third-party non-grouped AVP to the current Diameter session with the specified value. If a third-party AVP value is set in the current Diameter session, it will be sent with the corresponding outgoing message. The value parameter must correspond to the AVP data type; otherwise, the AVP shall not be set. If `New` is selected as the value for **custom AVP**, a new AVP is added to the message on every execution of this policy action, without considering that the same AVP name is present in the message.

The `value` string represents a third-party non-grouped AVP.

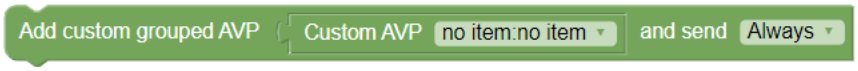
The custom AVP name must be an existing AVP name and Vendor ID. For the send mode, select any one of the following values from the drop-down field:

- Always

- Unless rejected
- If rejected

Add custom grouped AVP and send *Always*

This policy action, as shown in the following image, adds or sends new custom grouped AVP to the current reply. A condition can be set specifying that the AVP is always set to send mode. If you are defining a new grouped third-party AVP with members, the grouped AVP has to appear first in the policy. If you are adding a new member AVP that does not have its parent AVP added yet, the policy attempts to locate this grouped AVP in the rest of the policy. To include a grouped AVP multiple times in the same message, users must follow the order in which it appears in the message.

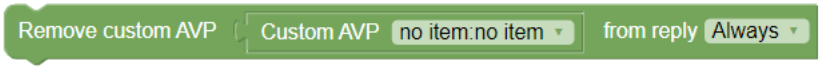


The Custom AVP name must be an existing AVP name and Vendor ID. For the send mode, select any one of the following valid values from the drop-down field:

- Always
- Unless rejected
- If rejected

Remove custom AVP from reply *Always*

This policy action, as shown in the following image, removes the custom AVP name set previously from the reply message.



The Custom AVP name, selected from the drop-down menu, must be an existing AVP name and Vendor ID. For the send mode, select any one of the following valid values from the drop-down field:

- Always
- Unless rejected
- If rejected

Mark request AVP as failed if exists and send *Always*

This policy action, as shown in the following image, marks request AVP as failed if it exists.

For the send mode, select any one of the following valid values from the drop-down field:

- Always
- Unless rejected
- If rejected

3.10.4.3 Use Cases

This section describes use cases for policy conditions specific to AVP.

Use Case - AVP Name *exists*

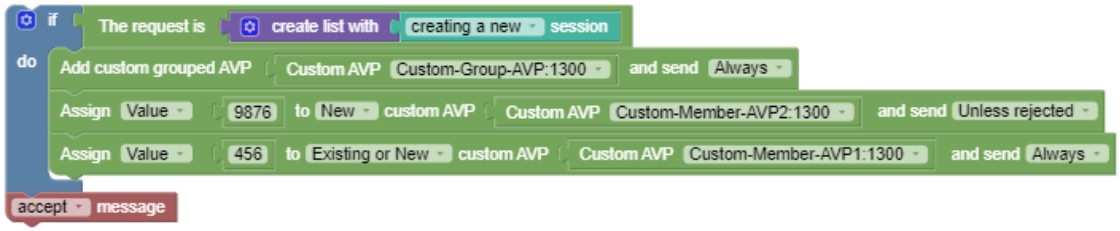
The following screen capture shows a sample policy condition that determines whether the AVP Media-Component-Description is accessible.

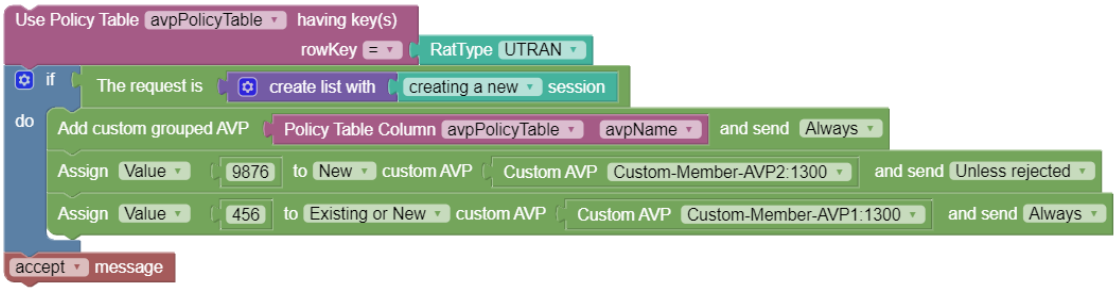
Use Case - Add custom grouped AVP and send *Always*

In the following sample policy, a third party grouped AVP `Custom-Group-AVP:1300` is added to the current Diameter session. It adds the third party non-grouped AVP `Custom-Member-AVP2:1300` as a new AVP to the current Diameter session with the specified value 9876 and this AVP can only be send if the policy is not rejected. It adds the third party non-grouped AVP `Custom-Member-AVP1:1300` to the current Diameter session with the specified value 4566 and if there are multiple instances of this existing AVP the new value will be set to all of them and this AVP can be sent always regardless of the policy execution outcome.

In CCA, the following AVP will be installed at the end:

```
Custom-Group-AVP (43,VM,v=1300,l=44) =
  Custom-Member-AVP2 (1322,V,v=1300,l=16) = 9876
  Custom-Member-AVP1 (1311,VM,v=1300,l=15) = 456
```



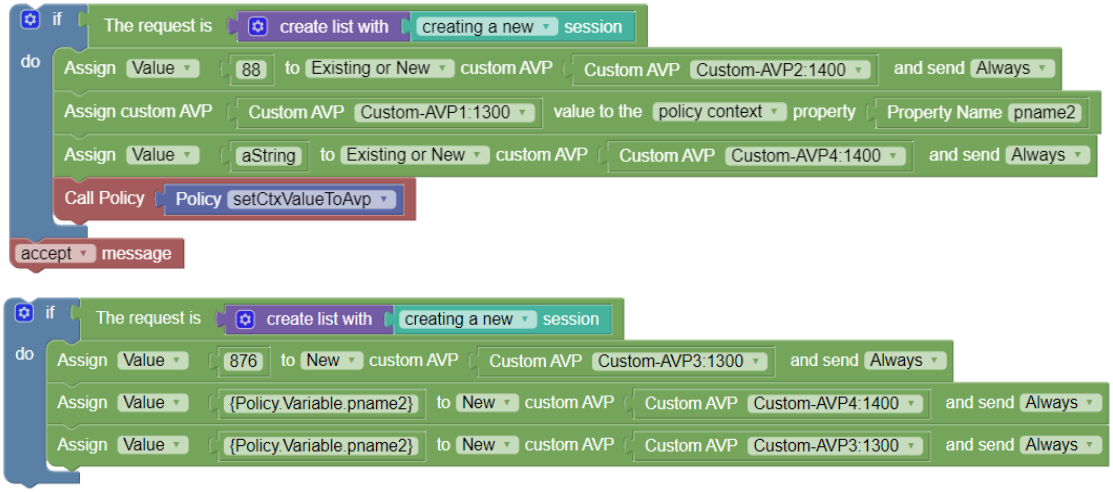


Use Case - Assign value to custom AVP and send response

The following screenshot shows a sample policy for Assign value to custom AVP and send response policy action:

Use Case - Assign custom AVP value to the property

The following screenshot shows a sample policy for Assign custom AVP value to the propert name pname2:



Use Case - Remove custom AVP from reply

The following screenshot shows a sample policy for Remove custom AVP policy action:

3.10.5 Closed User Group (CSG)

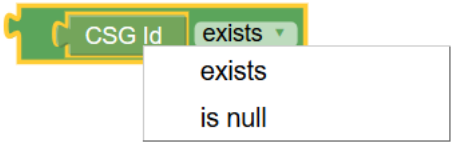
This section describes the Closed User Group (CSG) conditions and use cases for PCRF Core service.

3.10.5.1 Conditions

This section describes the policy conditions that can be used to configure AVP for PCRF Core service.

CSG Id *exists*

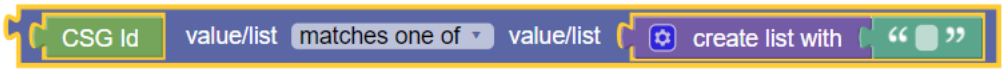
The **CSG Id *exists*** policy condition, as shown in the following image, checks if user **CSG id** is



present or is null in request.

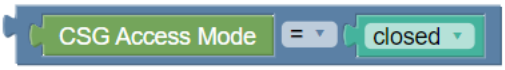
CSG Id value *matches one of* specified values

This policy condition, as shown in the following image, evaluates if the CSG Id value in the request matches or does not match with the one or more specified values in the **string** block.



CSG Access Mode is *closed*

The **CSG Access Mode** policy condition, as shown in the following image, checks if user **CSG Access Mode** is equal to the specified value.



User can select any one of the following valid values from the drop-down field:

- **Closed**
- **Hybrid**

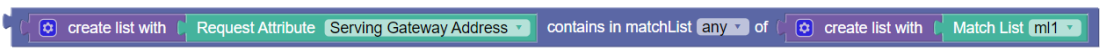
IP-CAN type

The **IP-CAN type** policy condition, as shown in the following image, triggers a policy that is only evaluated for a protocol message with a specific IP-CAN type.

The user can select any one of the following supported values using the **IP-CAN Type** drop-down field:

- **3GPP_GPRS**
- **3GPP_EPS**
- **NON_3GPP EPS**
- **3GPP2**
- **WiMAX**
- **DOCSIS**
- **xDSL**

Request Attribute present in specified match-list



UE is member of CSG

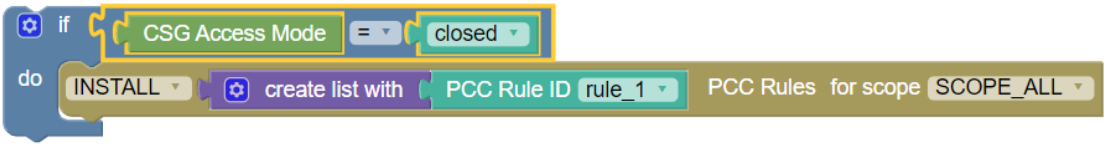
The **UE is member of CSG** policy condition, as shown in the following image, checks if UE is a member of CSG and returns a boolean value.

3.10.5.2 Use Cases

This section describes the use cases specific to CSG that can be used to configure AVP for PCRF Core service.

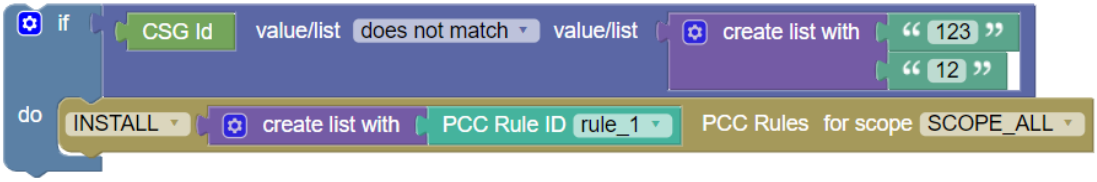
Use Case - CSG Access Mode

In the following sample policy, pccRule is installed if CSG Access Mode returns the hybrid_mode string value from request.



Use Case - CSG Id value matches one or more of specified values

In the following sample policy, pccRule is installed if CSG Id does not match with the list with values ["123", "12"].



Use Case - UE is member of CSG

In the following sample policy, pccRule is installed if UE is not a member of CSG.

3.10.6 Day/Time

Day and Time conditions, actions, and utils are related to the time at which the policy rules are being executed.

Configuring Local Time

To configure the local time, perform the following steps:

1. From the navigation menu, under **PCRF**, then under **Services**, click **Core Service**.
   The Core Service screen appears.
2. Click **Edit** to edit the core service configurations.
3. In **Advance Settings**, click **Create**.
   The Create page appears.
4. Enter **DB.User.DefaultLocalTimeMode** in the **Key** field.
5. Enter **True** in the **Value** field.

6. Click **Save**.

If no configuration is provided, the **SYSTEM_LOCAL_TIME** is considered as default local time.

3.10.6.1 Conditions

This section describes the conditions that can be used to configure day and time for PCRF Core service.

today is the specified day(s) of month in natural order using Configured Local Time

This policy condition, as shown in the following image, triggers a policy based on a day in a month. If current date matches specified number th day (a comma-delimited list of values) of specified months in *natural order* or *reverse order* as per the configured time then the condition returns true, otherwise false.

User can select any of the following valid values from the **Month** drop-down field:

- **January** (default)
- **February**
- **March**
- **April**
- **May**
- **June**
- **July**
- **August**
- **September**
- **October**
- **November**
- **December**

User can select any of the following valid values from the *time-zone* drop-down field:

- **CONFIGURED_LOCAL_TIME** (default)—Calculate the time from the location configured for this MPE device
- **SYSTEM_LOCAL_TIME**—Calculate the time from the location of this MPE device
- **USER_LOCAL_TIME**—Calculate the time from the location configured for the user equipment's location

the current time is within the Time Period

This policy condition, as shown in the following image, triggers a policy based on the time period. This condition gets time slots of all the time periods, and compares current time with these time slots. If the current time falls within the range of time slots configured in these time periods then the condition returns true, otherwise false.

The **Time Period** drop-down field lists the time periods, configured using the Time Periods page on CNC Console. To navigate to the Time Periods page, click **Policy**, and then **Policy Data Configurations**. Select **PCRF Core**, and then click **Time Periods**.

the current time is between start time and end time using Configured Local Time

This policy condition, as shown in the following image, triggers a policy based on time. If the present time is between start time and end time then the condition returns true, otherwise false. If start time is greater than end time then the condition is evaluated, where the end time is considered as the next day.

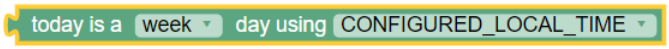
Enter the `start time` and `end time` in the format of *hh*:*mm*, where *hh* is a number in the range from 0 to 23.

User can select any of the following valid values from the *time-zone* drop-down field:

- **CONFIGURED_LOCAL_TIME** (default)—Calculate the time from the location configured for this MPE device
- **SYSTEM_LOCAL_TIME**—Calculate the time from the location of this MPE device
- **USER_LOCAL_TIME**—Calculate the time from the location configured for the user equipment's location

today is a week day using Configured Local Time

This policy condition, as shown in the following image, triggers a policy based on whether it is a *week day* or the *weekend*. If today *is week day* using the system time (**CONFIGURED_LOCAL_TIME**) then the condition returns true. If today *is not week day* using the system time, this policy condition returns false.



User can select any of the following valid values from the *time-zone* drop-down field:

- **CONFIGURED_LOCAL_TIME** (default)—Calculate the time from the location configured for this MPE device
- **SYSTEM_LOCAL_TIME**—Calculate the time from the location of this MPE device
- **USER_LOCAL_TIME**—Calculate the time from the location configured for the user equipment's location

today is Day Sunday using Configured Local Time

This policy condition, as shown in the following image, triggers a policy based on the day of the week. If today *is Sunday* using the system time (**CONFIGURED_LOCAL_TIME**) then the condition returns true. If today *is not Sunday* using the system time, this policy condition returns false.

User can select any of the following valid values from the **Day** drop-down field:

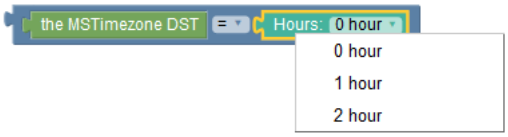
- **Sunday** (default)
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**

User can select any of the following valid values from the *time-zone* drop-down field:

- **CONFIGURED_LOCAL_TIME** (default)—Calculate the time from the location configured for this MPE device
- **SYSTEM_LOCAL_TIME**—Calculate the time from the location of this MPE device
- **USER_LOCAL_TIME**—Calculate the time from the location configured for the user equipment's location

the MSTimezone DST

The **the MSTimezone DST** policy condition triggers a policy that is only evaluated if the applied Daylight Saving Time offset for the location of a mobile subscriber or mobile station (MS) matches the parameter.



User can select any one of the following operators from the drop-down field:

- **=** (default)
- **!=**
- **<**
- **<=**
- **>**
- **>=**
- **Matches**
- **RegExp-Matches**

the MSTimezone offset

The **the MSTimezone offset** policy condition triggers a policy that is only evaluated if the applied time zone for a mobile subscriber or mobile station (MS) matches the parameter.

User can select any one of the following operators from the drop-down field:

- **=** (default)
- **!=**
- **<**
- **<=**
- **>**
- **>=**
- **Matches**
- **RegExp-Matches**

3.10.6.2 Actions

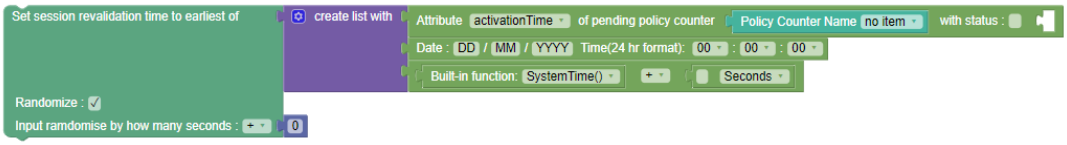
This section describes the actions that can be used to configure day and time for PCRF Core service.

Set session revalidation time to earliest of specified time

The **Set session revalidation time to the earliest of** action block returns the earliest time from the following list:

- Time in the specified policy counter ID or IDs
- Time defined in the `Seconds/Minutes/Hours/Days` format from the time when a policy is executed
- Specific time in `hh:mm` format (limited to 15-minute intervals) on a specific day of the week using either *SYSTEM TIME* or *UTC TIME* time-zone.
- Random time between a time range

Figure 3-76 Set session revalidation time to earliest of



This action block is Policy table compliant.

In addition, you can check the Randomize checkbox to select a random revalidation time from the time range.

You can define the range by using the number block (under Public category) for specifying the seconds and selecting any of the following values from the dropdown list:

- "**+**": It adds the specified seconds to the time entered.
- "**-**": It subtracts the specified seconds from the time entered.
- "**+/-**": The range is defined by [Time entered - specified seconds] to [Time entered + specified seconds].

If you select the Randomize option, the following message is printed in the Policy runtime logs:

{"messageTimestamp":"2022-01-25T08:10:41.698Z","logLevel":"WARN","pid":14692,"workerId":2,"fileName":"lib\\services\\sm_core-service.js","lineNo":"25","message":"**Applying randomization on earliest time**}

If you input anything other than a number for randomization, the following error is printed in the logs:

"message":"Error!! Entered seconds is not a number for randomization !!Please enter number in seconds field."

Note: On upgrading to Policy 22.1.0 or later versions, the **Set revalidation time to earliest of** block is upgraded automatically in the existing policies.

3.10.6.3 Utils

This section describes the utils that can be used to configure day and time for PCRF Core service.

Offset

The Offset util can be combined with policy conditions and actions to specify a time zone.

Time Period

The Time Period util can be combined with policy conditions and actions to specify a time period.

The **Time Period** drop-down field lists the time periods, configured using the Time Periods page on CNC Console. To navigate to the Time Periods page, click **Policy**, and then **Policy Data Configurations**. Select **PCRF Core**, and then click **Time Periods**.

Day

The Day util can be combined with policy conditions and actions to specify the day.

The available drop-down values are as follow:

- **Sunday** (default)
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**

- **Friday**
- **Saturday**

3.10.7 Identities/Addresses

The conditions categorized under Identities and Addresses are Policy Table compliant. The conditions can be used to manage policies for PCRF Core service.

3.10.7.1 Conditions

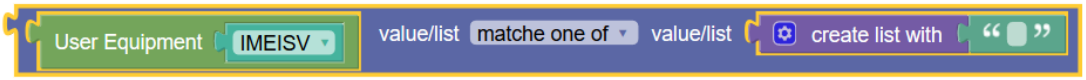
This section describes the conditions specific to user identities and addresses.

where the User IMSI

The **where the User IMSI** condition block, as shown in the following image, allows operators to identify users based on **IMSI**, **E.164**, **NAI** or **SIP URI** from the request received by the Policy Rule Engine.

User Equipment

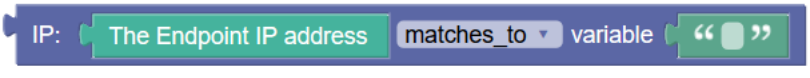
The **User Equipment** condition block, as shown in the following image, allows operators to evaluate one or more IMEISV or MAC values. The evaluation is based on matching wildcard patterns. On selecting **matches one of** from the drop-down menu, if the IMEISV/MAC value matches with the address present in the JSON request, then the condition returns true, otherwise false.



> **Note**
>
> A wildcard match pattern uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character. It can be of form "***-*-56-*-*-D?**" or "***:*:56:*:*:D?**" and not like "**00-***" etc.

The Endpoint IP address

In the **The Endpoint IP address** condition block, as shown in the following image, the **The Endpoint IP address** child block fetches endpoints IP address from the JSON path, and then compares the retrieved value with the value provided in the **string** block. It supports both IPv4 and IPv6 addresses.



The Endpoint IP Address condition block supports the following two comparison methods:

1. **matches_to** - On selecting this value, the block performs a string comparison, and matches the retrieved value with the value provided in the string block.

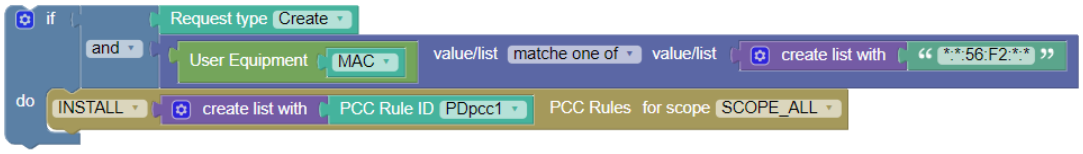
2. **is_in_subnet** - On selecting this value, the block performs a comparison based on node IP library, and verifies if the retrieved value is in subnet provided in the string block.

3.10.7.2 Use Cases

This section provides information about the use cases related to Identities/Addresses condition blocks.

Use Case - User Equipment

The following policy example shows a create request for a PCC rule when MAC address matches the specified value, that is, "*:*:56:F2:*:*".



Use Case - The Endpoint IP Address

The following policy example triggers a policy when the endpoint IP address matches *10.0.3.102*:

3.10.8 Location/Presence

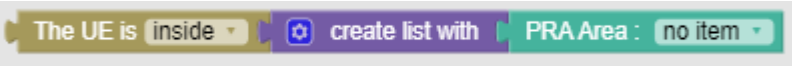
This section describes the conditions, actions, and utils specific to user location and presence reporting area.

3.10.8.1 Conditions

This section provides information on Location/Presence conditions available under PCRF Core Service.

The UE is *inside/outside/inactive* for PRA Area

This policy condition, as shown in the following image, triggers a policy that is only evaluated when the user equipment is or is not inside the subscribed PRA area.



Operators may select the location of the UE as inside, outside or inactive from the drop-down field.

The subscribed PRA area *matches/does not match* one or more PRA areas

This policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specific PRA values. If **default area** is selected as the definition for the

parameter *pra-areas*, the policy is only evaluated if the user equipment is already subscribed to a PRA.

A single area or multiple specific PRA areas selected from the defined PRA areas, manually input, or Default.

- **CMP defined PRA lists**
  Select one or more defined PRA lists
- **Manual Input**
  Enter the identifier for the PRA in hexadecimal format or a custom PRA from a subscriber profile in the format *{User.CustomField}*.

  The manual input format for multiple PRAs is:

  ```
  PRA
  identifier1 [;PRA element list1],PRA identifier2 [; PRA element
  list2],…
  ```

  The format of PRA identifier and PRA Element List is according to section 8.108 of TS 29.274[9]. It is specified in Hexadecimal format. If only has a PRA identifier then the PRA area is a predefined PRA area. If both PRA identifier and PRA Element List exists, then it is a UE-dedicated PRA Area. The manual input is typically used to input a temporally PRA area. The manual input can also be used to get a PRA area from Custom field of subscriber. For example, {User.Custom4}. If the operator wants to manually input a PRA area they need to get the Hexadecimal value for each. Different vendors/operators should interact or exchange PRA info using the Hexadecimal representation as defined in section 8.108 of TS 29.274[9].

  The manual input format for a single PRA is:

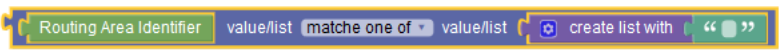
  ```
  PRA identifier [, PRA element list]
  ```

- **Default**
  The PRA to which the user equipment is already subscribed, if any.

  The Default option specifies using the default PRA area. The default PRA is the PRA area subscribed or provisioned by the PCRF for the UE during IP-CAN session life cycle. It is either a UE- dedicated or predefined PRA area. It can be a PRA area that is retrieved from the subscriber profile (normally UE-dedicated) or a PRA area defined in the CMP (normally predefined). When used , this Default option means to check whether the UE has subscribed to a PRA area but does not care what the PRA area is.

Routing Area Identifier

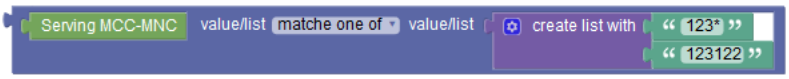
The **Routing Area Identifier** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specified Routing area identifier values (based on matching wildcard patterns).



> **Note**
>
> To know more about the format of routing area identifier, see the 3GPP TS 23.003 standard.

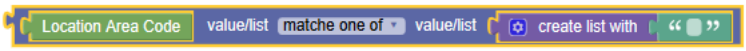
Serving MCC-MNC

The **Serving MCC-MNC** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specific mobile country code (MCC)-mobile network code (MNC) values. A valid value consists of a 3-digit mobile country code and a 2- or 3-digit mobile network code, such as *123045*.



Location Area Code

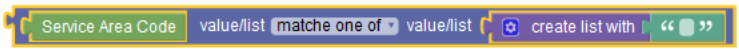
The **Location Area Code** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specified Location area code values (based on matching wildcard patterns).



A valid location area code is an integer between 0 and 65535.

Service Area Code

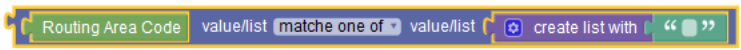
The **Service Area Code** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specified Service area code values (based on matching wildcard patterns).



A valid service area code is an integer between 0 and 65535.

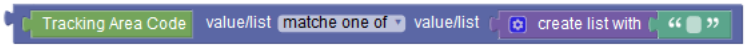
Routing Area Code

The **Routing Area Code** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specified Routing area code values (based on matching wildcard patterns).



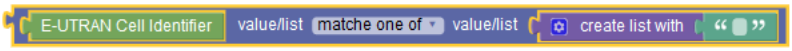
Tracking Area Code

The **Tracking Area Code** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specified Tracking area code values (based on matching wildcard patterns).



E-UTRAN Cell Identifier

The **E-UTRAN Cell Identifier** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specific E-UTRAN Cell Identifier values (based on matching wildcard patterns).



The values specified in the string block can be a comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

Cell Identifier

The **Cell Identifier** policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specific Cell Identifier values (based on matching wildcard patterns). A valid Cell Identifier is an integer between 0 and 65535.

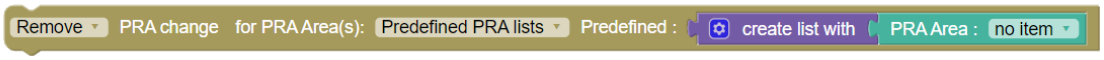
The values specified in the string block can be a comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and the ? (question mark) character to match exactly one character.

3.10.8.2 Actions

This section describes the actions specific to Presence Reporting Area, which can be used to create and manage policies for PCRF Core service.

Remove/Install/Subscribe PRA change for PRA Area(s)

This policy action, as shown in the following image, subscribes the user equipment to PRA changes in the specified PRA. If default area is selected as the definition for the parameter pra, subscribes the user equipment to PRA changes in the last subscribedPRA.



For PRA area, any of the following options can be selected:

- **predefined PRA list** — select a defined PRA list
- **manual input** — enter the identifier for the PRA in hexadecimal format or a custom PRA from a subscriber profile in the format {User.CustomField}.
- **default area** - the last PRA to which the user equipment was subscribed

PRA Subscription

This policy action, as shown in the following image, enable or disable PRA subscriptions.

3.10.9 Network Device Conditions

Network Device conditions are related to the specific network device for which the policy rule is being evaluated. This includes conditions based on the network device type, as well as those that refer to specific unique identifiers for network devices.

3.10.9.1 Conditions

This section provides information on conditions for Network Devices, available under PCRF Core service.

Enforcement network element type

The **enforcement network element type** policy condition, as shown in the following image, triggers a policy when enforcement network element type contains any, none or all the specified value of Device type.

The user can select any one of the following valid values from the **Device type** drop-down field:

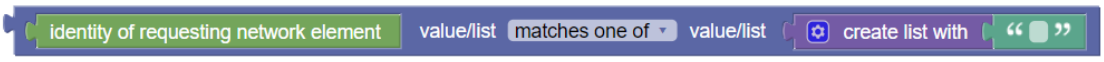
- PGW
- GGSN

Enforcement network element name

The **Enforcement network element name** policy condition, as shown in the following image, triggers a policy when enforcement network element name block contains any, all or none of the specified one or more values in the **string** block.

identity of requesting network element

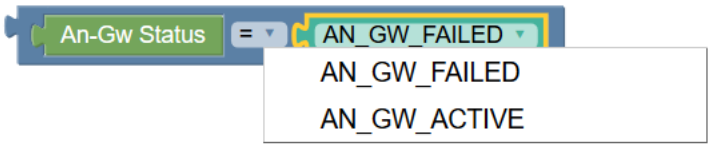
The **identity of requesting network element** block condition, as shown in the following image, triggers a policy when the identity of networking element, that is, ORIGIN_HOST AVP *matches one of* or *does not match* specified values or lists.



> **Note**
>
> The wildcards * (asterisk) and ? (question mark) are allowed for entries in the match-list.

An-Gw Status

The **An-Gw Status** policy condition, as shown in the following image, triggers a policy based on whether the An-Gw status is active or inactive. It compares the An-Gw status selected from the drop-down field with An-Gw status read from JSON (which is sent from PCRF-Core to PRE).



The user can select any one of the following valid values from the An-Gw Status drop-down field:

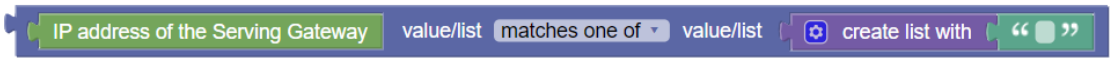
- AN_GW_FAILED
- AN_GW_ACTIVE

> **Note**
>
> The AN_GW_FAILED value indicates that the AN-Gateway has failed and that the PCRF should refrain from sending policy decisions to the PCEF until it is informed that the AN-Gateway has been recovered. This value shall not be used if the IP-CAN Session Modification procedure is initiated for PCC rule removal only.

In place of the dropdown, a string block can also be used, as shown in the following image:

IP Address of the Serving Gateway

The IP address of the Serving Gateway policy condition, as shown in the following image, triggers a policy that is only evaluated for one or more specific Serving Gateway addresses (based on matching wildcard patterns).



The Serving Gateway addresses in the string block can be a comma-separated list of values, where each value is a wildcard match pattern that uses the * (asterisk) character to match zero or more characters and ? (question mark) character to match exactly one character.

3.10.10 Priority/Emergency

This section describes the policy conditions and actions for multimedia priority support and emergency sessions.

3.10.10.1 Conditions

This section describes the conditions specific to multimedia priority support and emergency sessions.

Media component description reservation priority

This policy condition, as shown in the following image, selects Rx protocol messages based on the requested media component description reservation priority.

User can select any of the following valid values from the drop-down field:

- **DEFAULT**
- **PRIORITY_ONE**
- **PRIORITY_TWO**
- **PRIORITY_THREE**
- **PRIORITY_FOUR**
- **PRIORITY_FIVE**
- **PRIORITY_SIX**
- **PRIORITY_SEVEN**
- **PRIORITY_EIGHT**
- **PRIORITY_NINE**
- **PRIORITY_TEN**
- **PRIORITY_ELEVEN**
- **PRIORITY_TWELVE**
- **PRIORITY_THIRTEEN**
- **PRIORITY_FOURTEEN**
- **PRIORITY_FIFTEEN**

Media Type

Sets the value to one of the drop-down list options of Media Type:

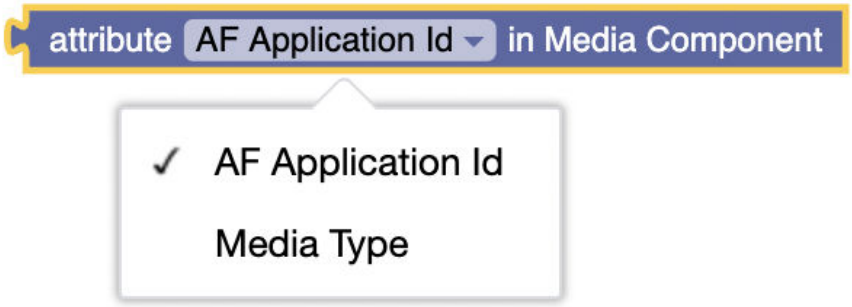
- AUDIO
- DATA
- VIDEO
- TEXT
- CONTROL
- APPLICATION
- MESSAGE
- OTHERS

Figure 3-77 Media Type

AF Application Identifier

This policy condition indicates the particular service that the AF session belongs to. This AVP can be provided at both AF session level, and Media-Component-Descriptionlevel. When provided at both levels, the AF-Application Identifier provided within the Media-Component-Description AVP will have precedence.

Figure 3-78 AF Application Identifier



MCPTT Identifier

This policy condition indicates that the new AF session relates to an MCPTT session with priority call. If PCRF receives the MCPTT-Identifier AVP related to that MCPTT session, PCRF can take specific actions on the corresponding IP-CAN to ensure that the MCPTT session is prioritized.

Figure 3-79 MCPTT Identifier

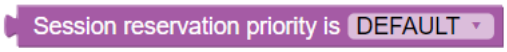
MCVideo-Identifier

This policy condition indicates that the new AF session relates toan MCVideo session with priority call. If PCRF receives the MCVideo-Identifier AVP related to that MCVideosession, PCRF can take specific actions on the corresponding IP-CAN to ensure that the MCVideo session isprioritized.

Figure 3-80 MCVideo Identifier

Session reservation priority is

This policy condition, as shown in the following image, selects Rx protocol messages based on the requested session reservation priority.



User can select any of the following valid values from the drop-down field:

- **DEFAULT**
- **PRIORITY_ONE**
- **PRIORITY_TWO**
- **PRIORITY_THREE**
- **PRIORITY_FOUR**
- **PRIORITY_FIVE**
- **PRIORITY_SIX**
- **PRIORITY_SEVEN**
- **PRIORITY_EIGHT**
- **PRIORITY_NINE**
- **PRIORITY_TEN**
- **PRIORITY_ELEVEN**
- **PRIORITY_TWELVE**
- **PRIORITY_THIRTEEN**
- **PRIORITY_FOURTEEN**
- **PRIORITY_FIFTEEN**

MPS identifier

The MPS identifier policy condition, as shown in the following image, determines the value of the MPS identifier.

the Service-URN is one of specified value(s)

This policy condition, as shown in the following image, selects Rx protocol messages based on the value of the Service-URN field.

3.10.10.2 Actions

This section describes the actions that can be performed to configure multimedia priority support and emergency sessions.

set *GCS* ARP to specified Priority Value with Preemption Capability and Preemption Vulnerability *enabled*

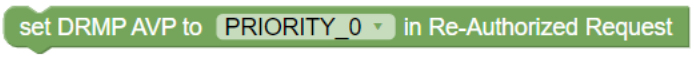
This policy action overrides the default ARP settings for *eMPS* or *GCS* ARP. The priority level defines the relative importance of a resource request. Enter a value from 1 to 15. The default is 1.

The **Preemption Capability** defines whether a service data flow can get resources that were assigned to another service data flow with a lower priority level. Select **Enable** (default) or **Disable** from the drop-down field.

The **Preemption Vulnerability** defines whether a service data flow can release the assigned resources so that a service data flow with a higher priority level can be admitted. Select **Enable** (default) or **Disable** from the drop-down field.

set DRMP AVP to specified priority in Re-Authorized Request

This policy action sets the priority level of the Diameter routing message priority (DRMP) AVP for Gx: RAR messages. Select one of the *drmp-level* values from the drop-down field, where PRIORITY_0 is the highest priority and PRIORITY_15 is the lowest priority.



3.10.11 Roaming

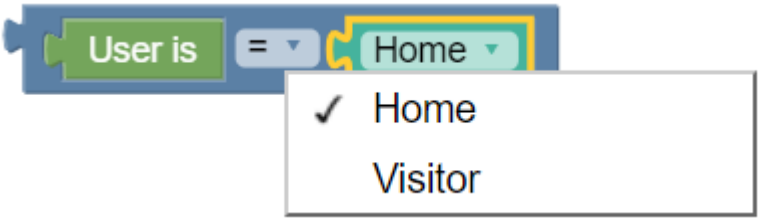
This section describes the policy conditions that can be used to configure policies for roaming scenarios under PCRF Core service.

3.10.11.1 Conditions

This section describes the conditions categorized under Roaming for PCRF Core service.

User is *Home*

The **User is *Home*** policy condition, as shown in the following image, evaluates whether the user is a home user or a visitor.



Current mobile country code

The Current mobile country code policy condition, as shown in the following image, retrieves the current mobile country code of the user from the request received by PRE.

3.10.12 Rules/Flows

This section describes the conditions and actions that can be used to configure rules and flows to manage policies for PCRF Core service.

3.10.12.1 Conditions

This section describes the conditions that can be used to configure rules and flows to manage policies for PCRF Core service.

Rule report contains one of rule name(s) and the rule status is *Active*

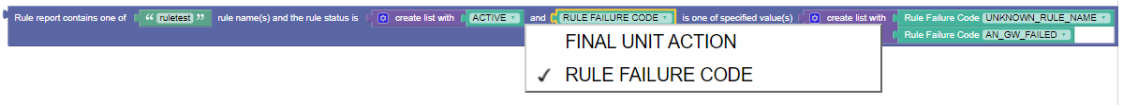
This policy condition, as shown in the following image, triggers a policy when the rule report contains one of the specified rule name(s) and the rule status for the specified rule name is active. This policy condition is policy table compliant.

User can select any of the following valid rule status values from the drop-down field:

- ACTIVE
- INACTIVE
- TEMPORARILY_INACTIVE

Rule report contains one of rule name(s) and the rule status is *Active* and the *Final Unit Action* is one of specified failure code(s)

This policy condition, as shown in the following image, triggers a policy when the rule report contains one of the specified rule name(s) that is **active**, and has **final unit action** as one of the specified values. In place of active rule names, the policy condition can evaluate policy for **inactive** or **temporarily inactive** rule names as well.



Instead of Final Unit Action, user can select **Rule Failure Code** and specify values for policy evaluation.

This policy condition is policy table compliant.

Flow type

The flow type policy condition, as shown in the following image, triggers a policy that is only evaluated for a specific flow type.

Select any of the following valid values using the **Flow type** drop-down field:

- **UE_FLOW** (default)
- **AF_FLOW**
- **PCC_RULE_FLOW**
- **ENF_APP_FLOW**

Flow request type

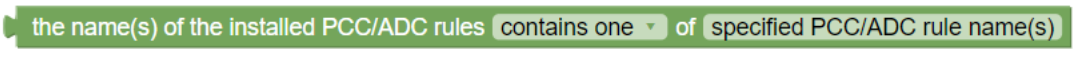
The flow request type policy condition, as shown in the following image, triggers a policy that is only evaluated for a specific flow request type.

Select any of the following valid values using the **Flow request type** drop-down field:

- **TYPE_NOCHANGE** (default)
- **TYPE_CREATE**
- **TYPE_MODIFY**
- **TYPE_DELETE**
- **TYPE_PROVISION**

the name(s) of the installed PCC/ADC rules *contains one* of specified PCC/ADC rules

This policy condition, as shown in the following image, triggers a policy when the installed PCC or ADC rules *contains one* of the specified PCC or ADC rules.

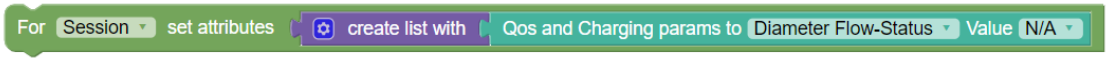


3.10.12.2 Actions

This section describes the policy actions that can be applied to configure rules and flows for PCRF Core service.

Apply QoS and Charging Parameter Values

The following policy action can be used to apply the QoS and charging parameter values for a particular session flow:

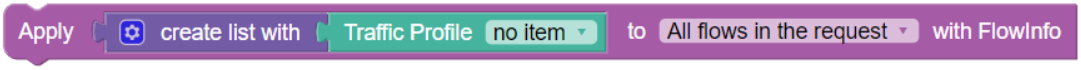


Use Case
The following is a sample policy rule to apply QoS and charging parameters to all the session flows:

The following is a sample policy rule to apply QoS and charging parameters on a particular session flow:

Apply Traffic Profile to *All flows in the request* with FlowInfo

This policy action, as shown in the following image, applies one or more traffic profiles to all flows or a specific flow with FlowInfo. It overwrites the corresponding settings in the protocol messages of the specified flows. If multiple traffic profiles are selected, they are applied in the order in which they are specified. If a traffic profile contains settings that are not relevant in the current protocol message, they are ignored. This policy condition is Policy Table compliant.



remove PCC rule for the specified flow

This policy action, as shown in the following image, removes the policy and charging control role from the current flow. Users can select either **ENF_APP_FLOW** or **UE_FLOW** from the drop-down list.

Install PCC Rules for specified scope

This policy action, as shown in the following image, installs or removes specified list of PCC Rules for a defined scope.

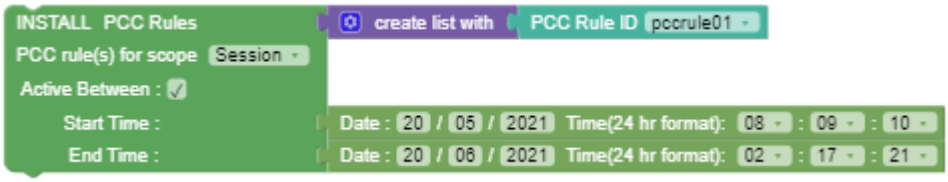
Users can select any one of the following valid drop-down values from the **scope** field:

- SCOPE_SESSION

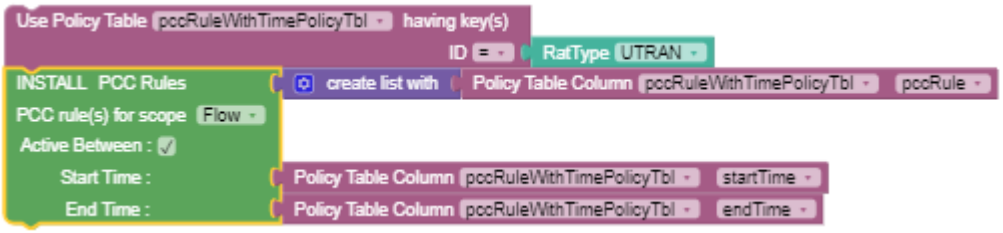
- SCOPE_FLOW
- SCOPE_ALL

Install PCC Rule with specified Active and Inactive time

The following policy action allows users to install PCC Rules for a specified time duration.



This policy action is Policy Table compliant and can be combined with the **Use Policy Table** condition block, as shown in the following image:



When the user selects the **Active Between** check box, the following scenarios are possible:

- **Start time only** - PCC rule becomes active at the specified time with a null value for the end time.

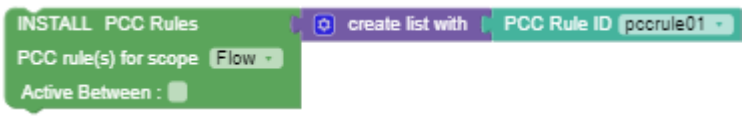
> **Note**
>
> To install a rule at the current system time, users are recommended to not use any block to specify the Start Time. Instead, leave the Start Time empty and the Rule-Activation-Time gets installed at the current system time in CCA.

- **End time only** - PCC rule takes current time as start time and gets inactive at the specified time.
- **Both Start time and End time** - PCC rule remains active between the specified duration.

The following time formats can be used to specify a time frame:

- Date and time block
- Relative Time
- now
- YYYY-MM-DDThh:mm:ss+UTCoffset

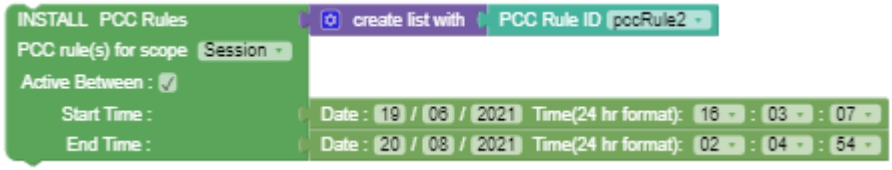
When the **Active Between** check box is deselected, the PCC rule is installed and becomes active (taking current time as default) with no end time.



Use Case

The following screenshot shows a sample policy that installs pccRule2 and sets values for `Rule-Activation-Time` and `Rule-Deactivation-Time` as `Sat Jun 19 16:03:07 UTC 2021` and `Fri Aug 20 02:04:54 UTC 2021` respectively.

The installed pccRule2 remains active from specified start time to end time. It also sets the `Revalidation-Time`, which is same as the `Rule-Deactivation-Time`.



Remove all ADC rules

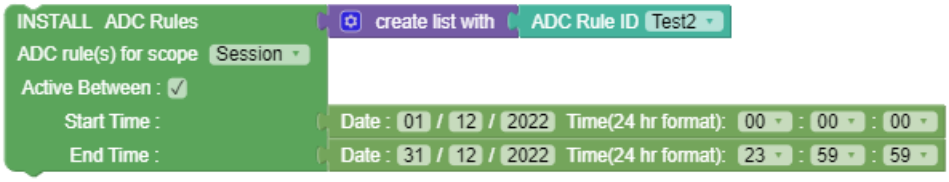
This policy action, as shown in the following image, removes all the ADC rules from the current flow. Users can select the session scope using the dropdown.

Remove ADC rule for the specified flow

This policy action, as shown in the following image, removes the specified ADC rule from the current flow. Users can select the ADC Rule ID using the dropdown.

Install ADC Rule with specified Active and Inactive time

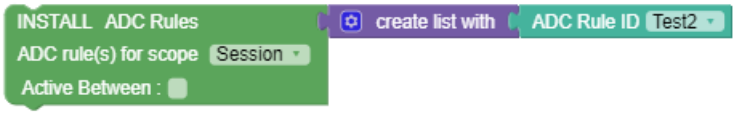
The following policy action allows users to install ADC Rules for a specified time duration.



When the user selects the **Active Between** check box, the following scenarios are possible:

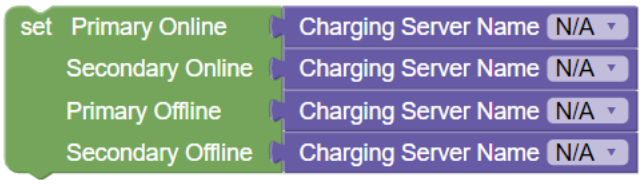
- **Start time only** - ADC rule becomes active at the specified time with a null value for the end time.
- **End time only** - ADC rule takes current time as start time and gets inactive at the specified time.
- **Both Start time and End time** - ADC rule remains active between the specified duration.

When the **Active Between** check box is deselected, the ADC rule is installed and becomes active (taking current time as default) with no end time.



Set values for Charging Server parameters

The following policy action can be used to set values for online or offline charging servers:



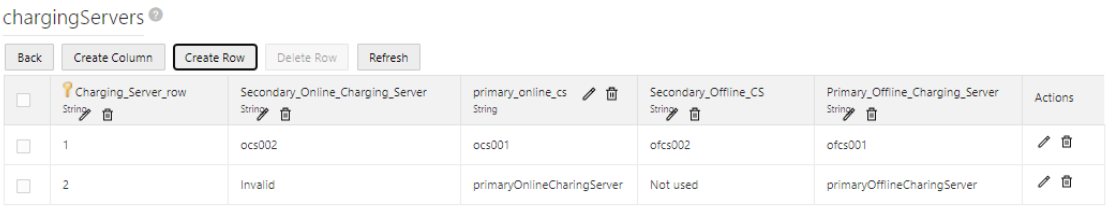
The block allows you to select the following Charging Servers:

- Primary Online
- Secondary Online
- Primary Offline
- Secondary Offline

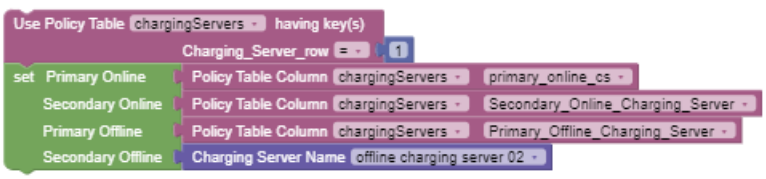
The Charging Server blocks are Policy Table compliant.

The following is a use case to configure Charging Server using the Policy Table block:

The following screen capture illustrates a charging server Policy Table configured on Policy GUI:



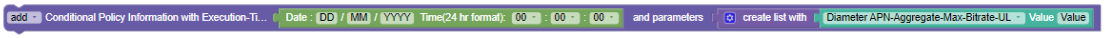
The Policy Table can be used in the Charging Server block as follows:



In the above example, the charging server Policy Table is already configured. You can select the particular row from the Policy Table. For more information, see Policy Table.

Add or *override* Conditional Policy Information with Execution-Time and specified parameters

The following policy action allows users to add a new Conditional-Policy-Information AVP with specified parameter values to the existing list of Conditional-Policy-Information AVPs. By selecting `override` value, user can replace an existing list of Conditional-Policy-Information AVPs.



Any of the following time formats can be used to specify time of execution:

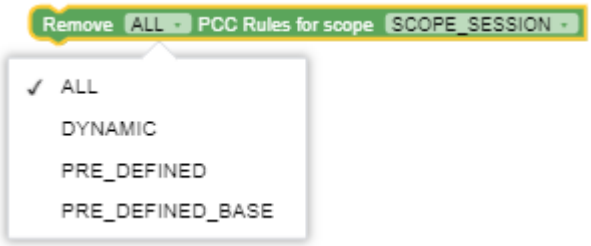
- Date and time block
- Relative Time
- now (the local date and time)
- Date and time in the format: `YYYY-MM-DDThh:mm:ss+UTCoffset`

For parameters, select any of the following from the drop-down menu and provide appropriate values:

- Diameter APN-Aggregate-Max-Bitrate-UL
- Diameter APN-Aggregate-Max-Bitrate-DL
- Diameter Default EPS Bearer QCI
- Diameter Default EPS Bearer ARP Priority Level
- Diameter Default EPS Bearer ARP Preemption Capability
- Diameter Default EPS Bearer ARP Preemption Vulnerability

Remove PCC Rules for a Defined Scope

This policy action removes the specified PCC rule for a defined scope as shown in the following image:

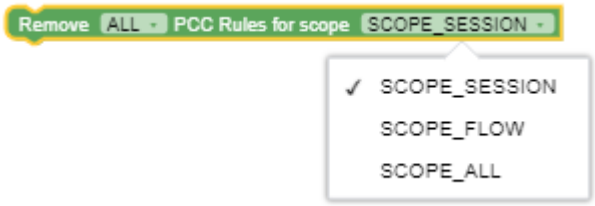


The user can select one of the following items from the *Remove* drop-down list:

- ALL
- DYNAMIC
- PRE_DEFINED
- PRE_DEFINED_BASE

Moreover, the user can select one of the following values from the *PCC Rules for scope* drop-down list to remove the PCC rule:

- SCOPE_SESSION
- SCOPE_FLOW
- SCOPE_ALL



Use case: The following image shows a sample policy when `Dynamic` is set for *Remove* field and `SCOPE_ALL` is set for *PCC Rules for scope* field:

The return-CCA must include:

```
Charging-Rule-Remove (1002,VM,v=10415,l=32) = Charging-Rule-Name
(1005,VM,v=10415,l=20) = pccRule1
```

Use case: The following image shows a sample policy when ALL is selected for the *Remove* field and *PCC Rules for scope* is set to SCOPE_ALL:

The return-CCA must include:

```
Charging-Rule-Remove (1002,VM,v=10415,l=84) = Charging-Rule-Name
(1005,VM,v=10415,l=20) = pccRule1 Charging-Rule-Name (1005,VM,v=10415,l=24) =
predPccRule1 Charging-Rule-Base-Name (1004,VM,v=10415,l=28) = predPccRuleBase1
```

3.11 Context Menu Options for All Blocks

The following table provides details about the context menu options for all the blocks:

Menu Options	Description
Duplicate	Creates a copy of this block.
Add Comment	Insert comments into the block.
Collapse Block	Compresses the elements within the block.
Disable Block	Deactivates or disables the block.
Delete Block	Removes the block.
Help	Opens Google Blockly webpage.

4 Use Cases

The following use cases describe different scenarios through which policies are getting installed with different set of conditions.

> **Note**
>
> The performance and capacity of the Policy system may vary based on the Call model, Feature/Interface configuration, underlying CNE and hardware environment, including but not limited to the complexity of deployed policies, policy table size , object expression and custom json usage in policy design.

4.1 Policy Control Function Use Cases

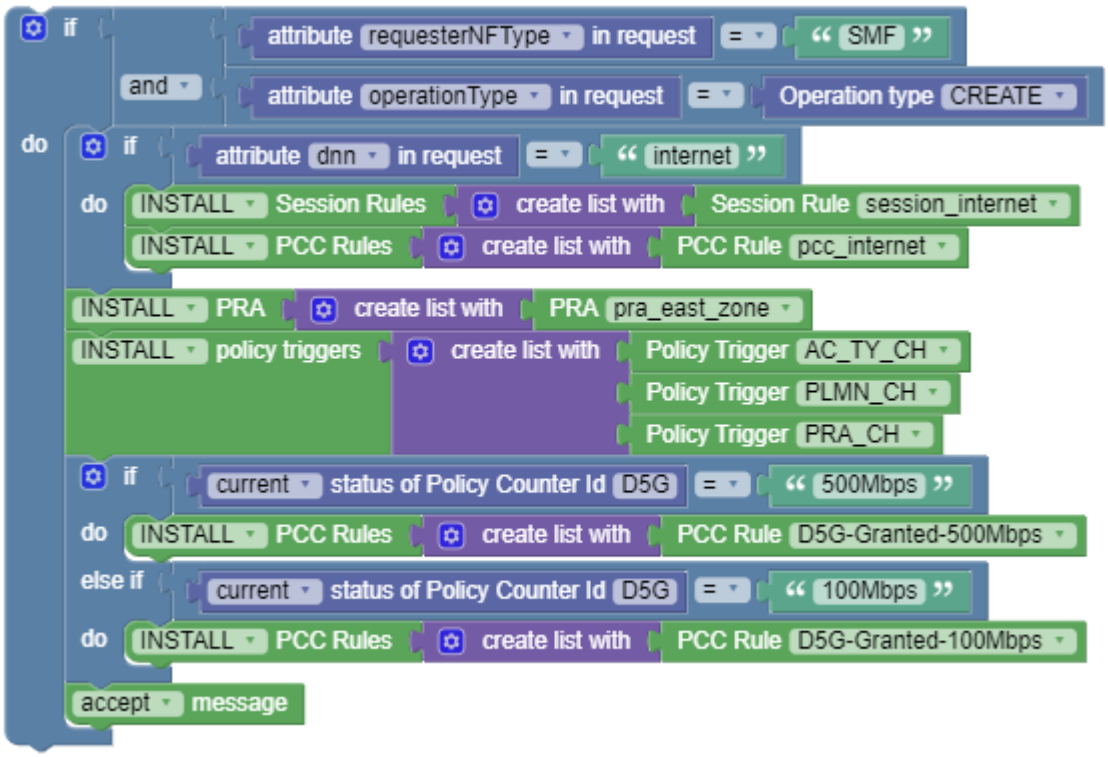
This section describes Policy Control Function use cases.

Use Case 1

When PCF receives a create association message, install the following:

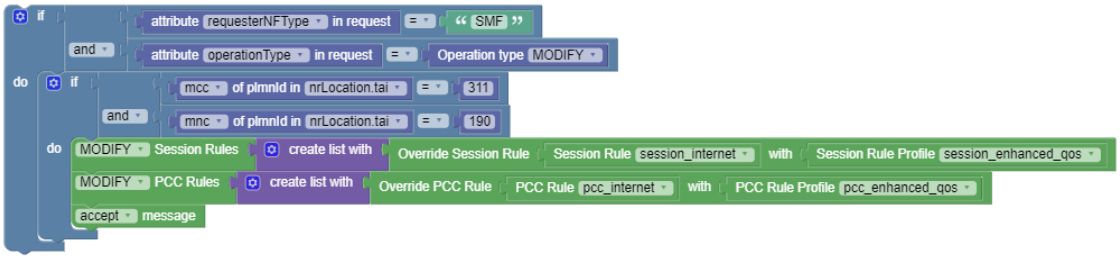
- a Session Rule and a PCC Rule for DNN “internet”
- a PRA Rule and a list of Triggers
- additional PCC Rules based on the initial status of Policy Counters received from CHF

The following screen capture shows the created policy after applying the above policy rules:



Use Case 2

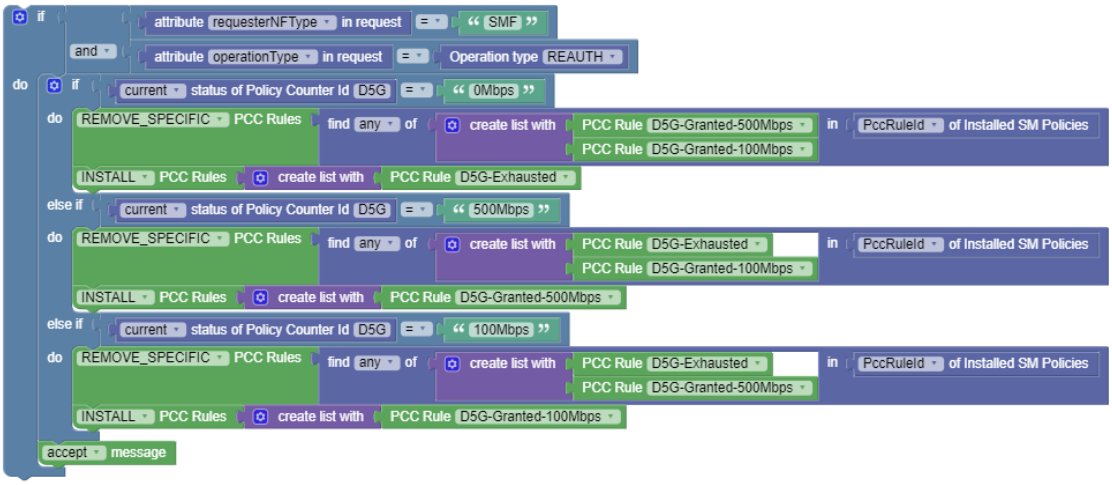
When PCF receives an npcf-smpolicycontrol update association message due to PLMN_CHANGE, update a Session Rule and PCC Rule based on the MCC-MNC received. The following screen capture shows the created policy after applying the above policy rules:



Use Case 3

When PCF receives Policy Counter Status from the Nchf interface, remove the previous rule and install a new PCC rule based on the current status of the Policy Counter.

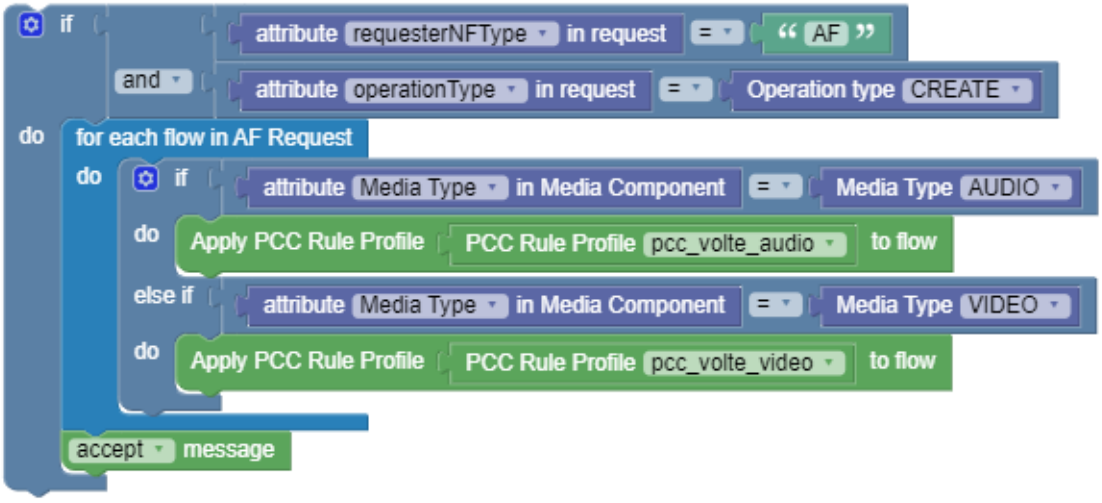
The following screen capture shows the created policy after applying the above policy rules:



Use Case 4

When PCF receives a npcf-policyauthorization create association request, which might be a translated Rx AAR request, then override PCC rules for the received flows based on the media type. If there are no policies, PCF generates a default flow and sends it to smf. To change this default flow, a policy is required.

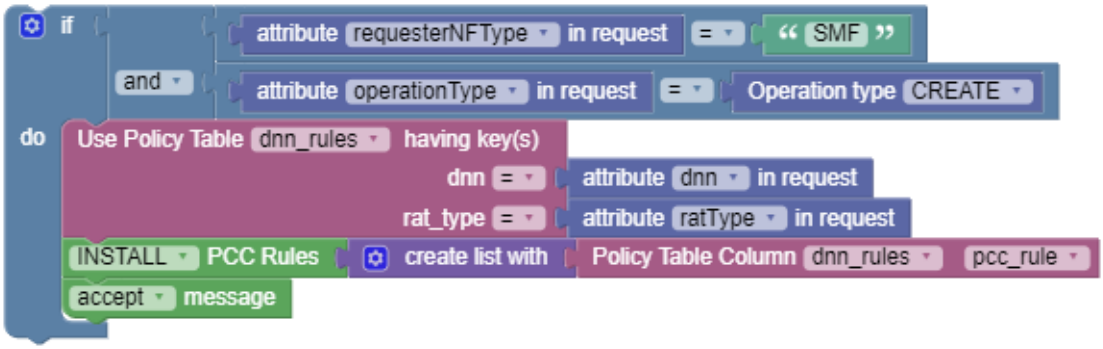
The following screen capture shows the created policy after applying the above policy rules:



Use Case 5

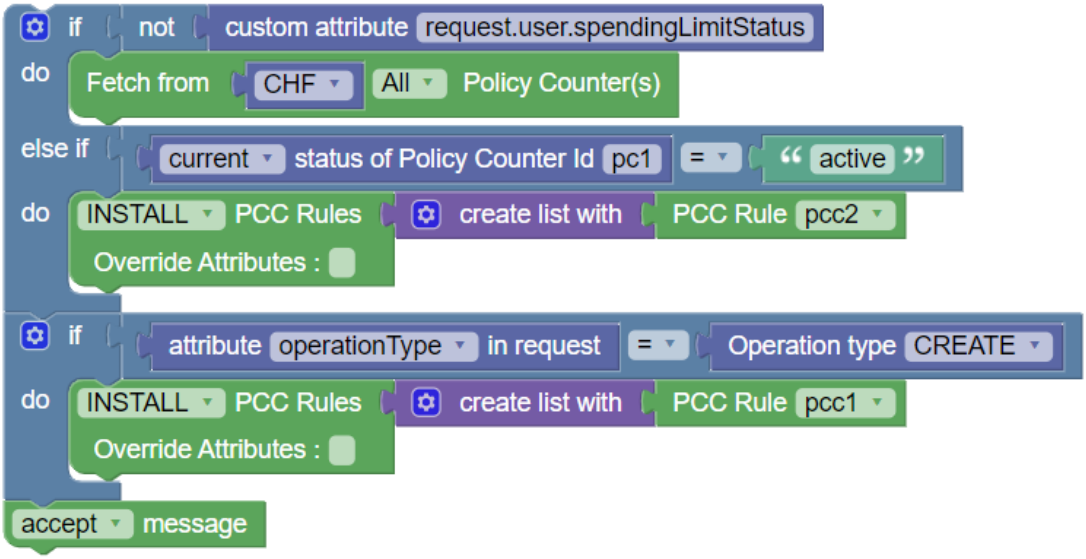
Check the DNN and RAT type in the smf create message, and then install a corresponding PCC Rule. The data is received from the Policy Table.

The following screen capture shows the created policy after applying the above policy rules:



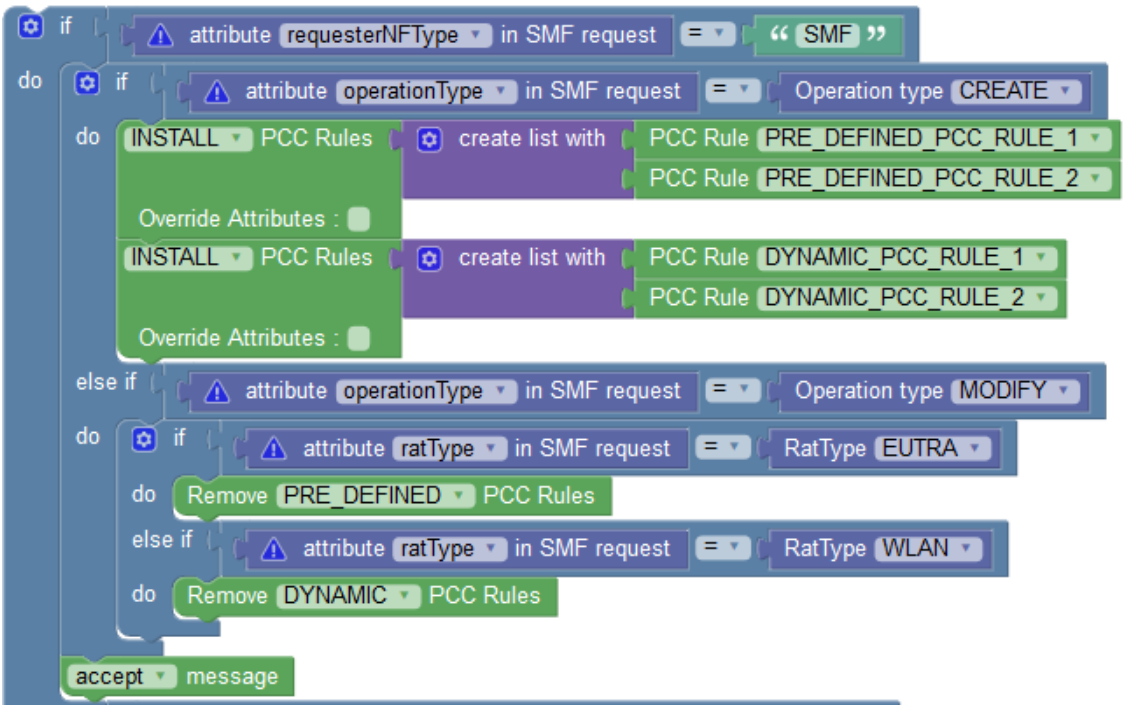
Use Case: Fetch Policy Counters from CHF

The following screen capture shows a sample policy condition to check if **spendingLimitStatus** is present or not in PRE request. If it is not present then it gives action to **fetchFromCHF** to SM service. Currently, PDS uses workflow for processing.



Use Case: Remove PCC Rules in Bulk

The following policy example shows how you can use **Remove PCC Rules** block to remove pre-defined and dynamic PCC rules in bulk.



In the above example, the policy removes pre-defined PCC rules when SM policy association update request changes *ratType* to EUTRA. Similarly, when SM policy association update request changes *ratType* to WLAN, policy removes dynamic PCC rules.

When PCF triggers INSTALL and REMOVE actions on the same PCC/Session Rules when the remove action is **Remove ALL** (ALL, Predefined, Dynamic, Conditioned, non-conditioned), the conflict is resolved based on the value of **Install/Remove Rule Conflicts Strategy** parameter under the **Rule** group on the **PCF Session Management** page in CNC Console.

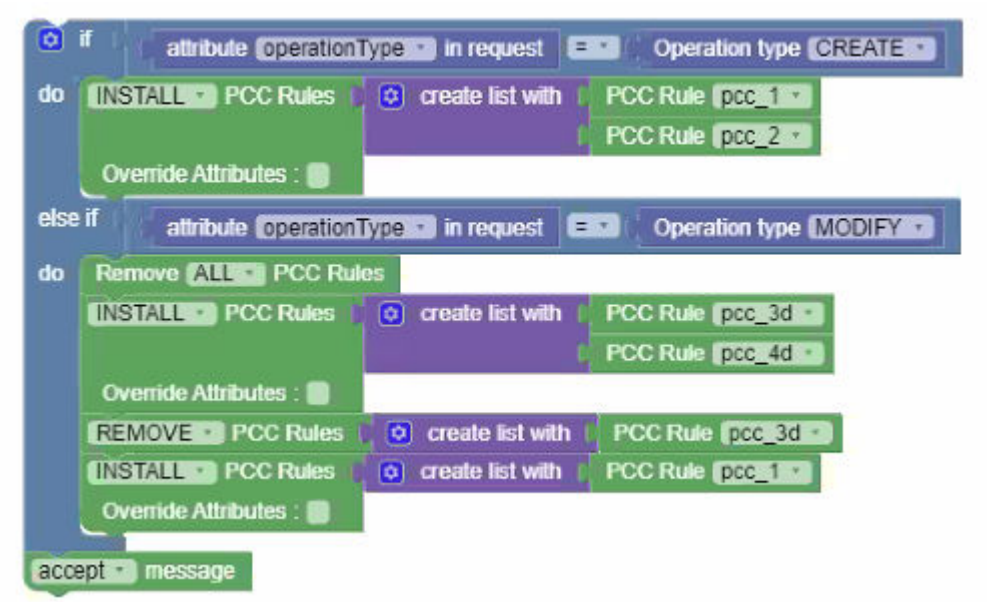
The **Install/Remove Rule Conflicts Strategy** parameter can take the following values:

- `INSTALL/MODIFY`: Indicates to Remove all Session/PCC Rules previously installed and ignore all the remove actions for rules in conflict.
- `REMOVE`: Indicates to Remove all Session/PCC Rules previously installed and ignore all the install actions for rules in conflict.
- `IGNORE`: Indicates to Remove all Session/Pcc Rules previously installed and ignore all actions for rules in conflict, and does not run anything(install/remove).
- `Default`: Process the remove actions and then the INSTALL or MODIFY actions.

If **Install/Remove Rule Conflicts Strategy** parameter is not configured, the project first runs the INSTALL and MODIFY actions and then runs REMOVE action for the PCC rule/ Session.

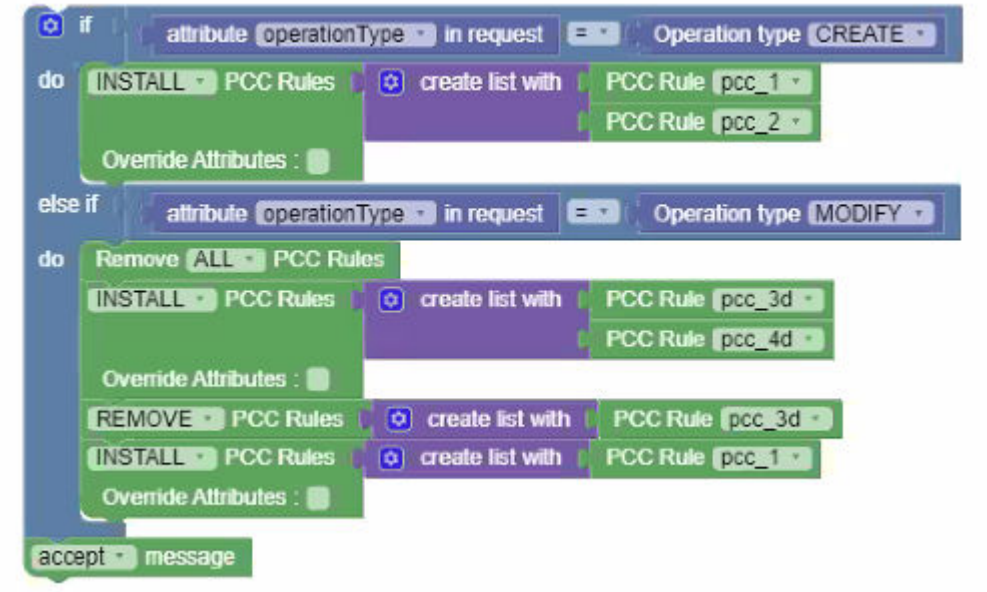
Following are some of the examples of conflict resolution:

Figure 4-1 Example 1



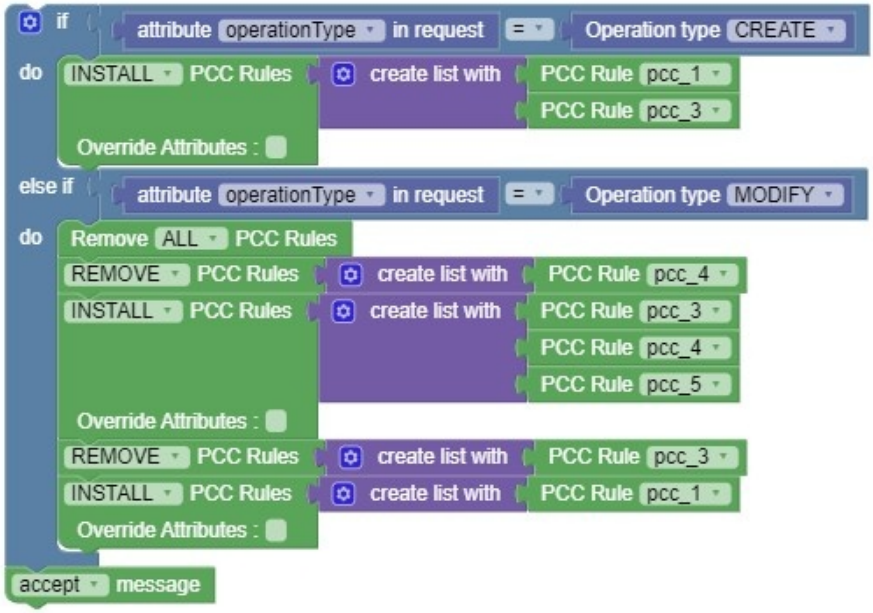
- Removes the previously installed pcc_1 and pcc_2.
- Installs pcc_3d and pcc_4d.

Figure 4-2 Example 2



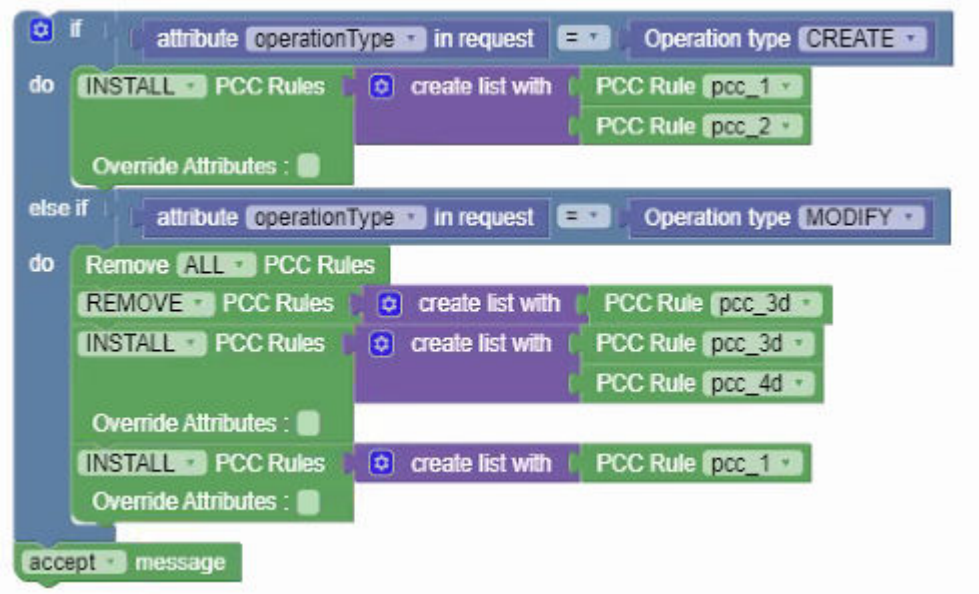
- Removes the previously installed pcc_1 and pcc_2.
- Installs pcc_4d.
- Ignores installation of pcc_1 and pcc_3d which are in conflict.

Figure 4-3 Example 3



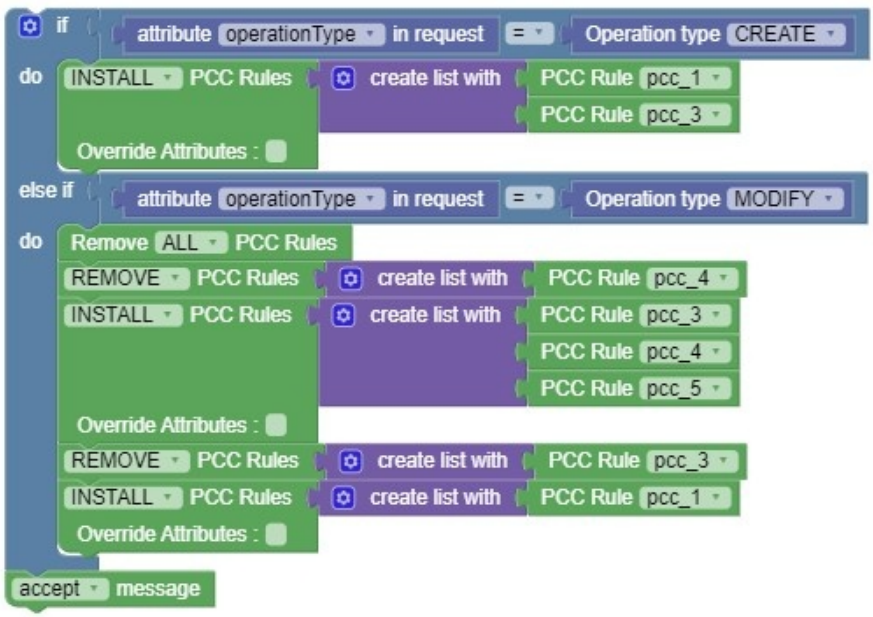
- Removes the previously installed pcc_1 and pcc_3.
- Installs pcc_4.
- Ignores install or remove actions on pcc_1 and pcc_3 which are in conflict.

Figure 4-4 Example 4



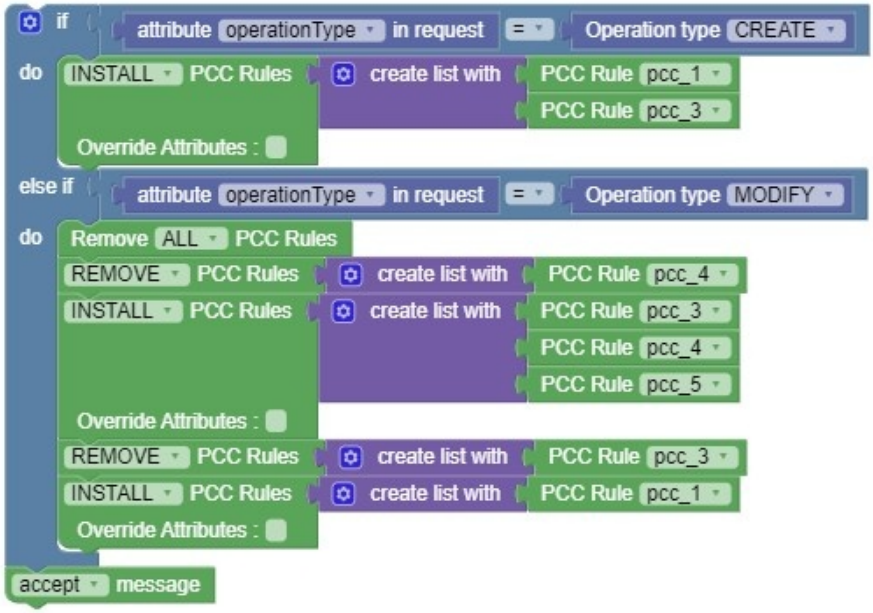
- Removes the previously installed pcc_1 and pcc_2.
- Installs pcc_3d, pcc_4d_ and pcc_1

Figure 4-5 Example 5



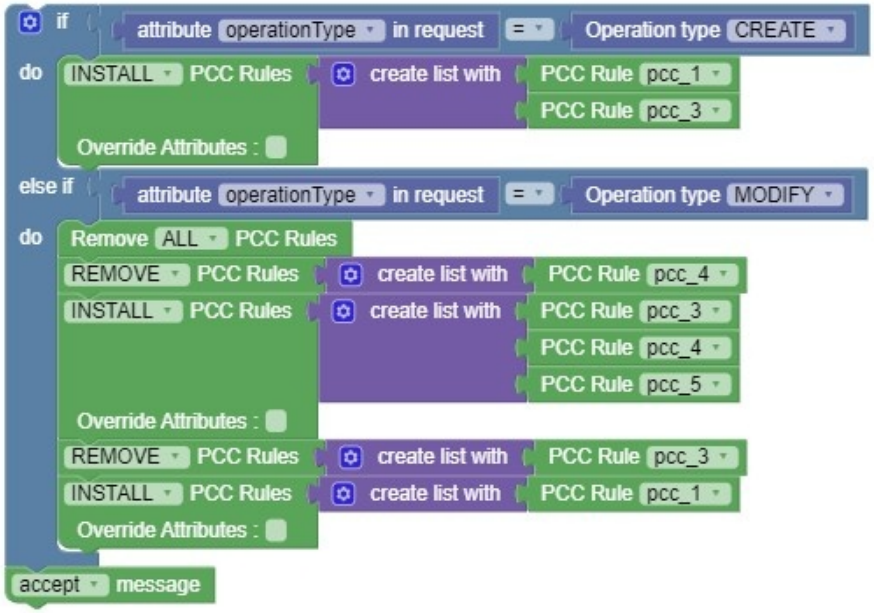
- Removes the previously installed pcc_1 and pcc_3.
- Installs PCC Rules pcc_4 and pcc_5.
- Ignores installation of pcc_1 and pcc_3 which are in conflict.

Figure 4-6 Example 6



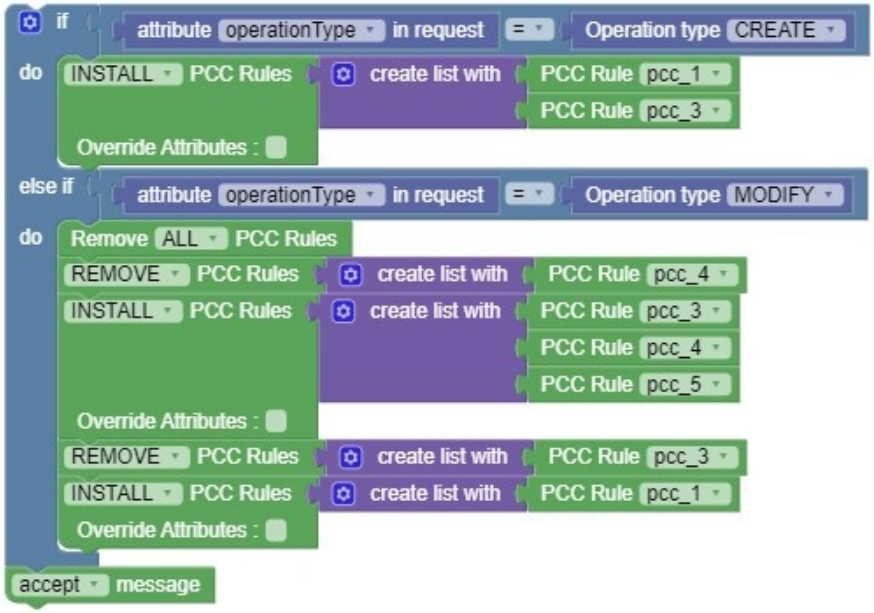
- Removes previously installed pcc_1 and pcc_3.
- Installs PCC Rule pcc_5.
- Ignores installation of pcc_3 and pcc_4.

Figure 4-7 Example 7



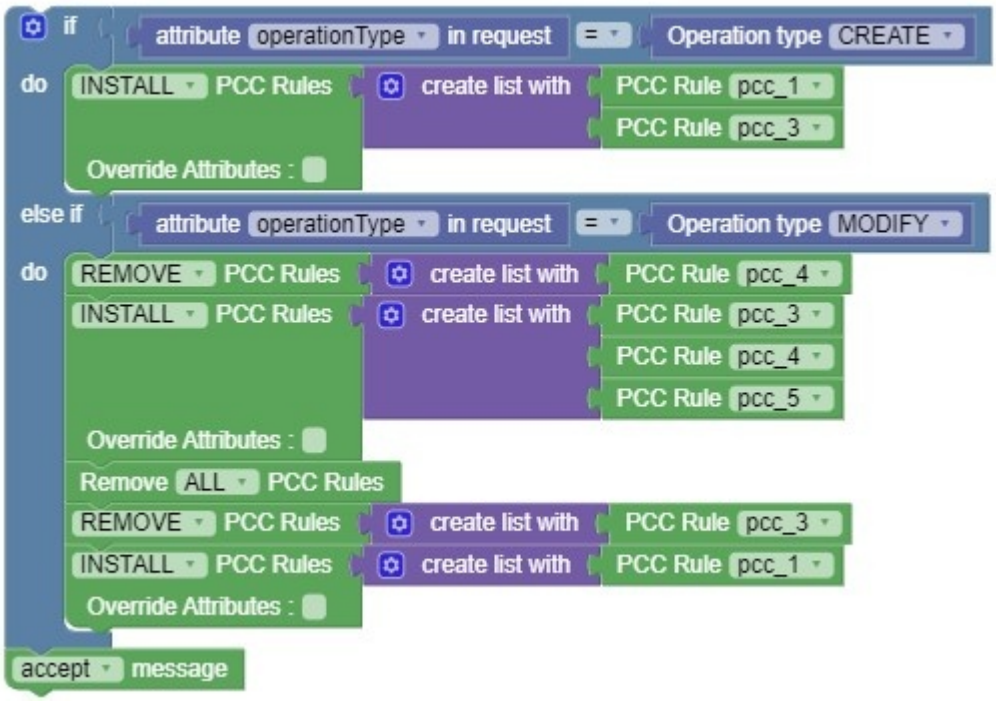
- Removes previously installed pcc_1 and pcc_3.
- Installs pcc_5.
- Ignores INSTALL/ REMOVE actions on pcc_1 and pcc_3.

Figure 4-8 Example 8



- Removes previously installed pcc_1 and pcc_3.
- Installs pcc_4 and pcc_5.

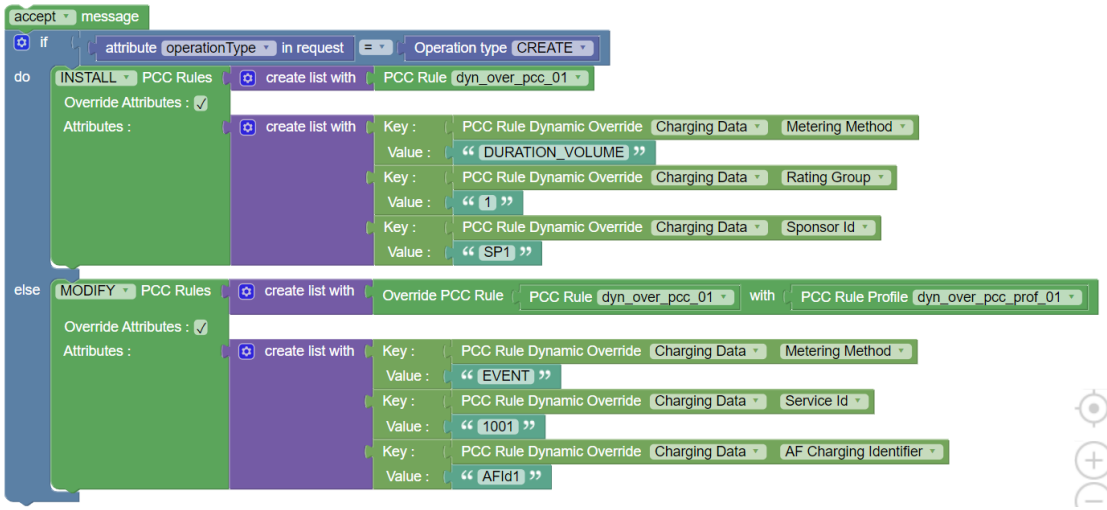
Figure 4-9 Example 9



- Removes previously installed pcc_1 and pcc_3.
- Installs pcc_4 and pcc_5

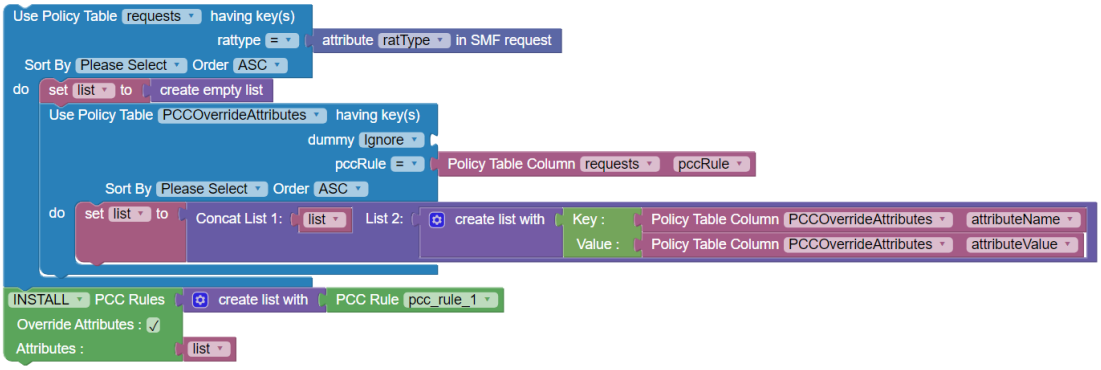
Use Case: Dyamic Update/Override of PCC Rule Attributes

The following policy example shows how you can override PCC rule attributes in real-time. It shows a create request to install PCC rule dynamically overriding Charging Data attributes.



Use Case: Dynamic Override of PCC Rule Attributes with Policy Tables

The following policy example shows how you can use nested policy tables to override PCC rule attributes in real-time.



In the above policy:

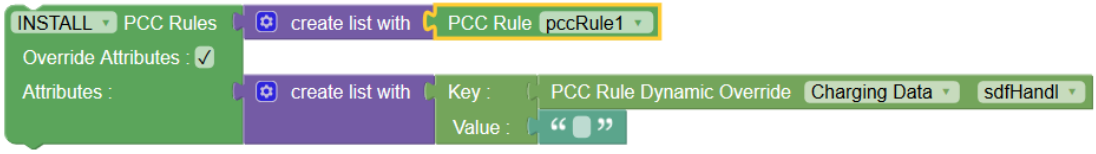
- Outer **Use Policy Table** block filters table data by rattype that is received in request.
- Inner **Use Policy Table** block loops through override attributes and their values for particular PCC Rule. After this step, list of override attributes becomes available.

> **Note**
>
> **Concat List** block is used to append {key:value} pair of attributes to **list** variable.

- The list, received in the previous step, is directly added to override attributes in **Install PCC Rule** block.

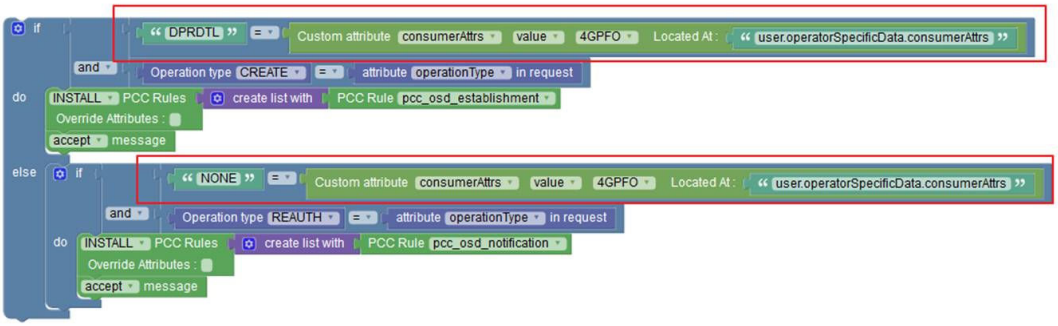
Use Case: Override sdfHandl attribute

The following sample policy shows how operators can use **PCC Rule Dynamic Override** block to override the value of sdfHandl attribute of Charging data. This attribute indicates whether the service data flow is allowed to start while the SMF is waiting for a response to the credit request from CHF.



Use Case: Using Custom Attributes block for OperatorSpecificData

The following policy example shows how you can use Custom Attributes block to get value from **OperatorSpecificData** object.



> **Note**
>
> When you select one attribute, the child attributes automatically appear in block. The attribute list is imported from the custom JSON schema.

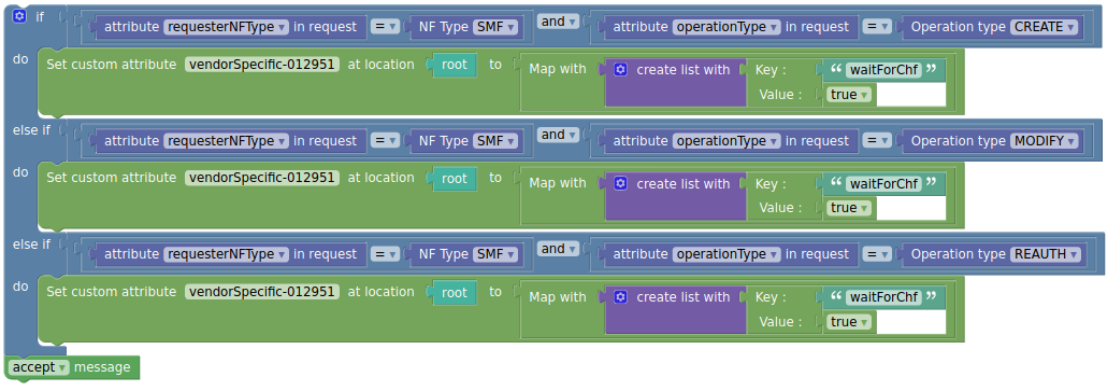
Use Case: WaitForChf VendorSpecific attribute provisioning over N7

Using the **Set custom attribute** block, operators may configure and send VendorSpecific **waitForChf** attribute to SMF in SMPolicyDecision via policy. Depending on the **waitForChf** attribute value, it is decided whether the SMF waits for the CHF session establishment response before installing rules in the UPF or sending the response towards the RAN.

If this attribute is included and set to true (default), SMF waits before proceeding with the UPF and RAN signaling.

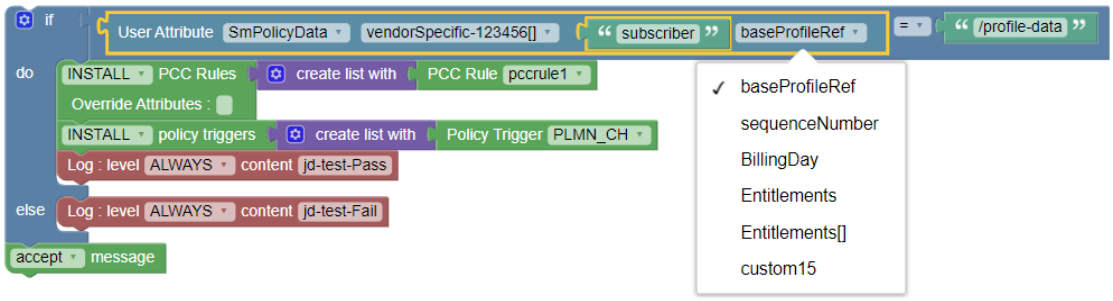
> **Note**
>
> The **waitForChf** attribute is not present when the online charging method is not applicable to the PDU session or to any of the PCC rules.

The following sample policy shows how operators can use **Set custom attribute** block to send VendorSpecific **waitForChf** attribute to SMF in SMPolicyDecision:



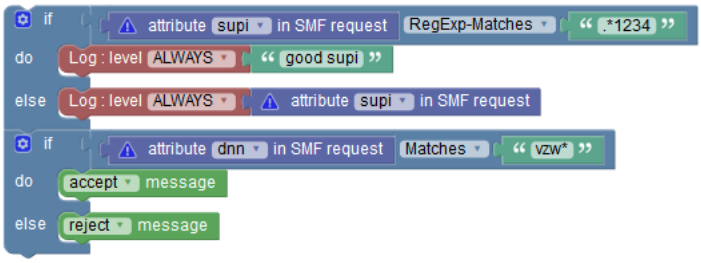
Use Case: Using User Attributes block for SmPolicyData

The following screen capture shows a sample policy where User Attributes block is used to access `vendorSpecific-123456` attribute and trigger a policy:



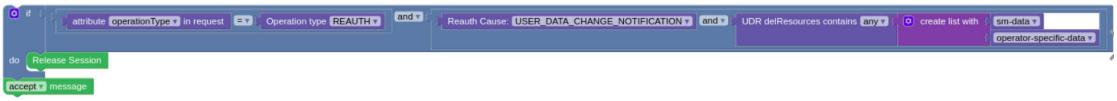
Use Case: Wildcard character matching

The following policy example shows how operators can use comparison block for wildcard pattern matching:



Use Case: UDR Subscriber Delete Resources

The following screen capture shows a sample policy to release a policy association and terminate active subscriber session by SM service when the subscriber resources are deleted on the UDR.



Use Case: PRE capturing log information using Log Blocks

PRE service records log information when an event occurs using blockly. In blockly, any condition blocks such as the accessor blocks are used along with log blocks to log application information. It logs subscriber identifier values of SUPI, GPSI, DNN, MCC-MNC. The Policy tables data are also logged.

The following screen capture shows a sample of enabling logging in PCF-SM.

Figure 4-10 Example 1: Blockly logging supi, gpsi, dnn and ratType values

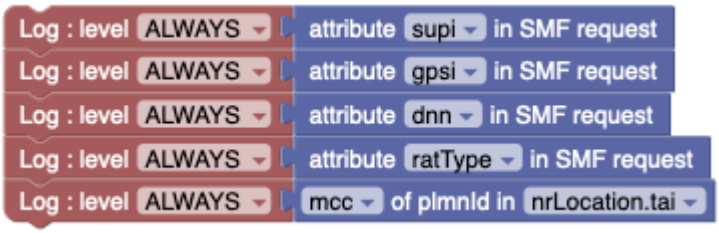


Figure 4-11 Example 2: Blockly logging the SM Policy data from the Policy table

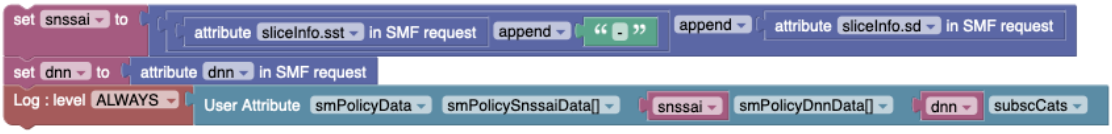
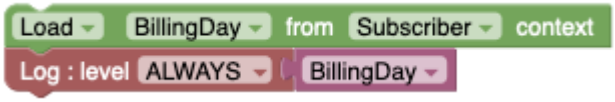


Figure 4-12 Example 3: Blockly logging the Subscriber billing details



4.2 PCF UE Use Cases

This section describes use cases where PCF UE blocks are used to evaluate policies.

Support for policy Evaluation after N1Message Notify

Table 4-1 Sample Policies Project

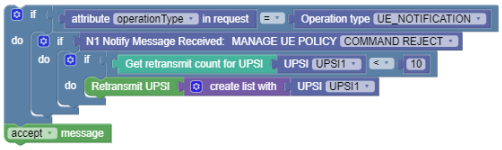
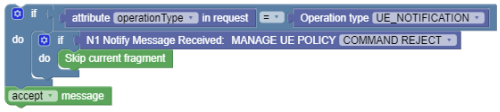
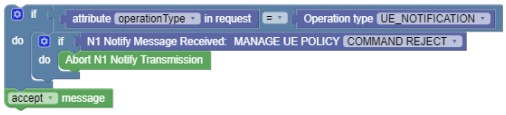
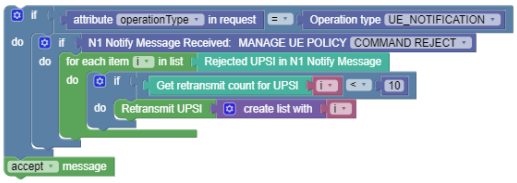
Policy	Description
Figure 4-13 Use case scenario 1: 	This policy will retransmit UPSI1 until the retransmit action has happened 10 times. **Note**: The get retransmit count for UPSI statement is important since it will allow the policy to retransmit in a finite amount of times, otherwise it can go in an infinite loop.
Figure 4-14 Use case scenario 2: 	This policy skips the current transmit after encountering a Command Reject message from the AMF.
Figure 4-15 Use case scenario 3: 	This policy aborts the current transmit after encountering a Command Reject message from the AMF.

Table 4-1 (Cont.) Sample Policies Project

Policy	Description
	This policy retransmits every rejected UPSI up to a maximum of 10 times.

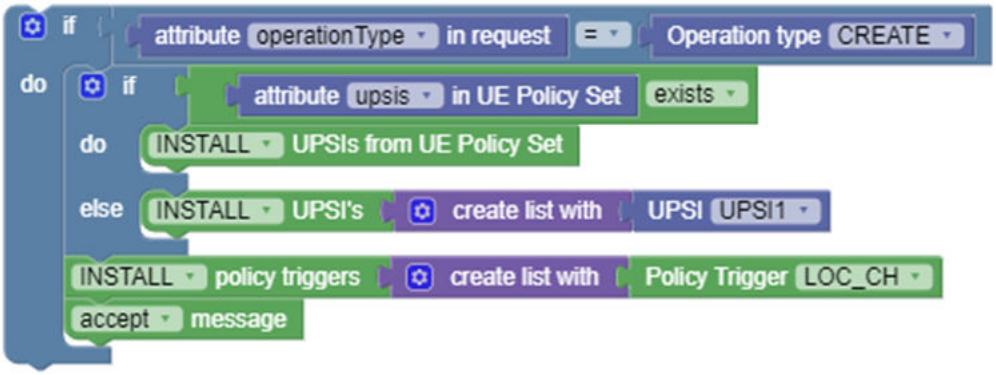
Figure 4-16 Use case scenario 4:



Use Case 1

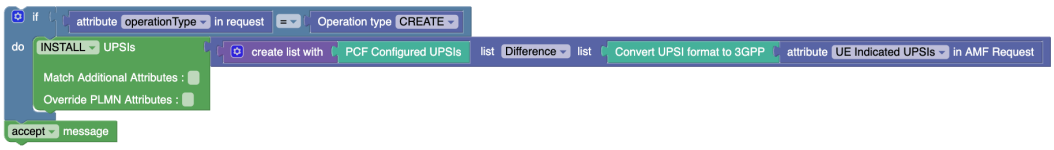
The given screen capture shows a sample UE policy that evaluates if the subscriber profile for UE Policy in the UDR (UEPolicySet) has UPSIs provisioned, and then sends the same to UE in the N1 message transfer command. If not, it sends a configured UPSI. In addition, it arrms the location change trigger on the AMF.

Figure 4-17 PCF UE use case



Sample projects to list and compare UPSIs received from UDR

To get the delta of UPSIs between the PCF configured UPSIs and the ones on AMF



Example:

PCF Configured UPSIs has UPSIs ids 1,2,3,4.

UE Indicated UPSIs in AMF Request has UPSIs ids 3,4,5,6.

Expected output of this project:

Install the delta of the UPSIs 1 and 2.

To get the Intersection of UPSIs between the PCF configured UPSIs and the ones from UDR

Example:

PCF Configured UPSIs has UPSIs ids 1,2,3,4,5.

UE Policy Set from UDR has UPSIS 5,6.

Expected output of this project:

Remove the common UPSI 5.

To get the delta of UPSIs between the PCF configured UPSIs and the ones on AMF and validate the matching parameters

Example:

PCF Configured UPSIs has UPSIs ids 1,2,3,4

UE Indicated UPSIs in AMF Request has UPSIs ids 3,4,5,6.

VSA UPSIs from UDR has UPSIS 5,6.

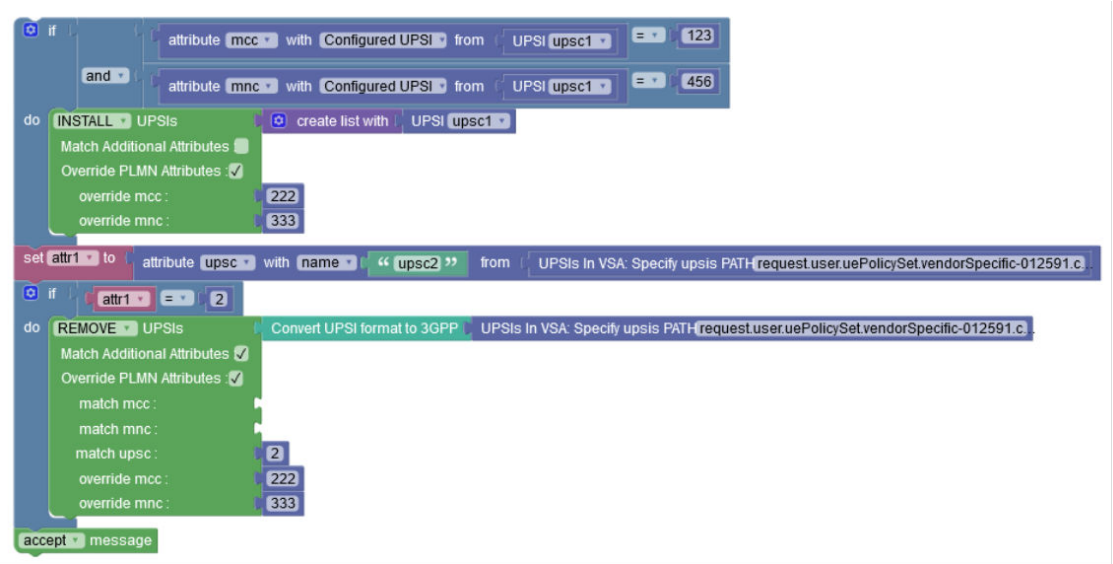
Expected output of this Policy project:

1. Install the UPSIs 1 and/or 2 if, for each of these UPSIs, its corresponding upsc is equal to 345, and override its PLMN to be 222-333.

2. Remove the UPSIs 5 and/or 6 if, for each of theseUPSIs, its corresponding mcc is equal to 340 and mnc equals to 350, and override its PLMN to be 222-333.

Note: When Match Additional Attributes option is enable, it is not mandatory to fill all the attributes with a value, as shown in example.

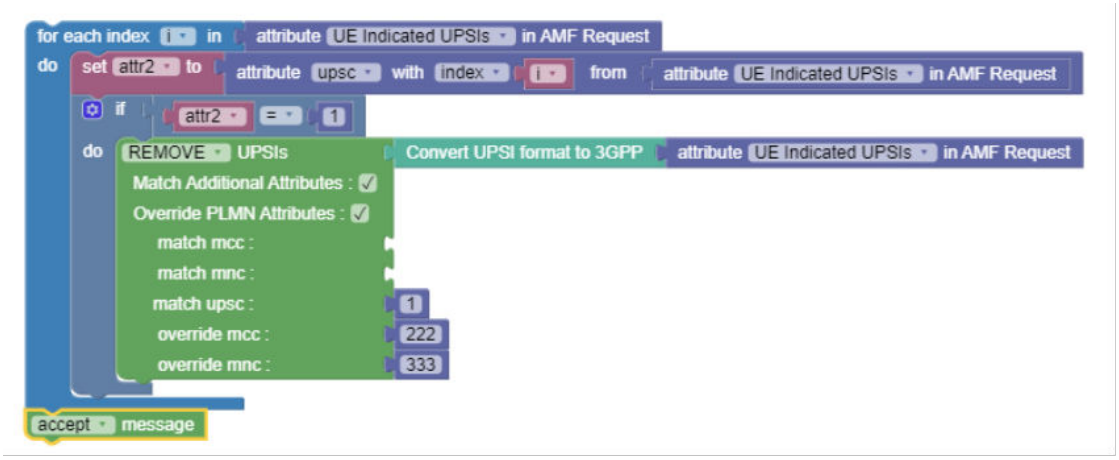
To check for specific attributes values from the PCF Configured UPSIs and the ones that are on VSA by name



In this example, the first part of the blockly will install the "upsc1" upsi if its mcc equals to 123 and mnc equals to 456 and override its PLMN to be 222-333.

Similar for the second part, it will assign a variable called attr1 with the attribute of upsc from the UPSI which has the name "upsc2" on the VSA UPSIs list, and if this value is equal to 2, it will remove this UPSI and will override its PLMN to be 222-333.

To loop on all the UPSIs that are located on AMF Request



This policy will loop on all the UPSIs that are located on AMF Request.

It allows to access an attribute from specific UPSI on AMF Request. In this example, it allows to check if any of the UPSIs on the list has its upsc as 2.

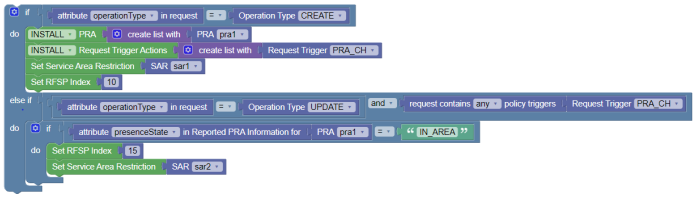
If found, it removes the corresponding UPSI and overrides its PLMN to be 222-333.

4.3 AM Use Cases

This section describes use cases where PCF AM blocks that are used to evaluate policies.

Use Case 1

The given screen capture shows a sample AM policy that if the request received by AM service is create, it installs configured PRA (Presence Reporting Area), trigger, i.e., PRA_CH, SAR (Serivce Area Restriction) and RFSP Index. If the service receives Update request and request contains trigger PRA_CH and if the value in already configured PRA for that user is "IN_AREA" then the RFSP index and SAR for that user is updated.



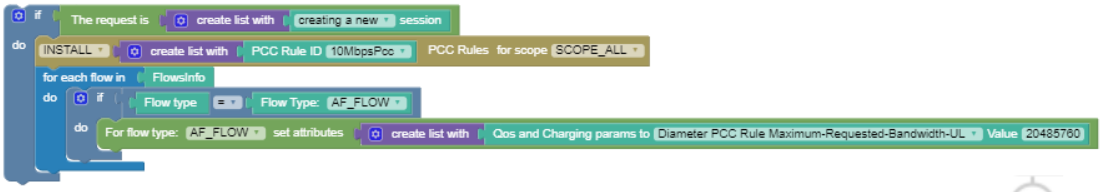
4.4 Cloud Native Policy Charging and Rules Function Use Cases

Following are the Cloud Native Policy Charging and Rules Function (PCRF) use cases:

Use Case 1

When Cloud Native PCRF receives CCR-Initial requests, install 10MbpsPcc Rule. When Rx flow is observed, then modify the upload limit to 20 MBPS**.**

The following screen capture shows the created policy after applying the above policy rules:

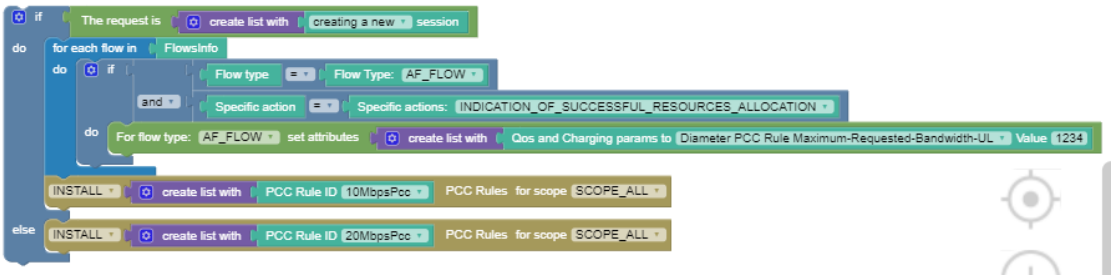


Use Case 2

When Cloud Native PCRF receives CCR-Initial requests, install 10MbpsPcc Rule. When Cloud Native PCRF receives CCR-Update requests, install 20MbpsPcc Rule.

After Cloud Native PCRF receives CCR-Initial requests, when Rx flow is observed and specific action is INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION taken, then modify the maximum upload limit to 1234 MBPS.

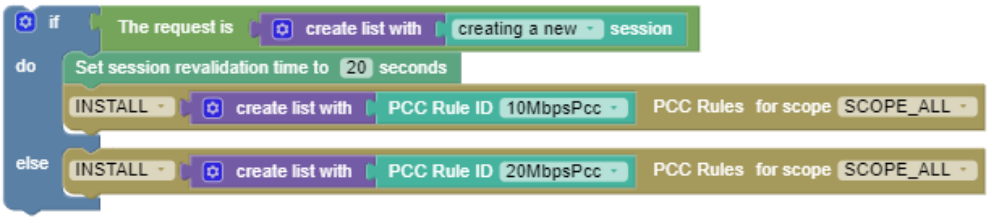
The following screen capture shows the created policy after applying the above policy rules:



Use Case 3

When Cloud Native PCRF receives CCR-Initial requests, install 10MbpsPcc Rule for the next 20 seconds. When Cloud Native PCRF receives CCR-Update requests, install 20MbpsPcc Rule.

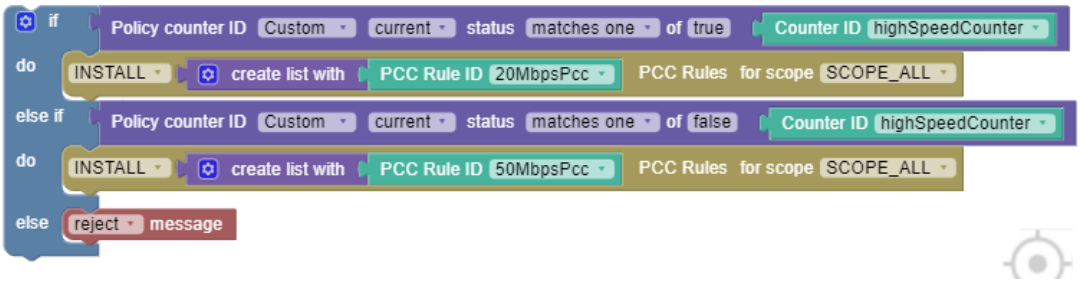
The following screen capture shows the created policy after applying the above policy rules:



Use Case 4

When highSpeedCounter is received with current status as true from OCS, install 20MbpsPcc Rule. When highSpeedCounter is received with current status as false from OCS, install 50MbpsPcc Rule. For rest of the scenarios, such as when highSpeedCounter is not received from OCS or does not have current status as true or false, perform the "reject message" action.

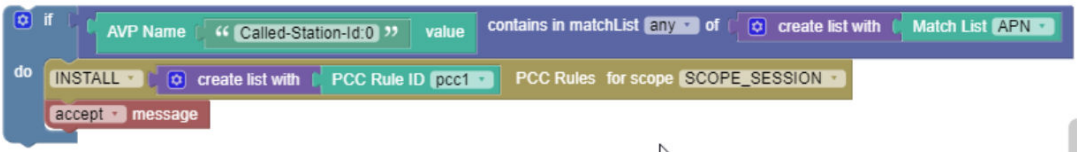
The following screen capture shows the created policy after applying the above policy rules:



Use Case 5

When Cloud Native PCRF receives requests with APN, install pcc1 Rule.

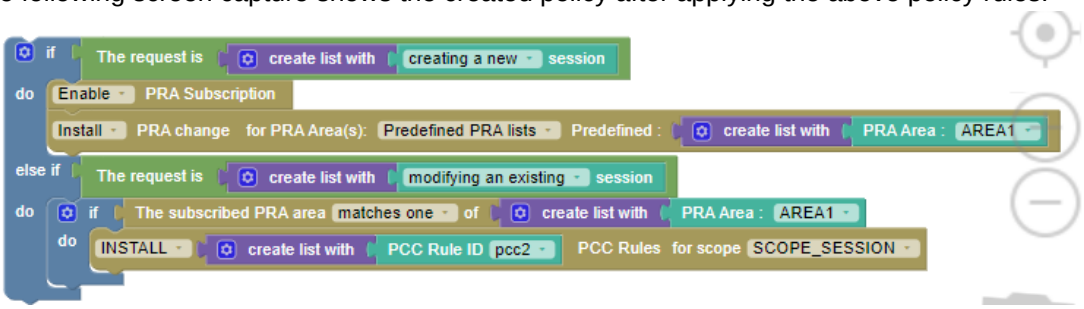
The following screen capture shows the created policy after applying the above policy rules:



Use Case 6

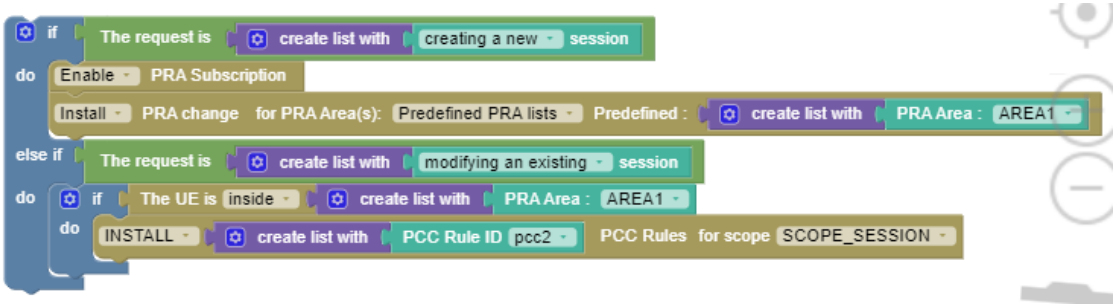
Single PRA: Installing PRA on initial request and removing on update request.

The following screen capture shows the created policy after applying the above policy rules:



Multiple PRA: Installing PRA on initial request and removing on update request.

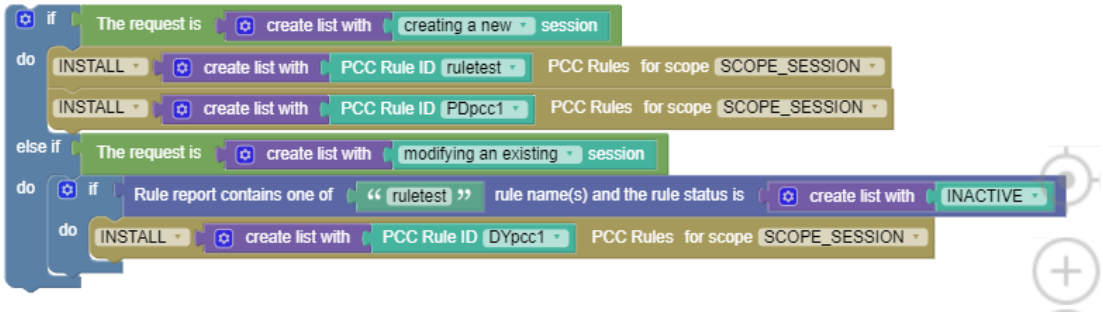
The following screen capture shows the created policy after applying the above policy rules:



Use Case for Rule Report Conditions

The following screen capture shows the created policy for rule report conditions:

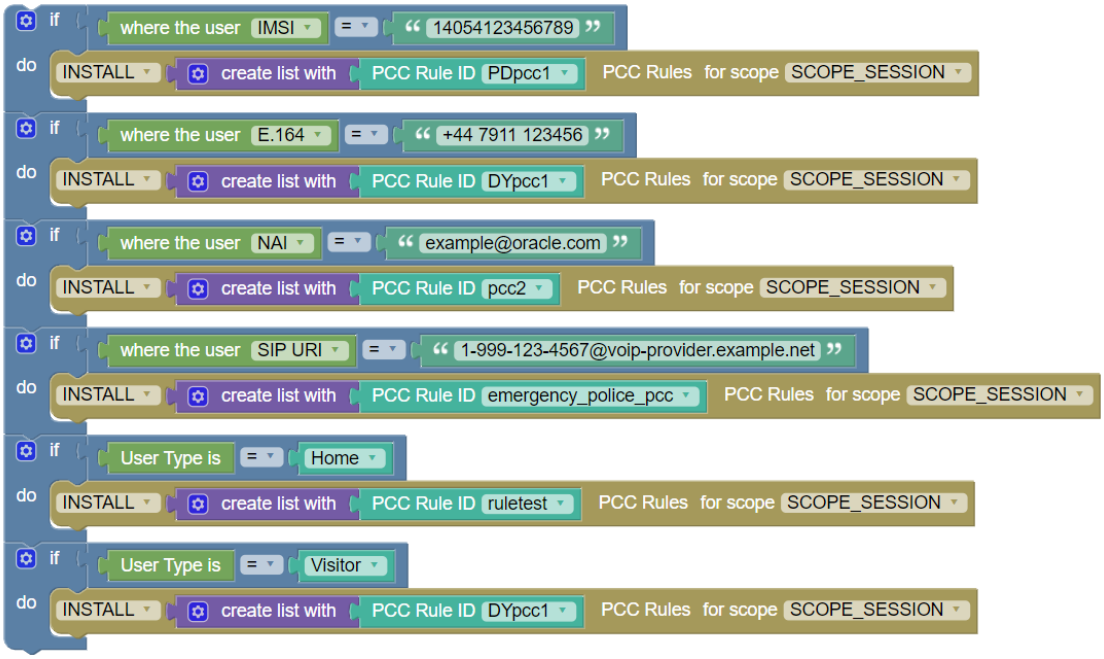
Figure 4-18 Use case for Rule Report Conditions



Use Case for User Specific Conditions

The following screen capture shows the created policy for user specific conditions:

Figure 4-19 Use case for User specific conditions



4.5 Subscriber Notification Use Cases

This section describes the Subscriber notification use cases.

Use Case 1

When HTTP end point is used for communication between Notification Service and the external Notification Server, to configure the URI based parameters, use the `PATH` key for HTTP Header blockly.

The `PATH` key accepts the url values from dynamic variables that are built with variables taken from object expression or other blocks.

> **Note**
>
> The HTTP Header key: `PATH` must be in all capital letters as shown here.

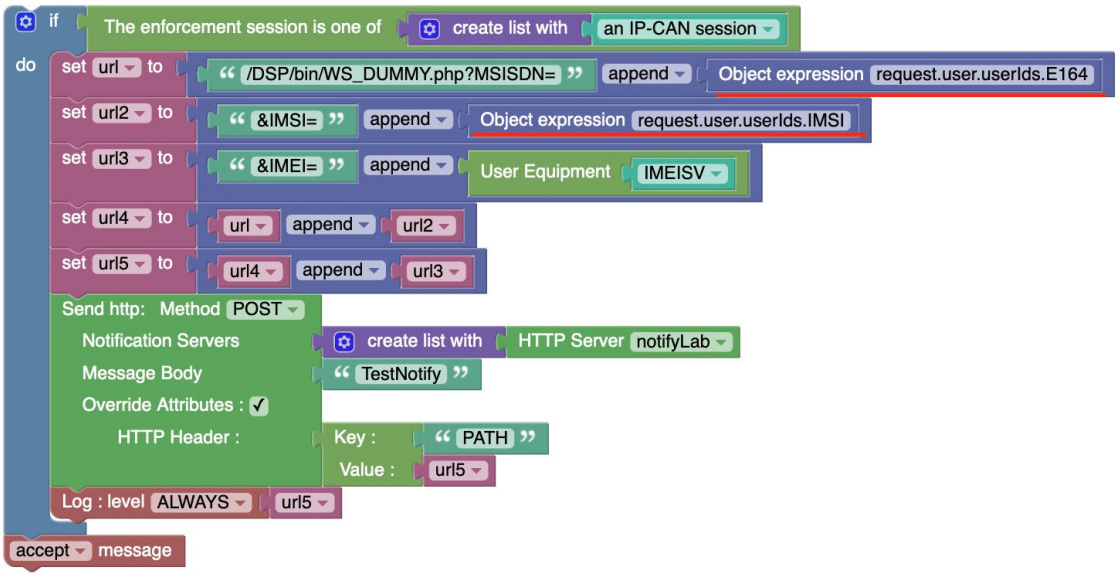
The complete URI comprises the IPv4/IPv6/FQDN[:Port] (from the static configuration) followed by the value of the `PATH` key.

where [:Port] is optional. If port number is not specified, default port will be used.

If you are not using dynamic parameters, you can use the static UriPath from the configuration.

The value of `PATH` key will override the statically configured `URI Path`.

Figure 4-20 Configuring URI Based Parameters for Subscriber Notification



Use Case 2

When Notifier Service uses Short Message Service (SMS) based notification via an SMS gateway for communication between External Short Message Entities (ESME) and internal Message Centres (MC), use `Send SMS` action.

You can include text strings as message body and specify the Destination address with User IDs.

The list of User IDs includes:

- E164
- IMSI
- NAI
- IP
- SIP
- IMEI

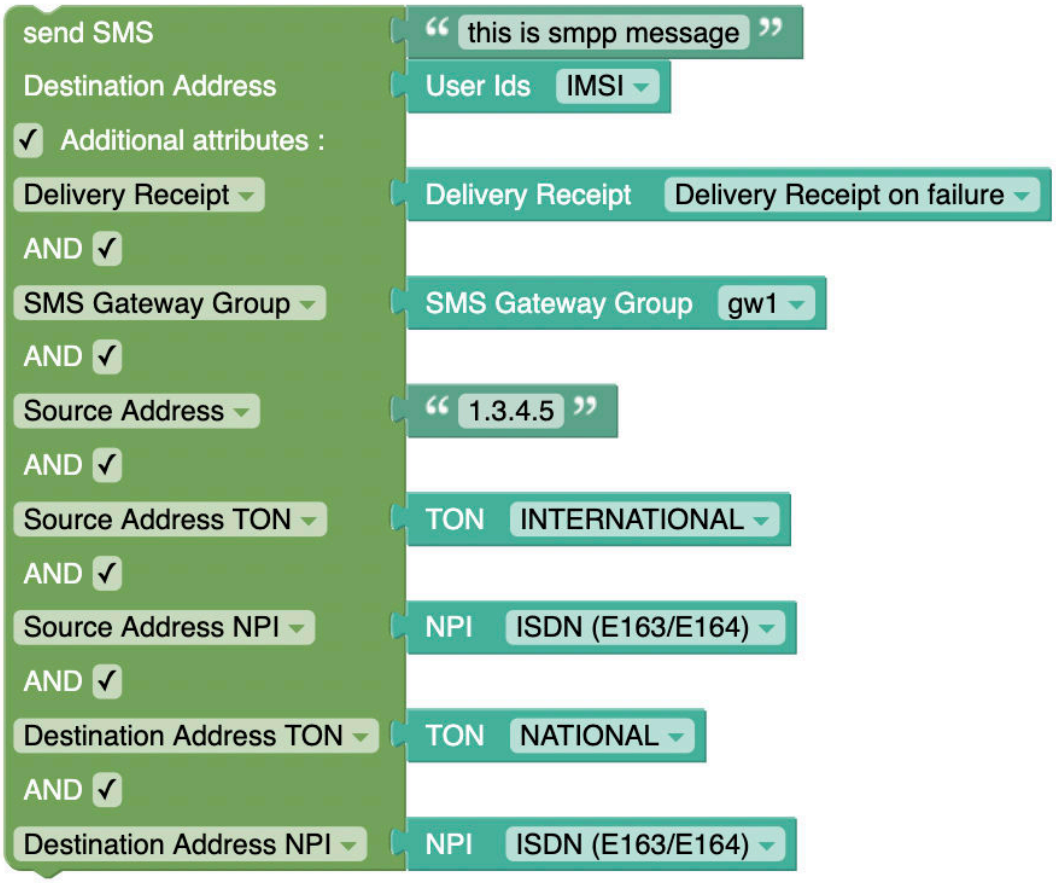
- IPO

The text message accepts string values and supports multiple languages.

To use `Send SMS` action, you must also configure additional attributes:

- Source Address
- Source Address TON
- Source Address NPI
- Destination Address TON
- Destination Address NPI
- Delivery Receipt
- SMS Gateway Group

Figure 4-21 Sample Send SMS blockly configuration



For more details on `Send SMS` action and the additional attributes that must be configured, see *Subscriber Notification* under Public Category.

> **Note**
>
> As of Policy 23.2.0, this action is supported only for PCRF-Core call flows.

4.6 Usage Monitoring Use Cases

This section includes some of the Usage Monitoring and Control Use Cases.

Home Monthly Plan with Throttling

Scenario

- All data plans are configured in CNC Console.
- Subscriber has purchased a monthly plan. Name of the plan is provided in a vendor specific custom attribute "homePlanName" under SmData.
- As long as subscriber is in the home region and has data left, the subscriber can use this plan.
- Data is denied if the subscriber is in a roaming region.
- QoS Throttling is applied when the data in the plan is exhausted.
- The Billing Day is provided in a vendor specific custom attribute "billingDay" under SmData.

ConfigurationData Limit Profile
In CNC Console, Navigate to Policy Data Configurations → Usage Monitoring → Data Limit Profiles and create a Data Limit Profile.

The following fields are mandatory to be set:

- Name
- Usage Limit
- Reset Period

Attribute Forwarding Profile
In CNC Console, Navigate to Service Configurations → Common Data → Attribute Forwarding Profile and create a Attribute Forwarding Profile with the field values as displayed in the below screenshot.

Figure 4-22 Forwarded Attributes for Home Monthly Plan with Throttling

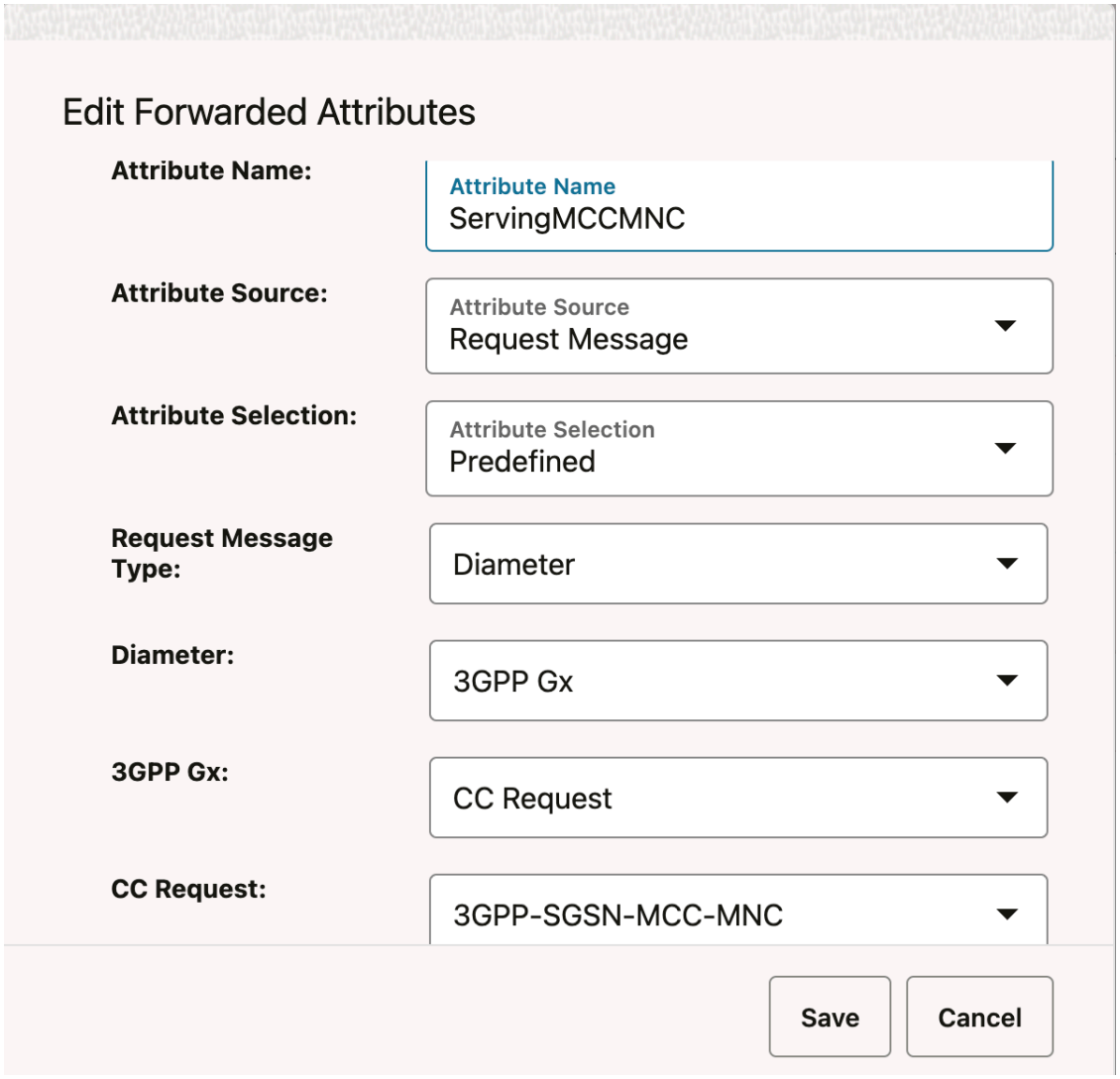


Figure 4-23 Forwarded Attributes for Home Monthly Plan with Throttling for Billing Day as per Vendor Specific attribute in SMData

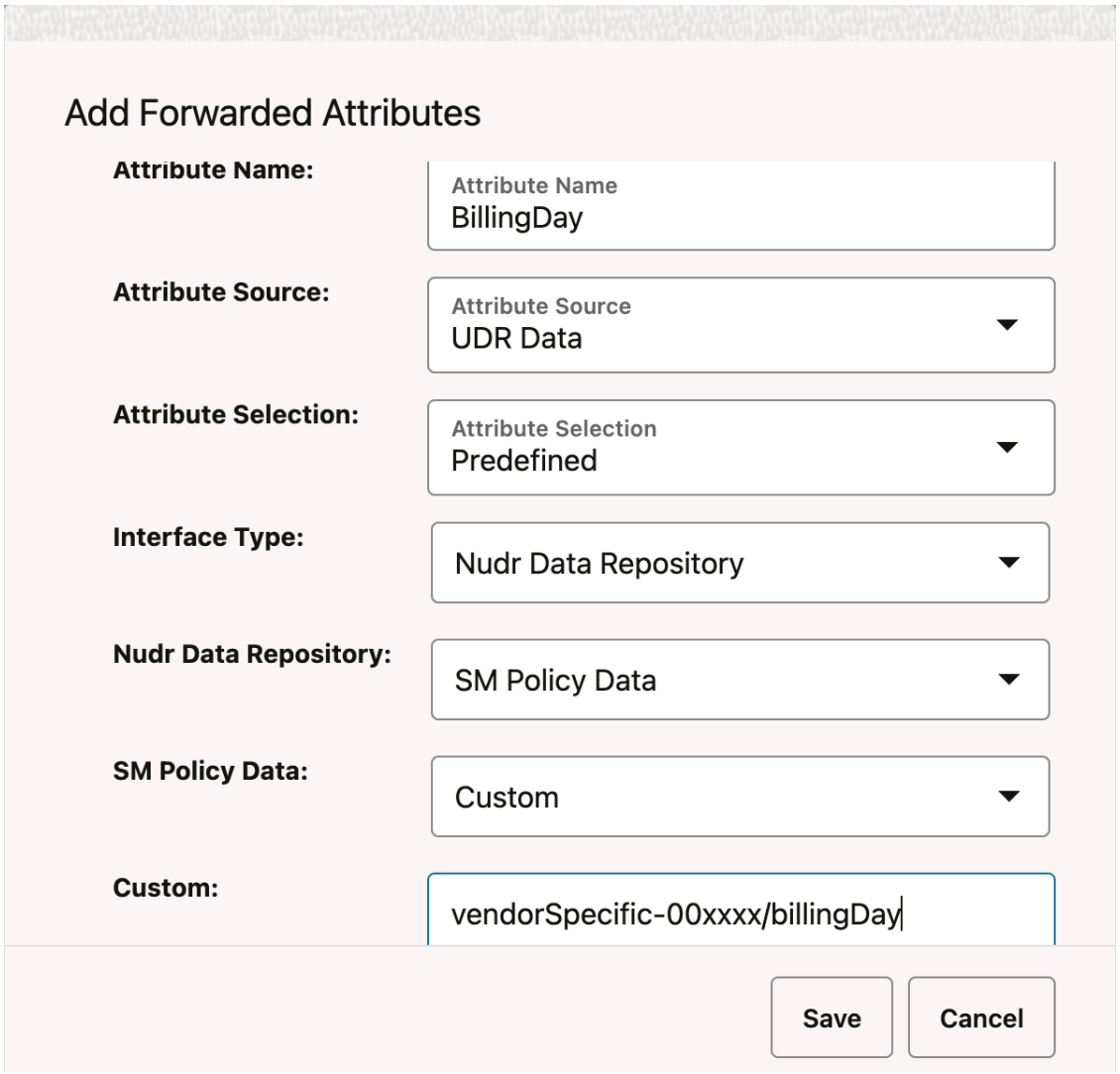
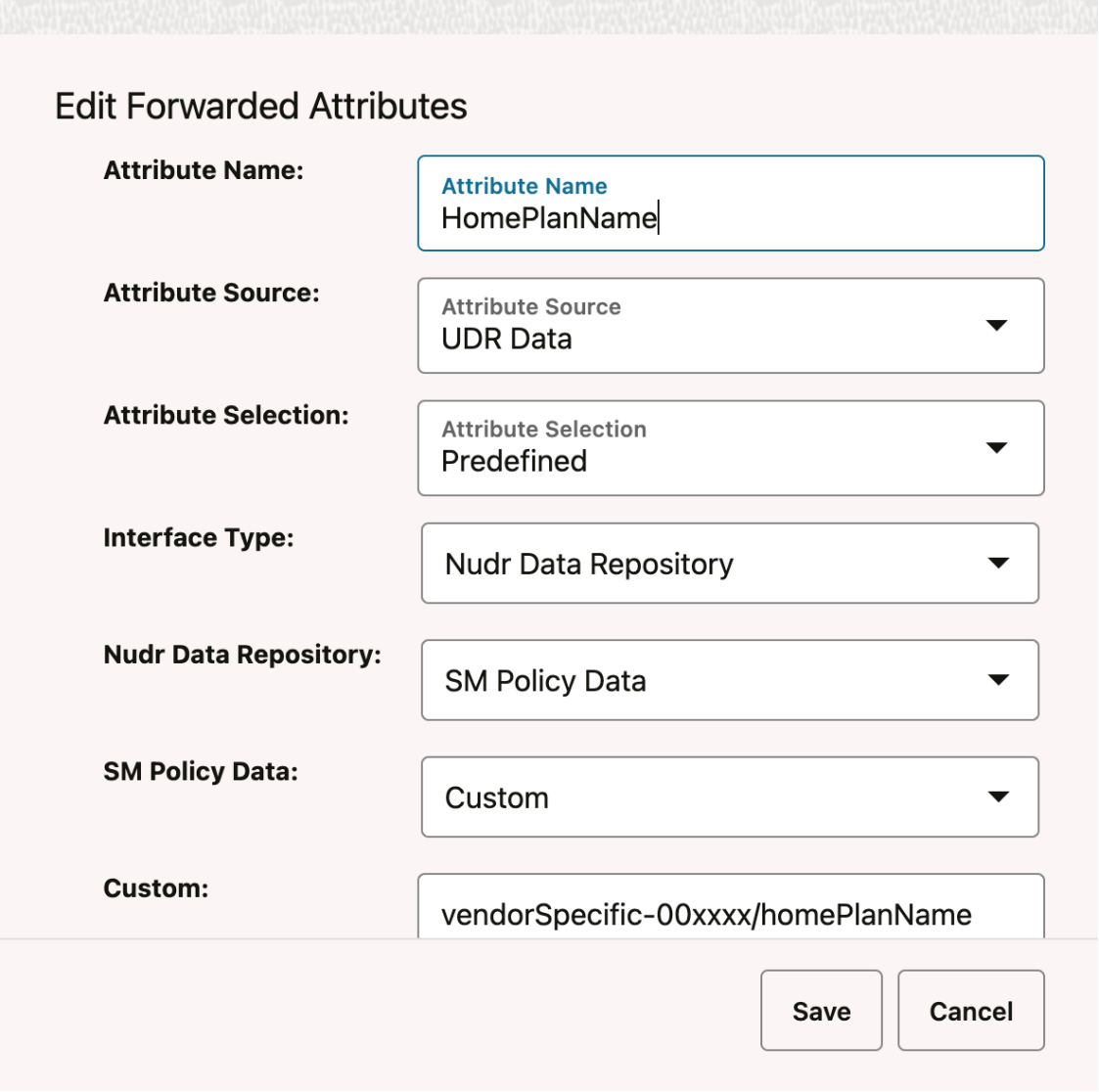


Figure 4-24 Forwarded Attributes for Home Monthly Plan with Throttling



PCRF Core Configuration
In CNC Console, Navigate to Service Configurations → PCRF Core → Settings and set the following field(s) under Usage Monitoring Group:

- Enabled: true
- APN List: the list of APNs for which Usage Monitoring is required.
- Attribute Forwarding: the forwarding profile created for each desired interface/message type.

Usage Monitoring Service Configuration
In CNC Console, Navigate to Service Configurations → Usage Monitoring and set the following field(s):

- Enable PRE: true

Configure other fields as necessary.

Match List

In CNC Console, Navigate to Policy Data Configurations → Common → Match List and create a Match List to fill in the home MCC/MNCs.

Policy Table
Not required for this scenario.

Usage Monitoring Policy

Figure 4-25 Policy Project

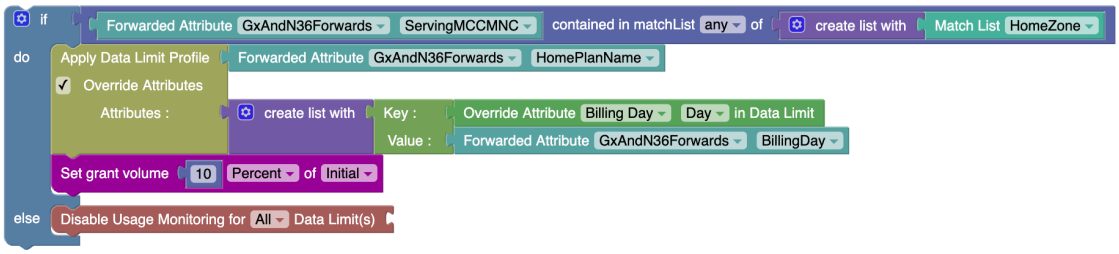
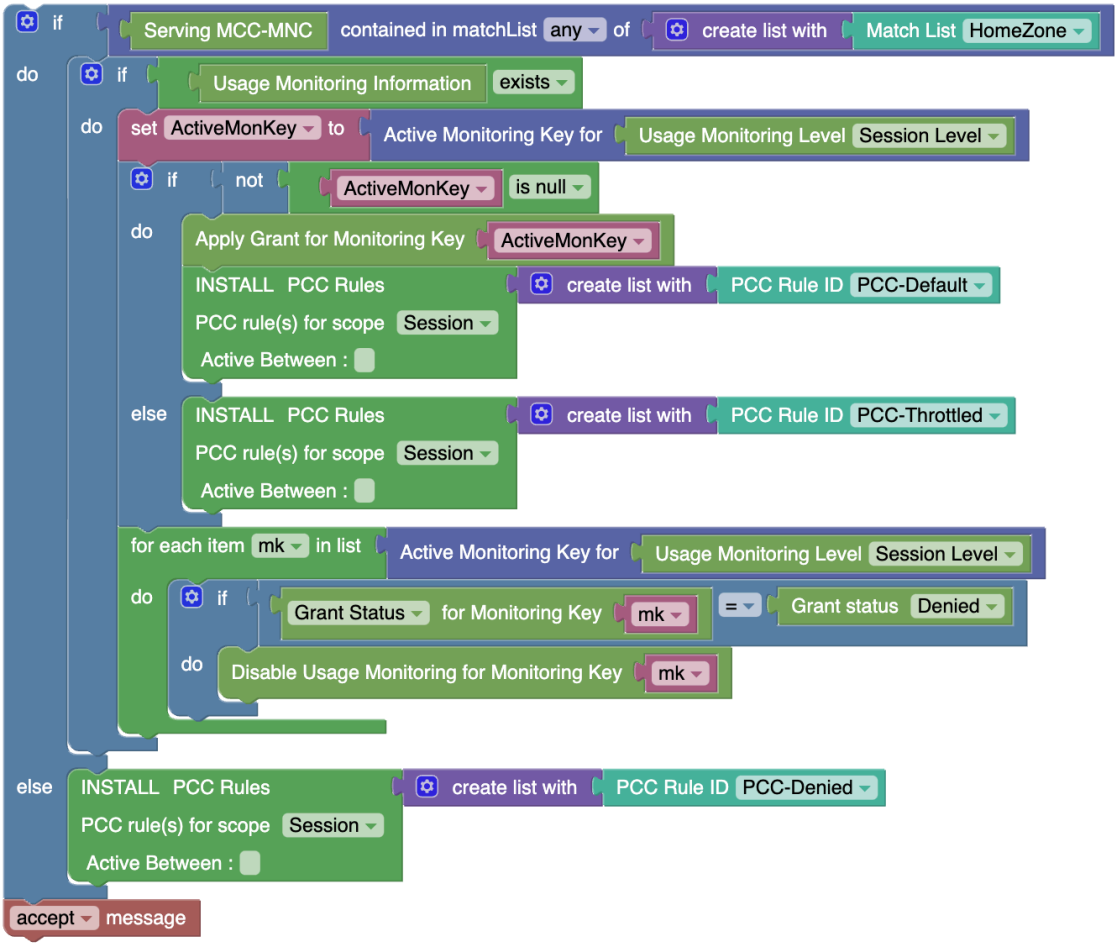


Figure 4-26 PCRF Core Policy Project



Home Monthly Plan with Roaming Pass

Scenario

- All data plans are configured CNC Console.
- Subscriber has purchased a monthly plan. Name of the plan is provided in a vendor specific custom attribute "homePlanName" under SmData.
- As long as subscriber is in the home region and has data left, the subscriber can use this plan.
- QoS Throttling is applied when the data in the home plan is exhausted.
- The Billing Day for home plan is provided in a vendor specific custom attribute "billingDay" under SmData.
- Subscriber has also purchased a roaming plan (Roaming Pass). Name of the plan is provided in a vendor specific custom attribute "roamingPlanName" under SmData. The start and end dates are also provided in vendor specific custom attributes "roamingPlanStartDate", "roamingPlanEndDate" under SmData. This is a one-time plan and will expire when entirely consumed.
- As long as subscriber is in the roaming region, the plan is within its validity time and has data left, the subscriber can use this plan.
- When Roaming Quota is exhausted, the subscriber is redirected to a charging portal.
- Subscriber is entitled to different Home and Roaming QoS and Charging.

ConfigurationData Limit Profile
In CNC Policy, Navigate to Policy Data Configurations → Usage Monitoring → Data Limit Profiles and create a Data Limit Profile for Home Plan.

The following fields are mandatory to be set:

- Name
- Usage Limit
- Reset Period

For Roaming Plan, follow the same steps, however set the following field values:

- Plan Type: Pass
- Reset Period: Empty

Attribute Forwarding Profile
In CNC Policy, Navigate to Service Configurations → Common Data → Attribute Forwarding Profile and create a Attribute Forwarding Profile with the field values as displayed in the below screenshot.

Figure 4-27 Forwarded Attributes for Home Monthly Plan with Roaming Passes

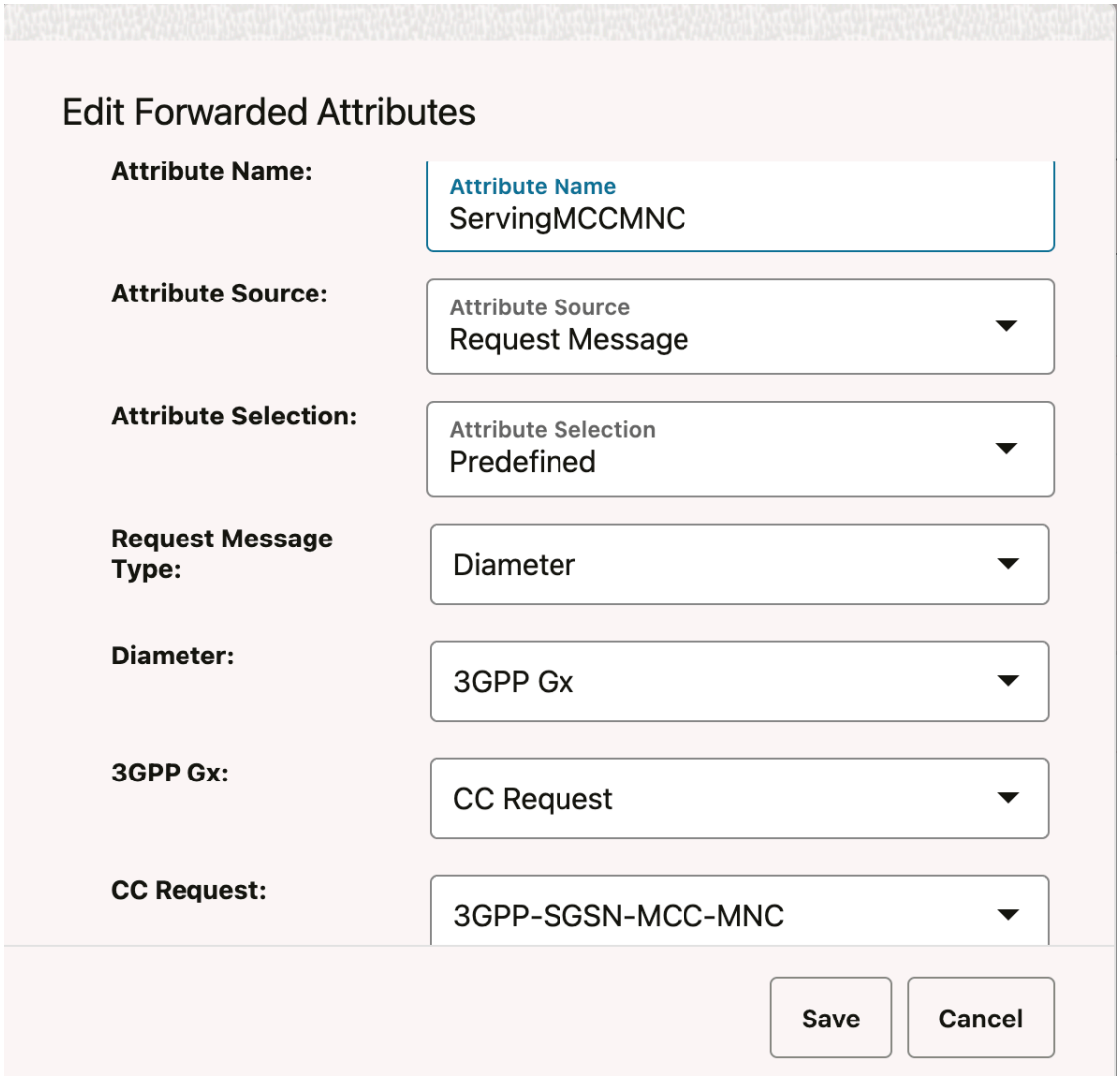


Figure 4-28 Forwarded Attributes for Home Monthly Plan with Roaming Passes

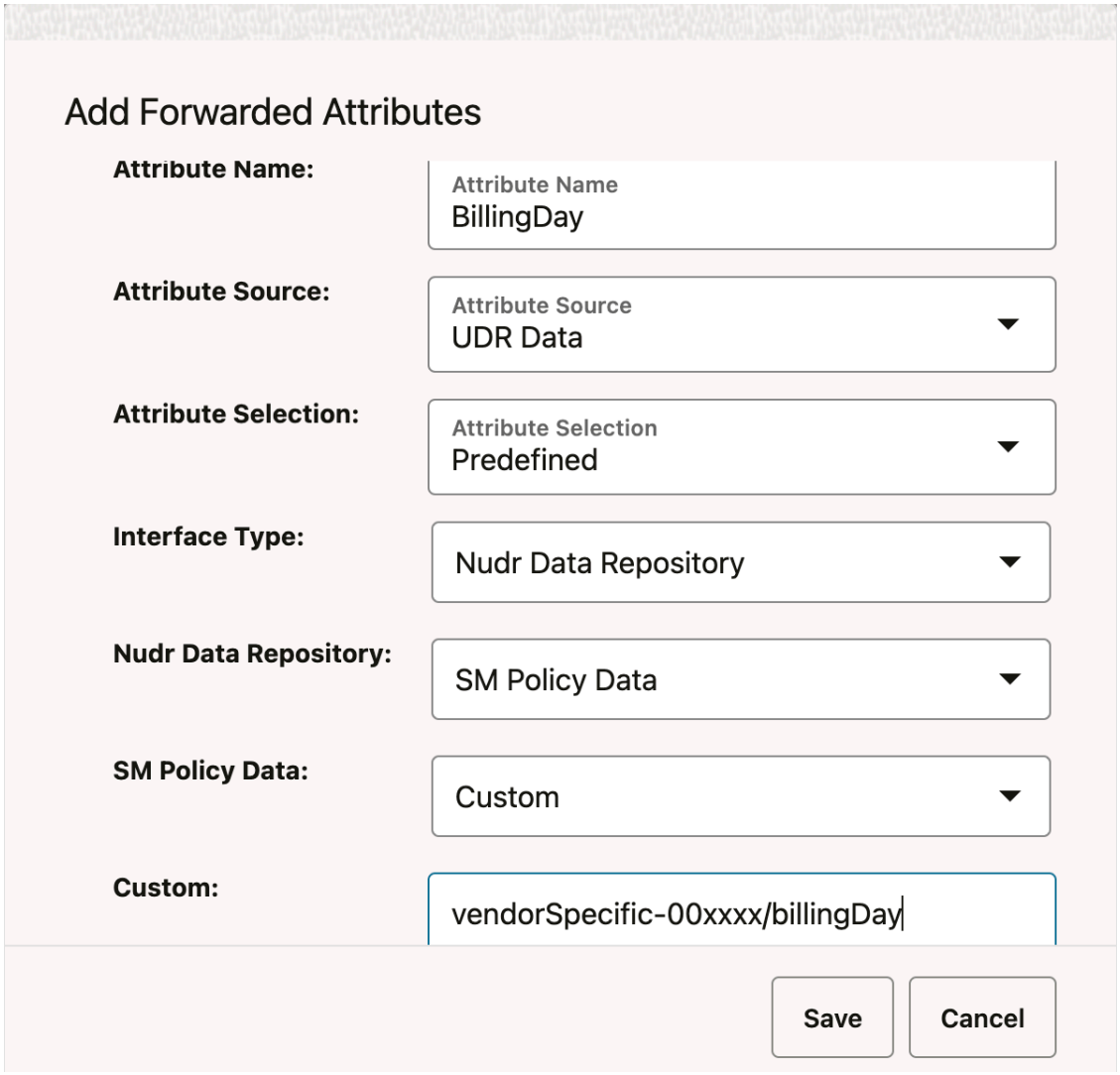


Figure 4-29 Forwarded Attributes for Home Monthly Plan with Roaming Passes

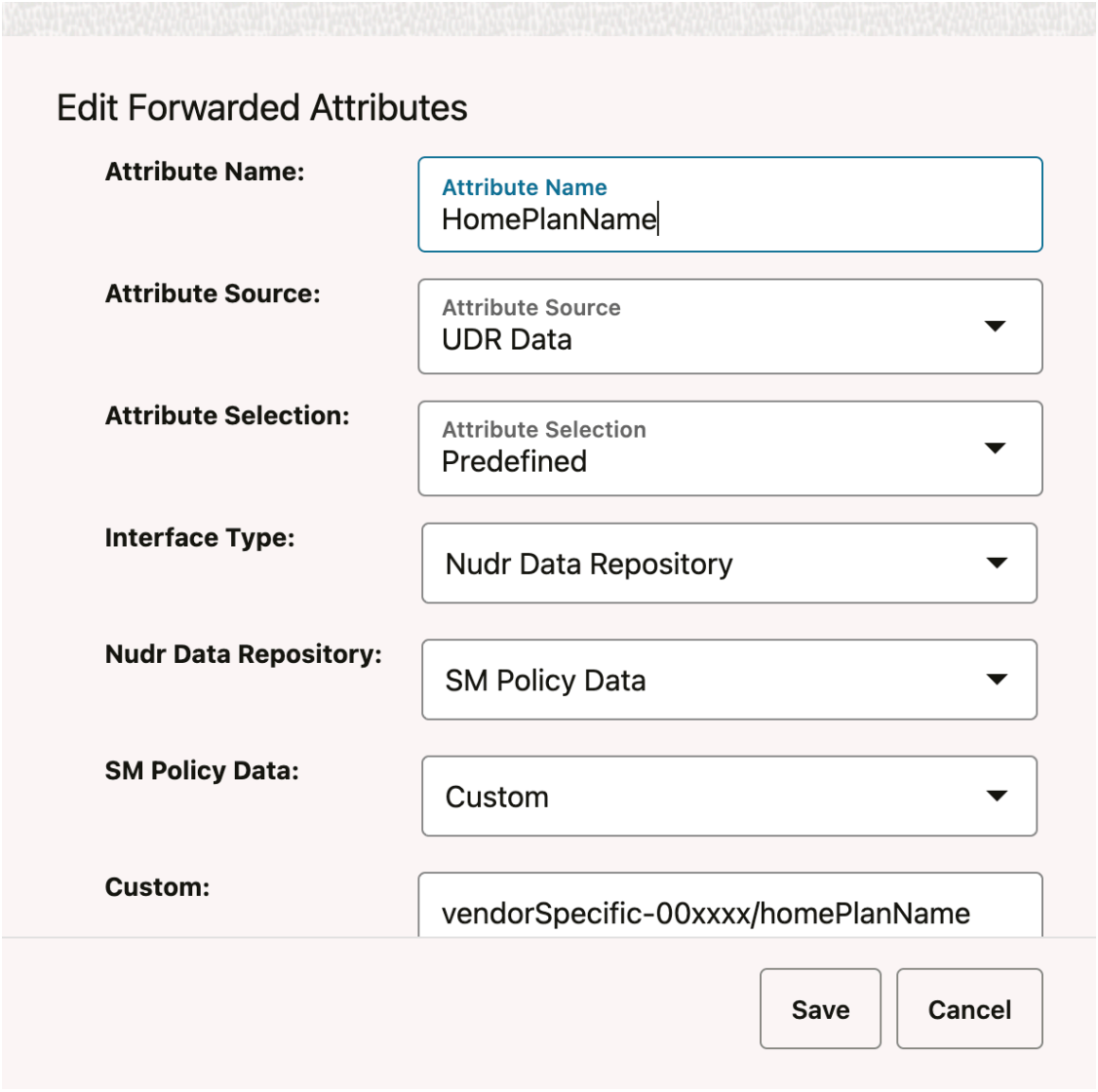


Figure 4-30 Forwarded Attributes for Home Monthly Plan with Roaming Passes

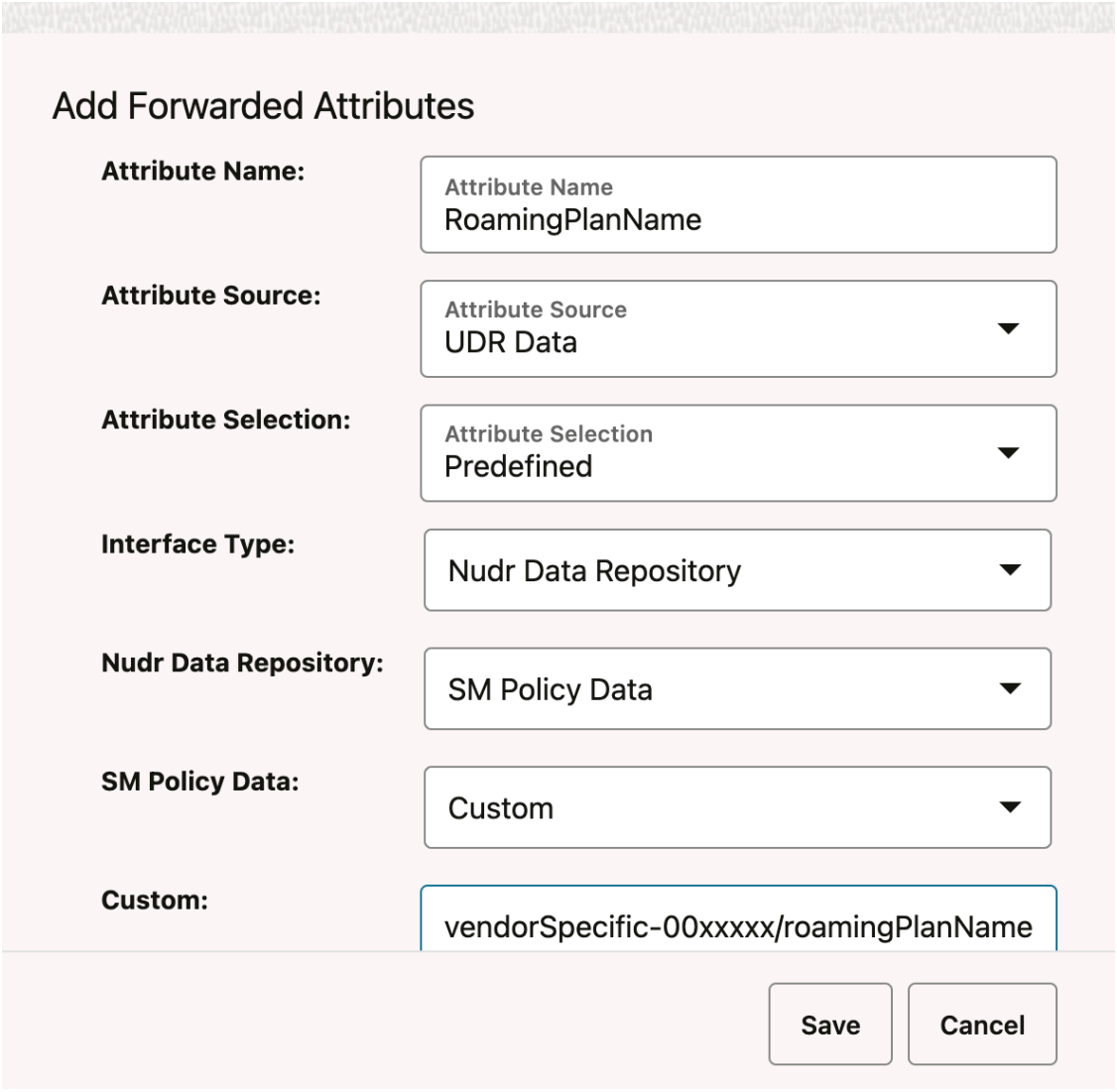


Figure 4-31 Forwarded Attributes for Home Monthly Plan with Roaming Passes

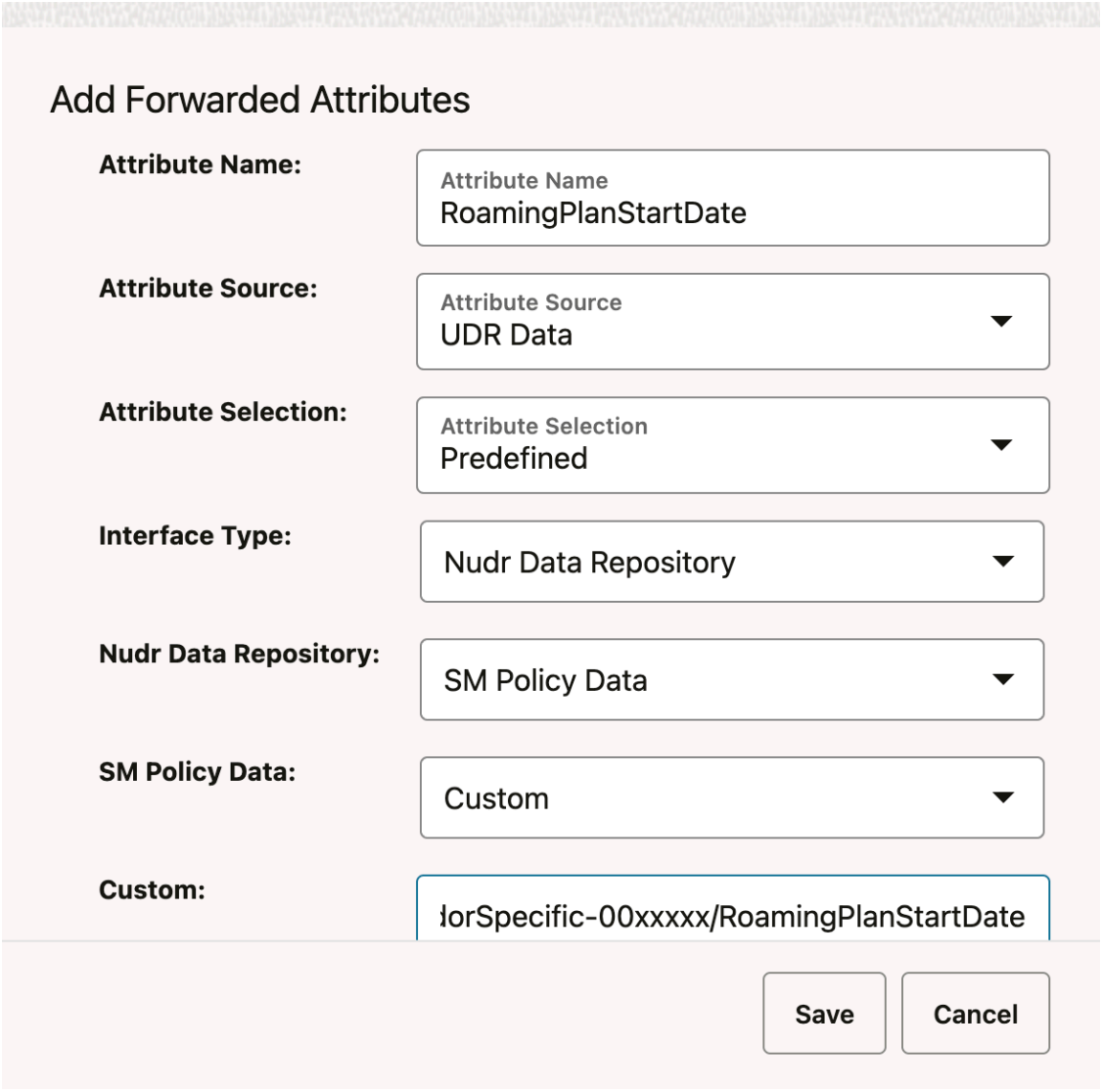
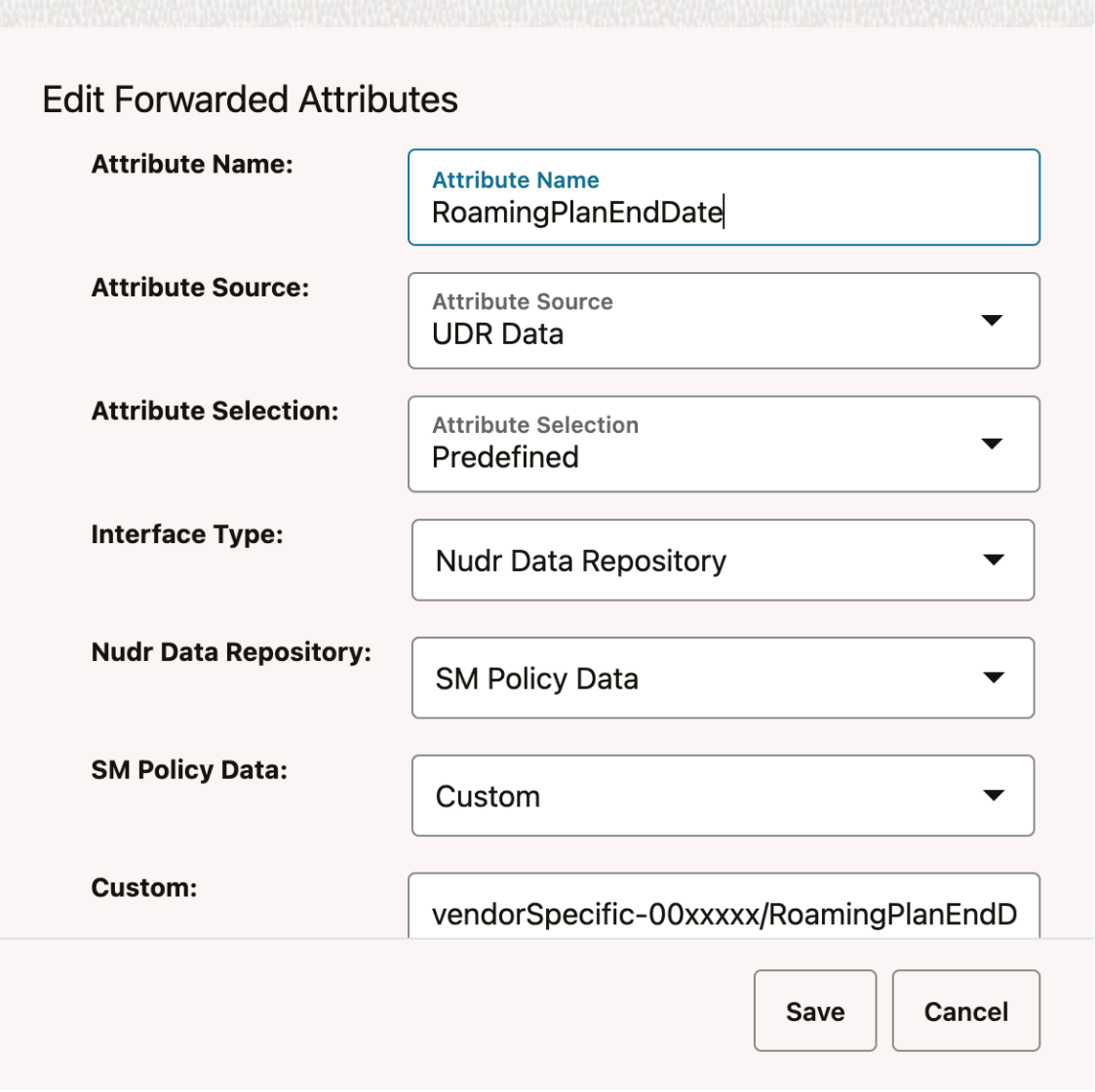


Figure 4-32 Forwarded Attributes for Home Monthly Plan with Roaming Passes



PCRF Core Configuration
In CNC Policy, Navigate to Service Configurations → PCRF Core → Settings and set the following field(s) under Usage Monitoring Group:

- Enabled: true
- APN List: the list of APNs for which Usage Monitoring is required.
- Attribute Forwarding: the forwarding profile created for each desired interface/message type.

Usage Monitoring Service Configuration
In CNC Policy, Navigate to Service Configurations → Usage Monitoring and set the following field(s):

- Enable PRE: true

Configure other fields as necessary.

Match List

In CNC Policy, Navigate to Policy Data Configurations → Common → Match List and create a Match List to fill in the home MCC/MNCs.

Policy Table
Not required for this scenario

Usage Monitoring Policy

Figure 4-33 Policy Project for Home Monthly Plan with Roaming Passes

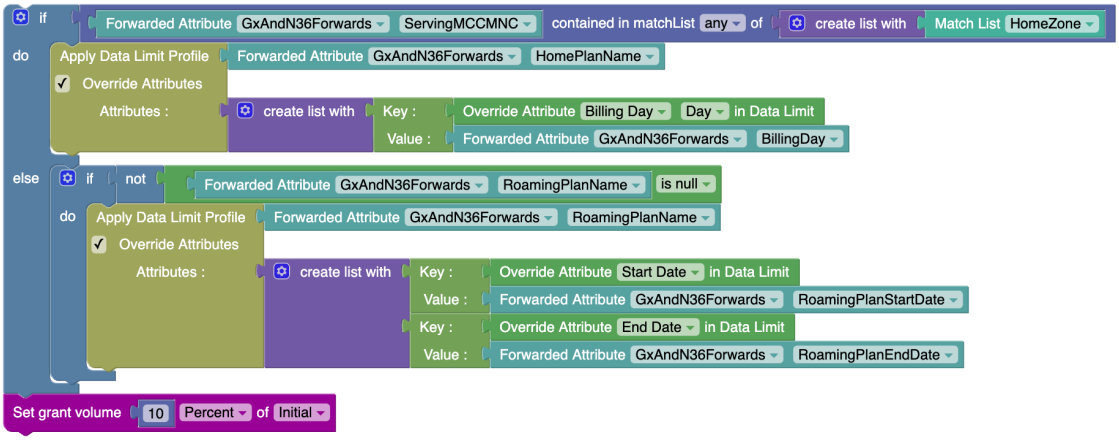
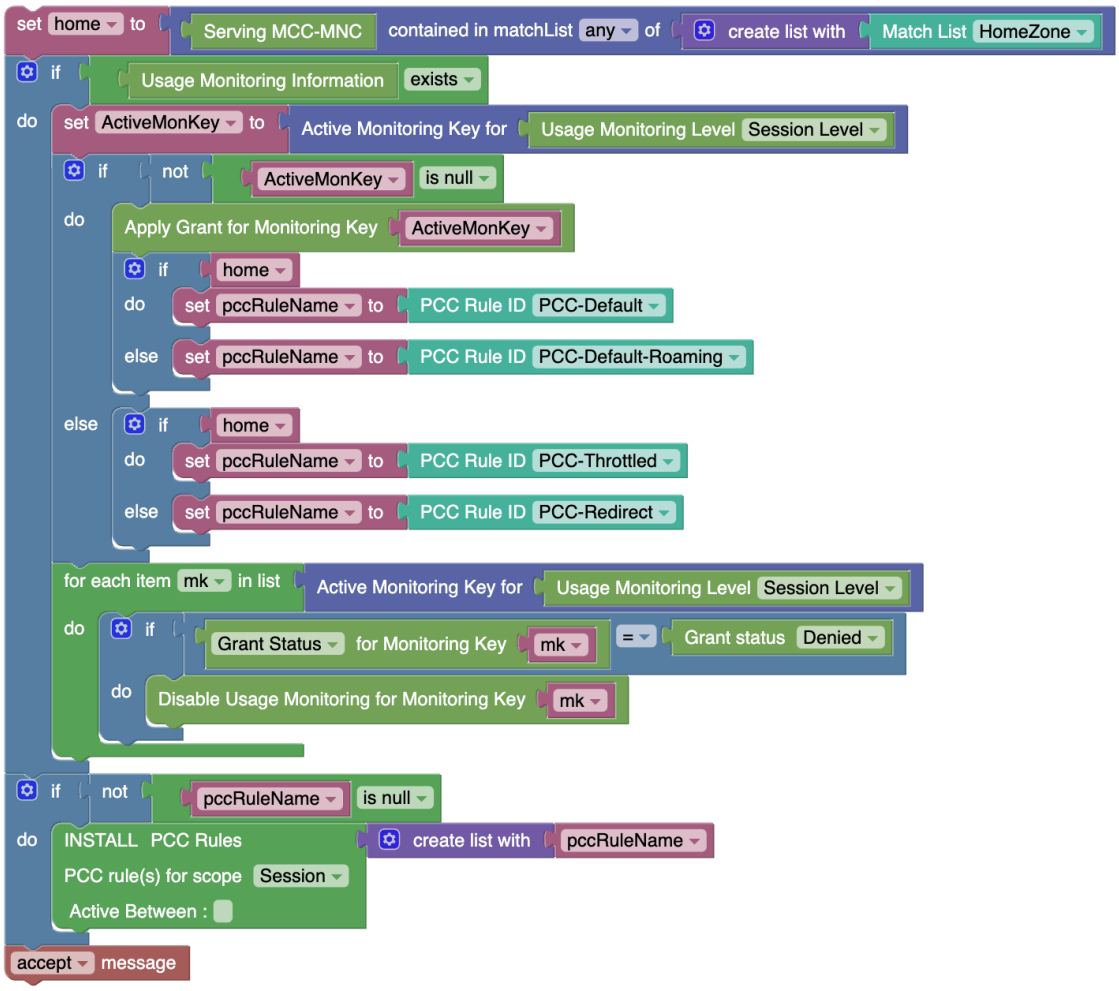


Figure 4-34 PCRF Core Project for Home Monthly Plan with Roaming Passes



Home Monthly Plan with Top-up

Scenario

- All data plans are configured In CNC Policy
- Subscriber has purchased a monthly plan. Name of the plan is provided in a vendor specific custom attribute "homePlanName" under SmData.
- As long as subscriber is in the home region and has data left, the subscriber can use this plan.
- The Billing Day is provided in a vendor specific custom attribute "billingDay" under SmData.
- Subscriber has also purchased a Top-up. Name of the Top-up is provided in a vendor specific custom attribute "topUpName" under SmData. The start and end dates for this top-up are also provided in vendor specific custom attributes "topUpPlanStartDate", "topUpPlanEndDate" under SmData. This is a one-time plan and will expire when entirely consumed.
- The base plan will be consumed before the top-up as long as there is quota left in the base plan.
- QoS and Charging for base and top-up plans are same.

- When both base and top-up quota are exhausted, QoS throttling is applied.
- Data is denied if the subscriber is in a roaming region.

ConfigurationData Limit Profile
In CNC Policy, Navigate to Policy Data Configurations → Usage Monitoring → Data Limit Profiles and create a Data Limit Profile for Home Plan.

The following fields are mandatory to be set:

- Name
- Usage Limit
- Reset Period

For Top-up, follow the same steps, however set the following field values:

- Plan Type: Top-up
- Reset Period: Empty

Attribute Forwarding Profile
In CNC Policy, Navigate to Service Configurations → Common Data → Attribute Forwarding Profile and create a Attribute Forwarding Profile with the field values as displayed in the below screenshot.

Figure 4-35 Forwarded Attributes for Home Monthly Plan with Top-up

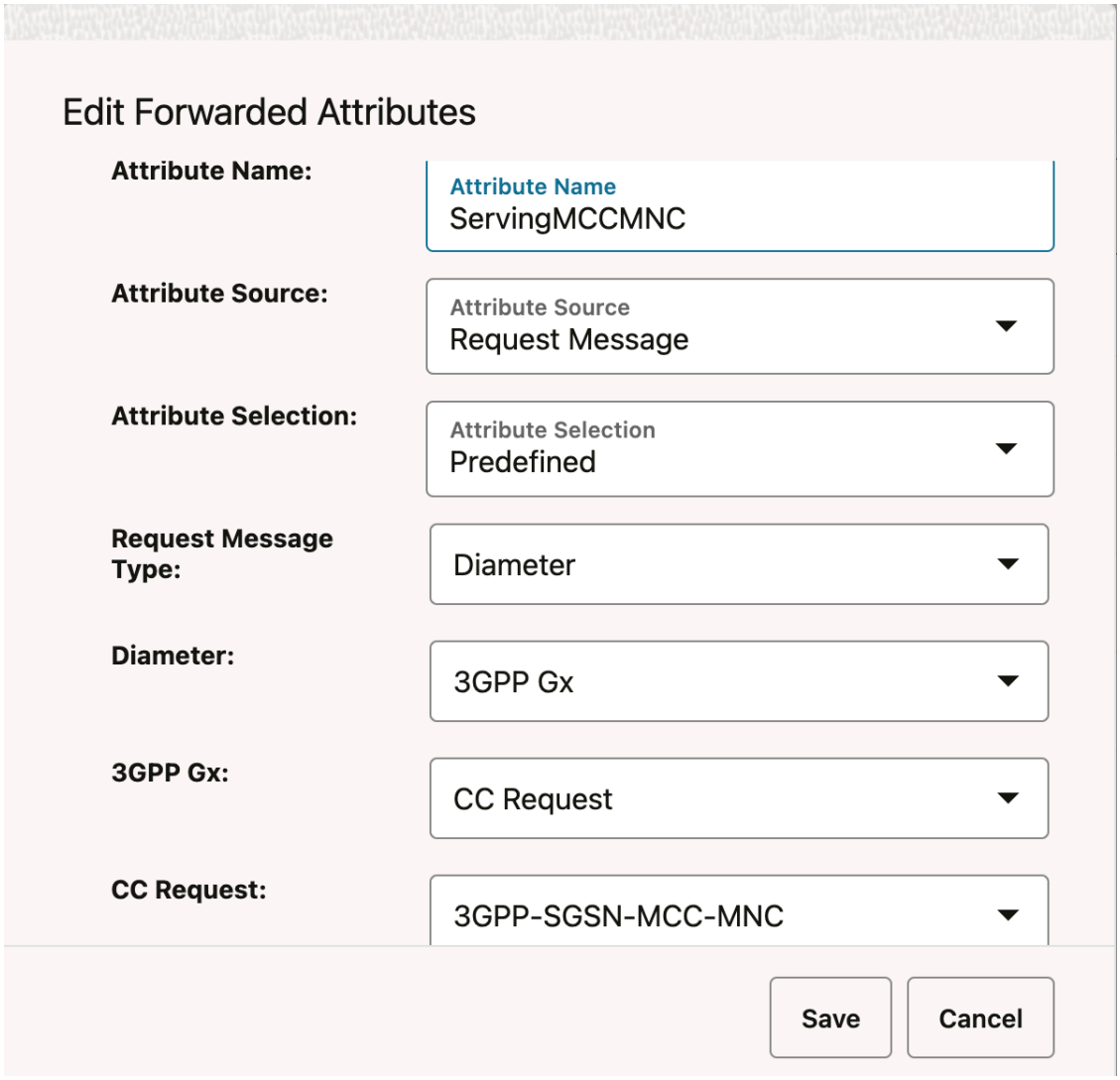


Figure 4-36 Forwarded Attributes for Home Monthly Plan with Top-up

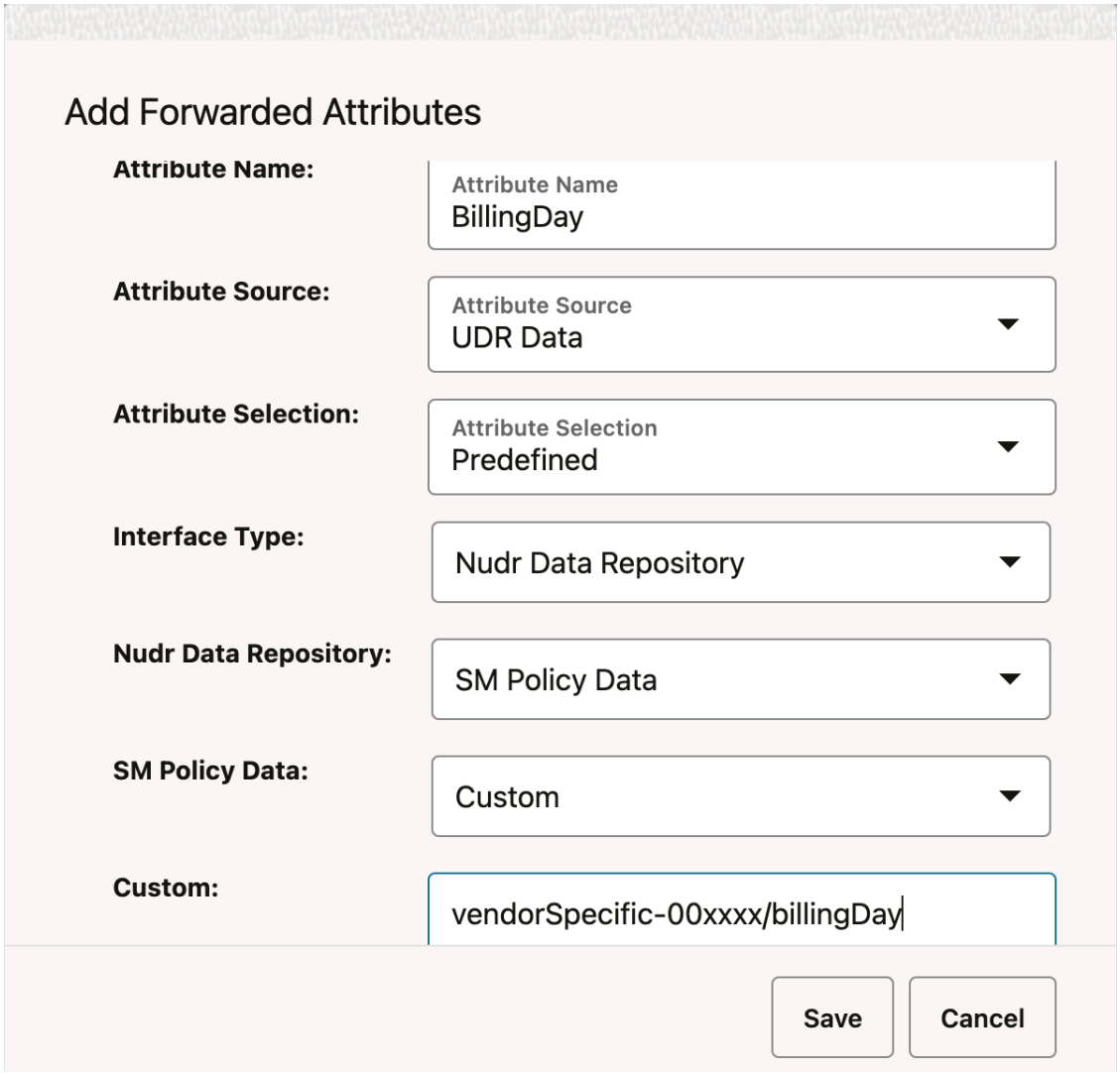


Figure 4-37 Forwarded Attributes for Home Monthly Plan with Top-up

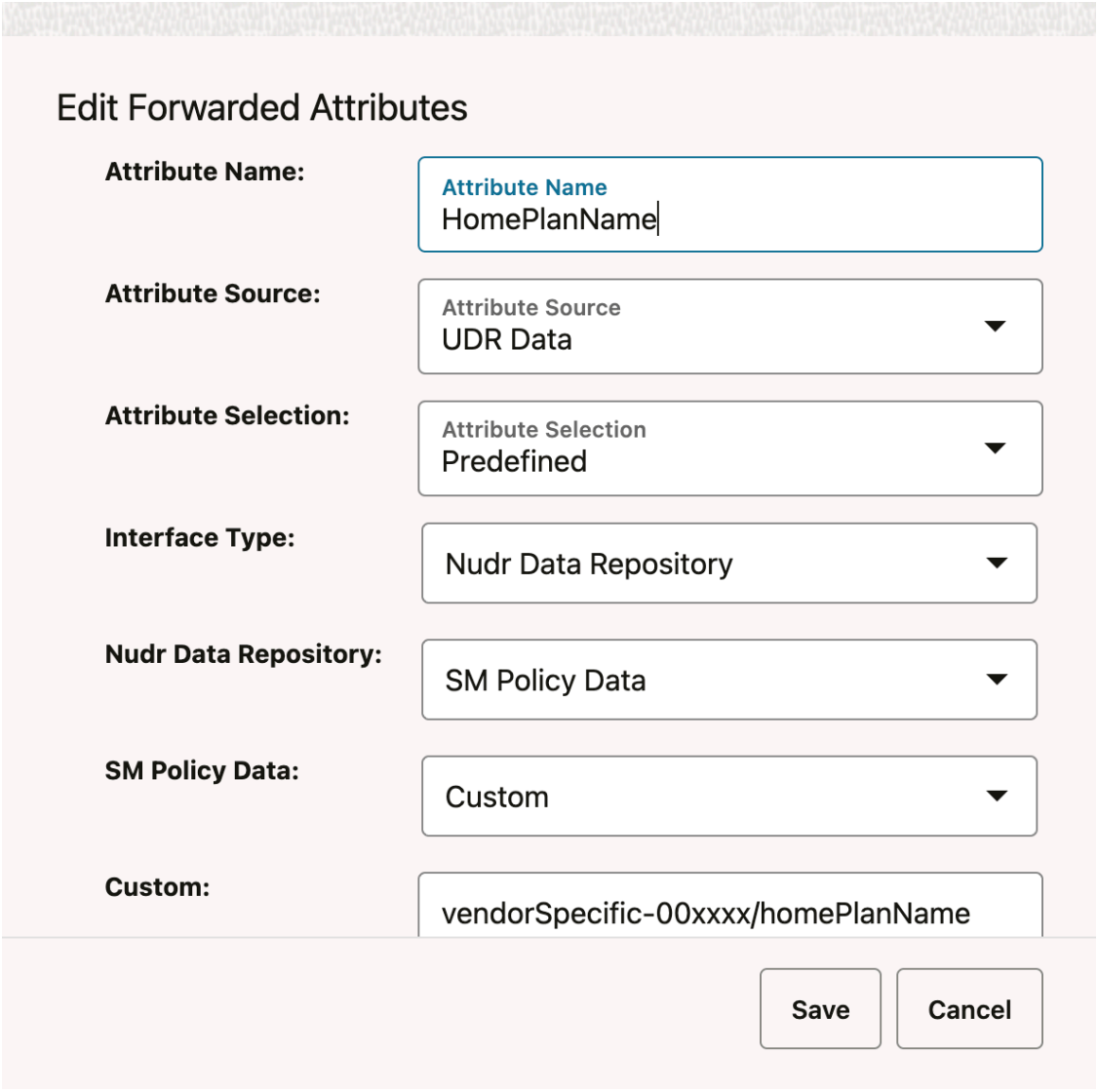


Figure 4-38 Forwarded Attributes for Home Monthly Plan with Top-up

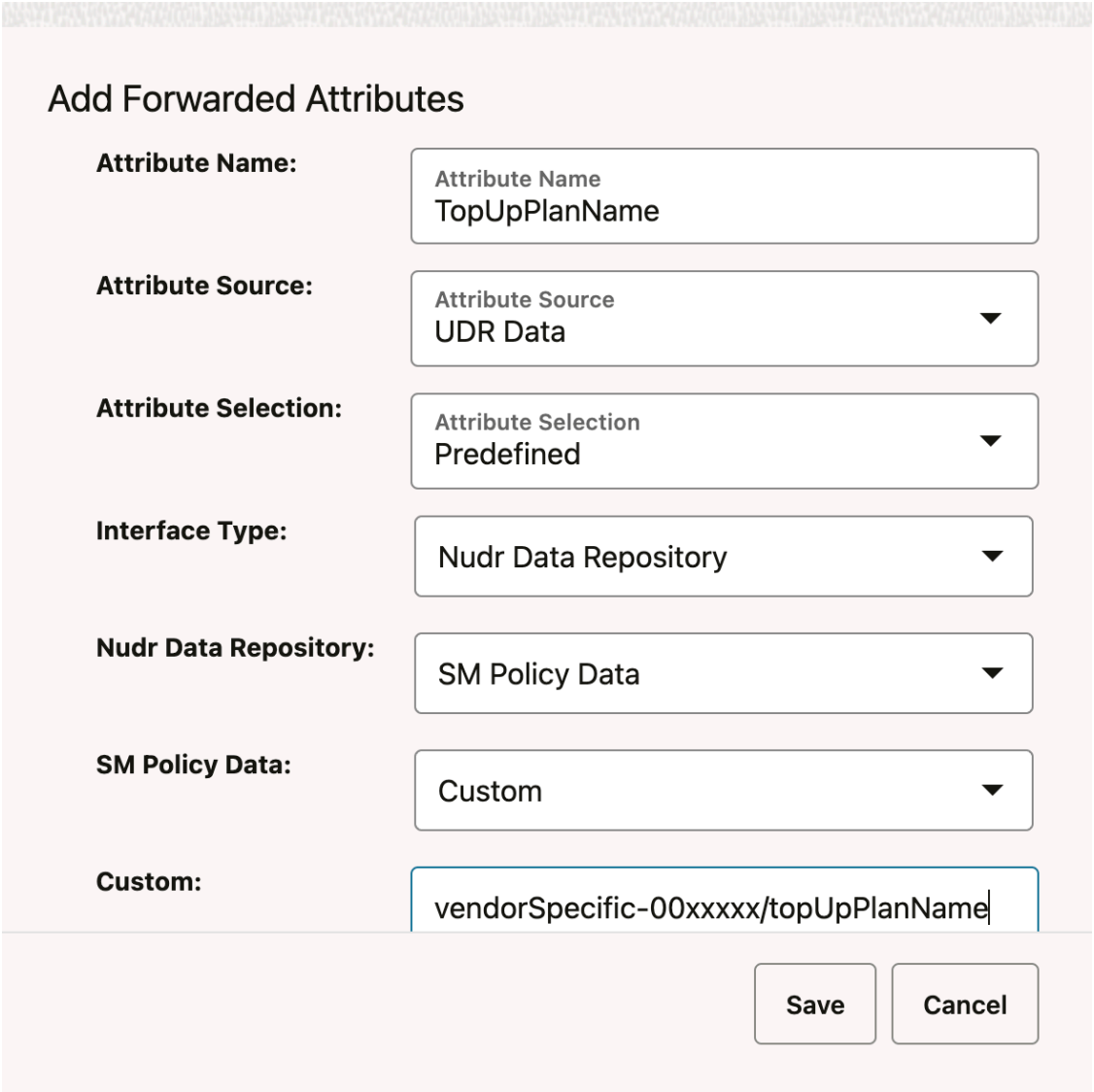
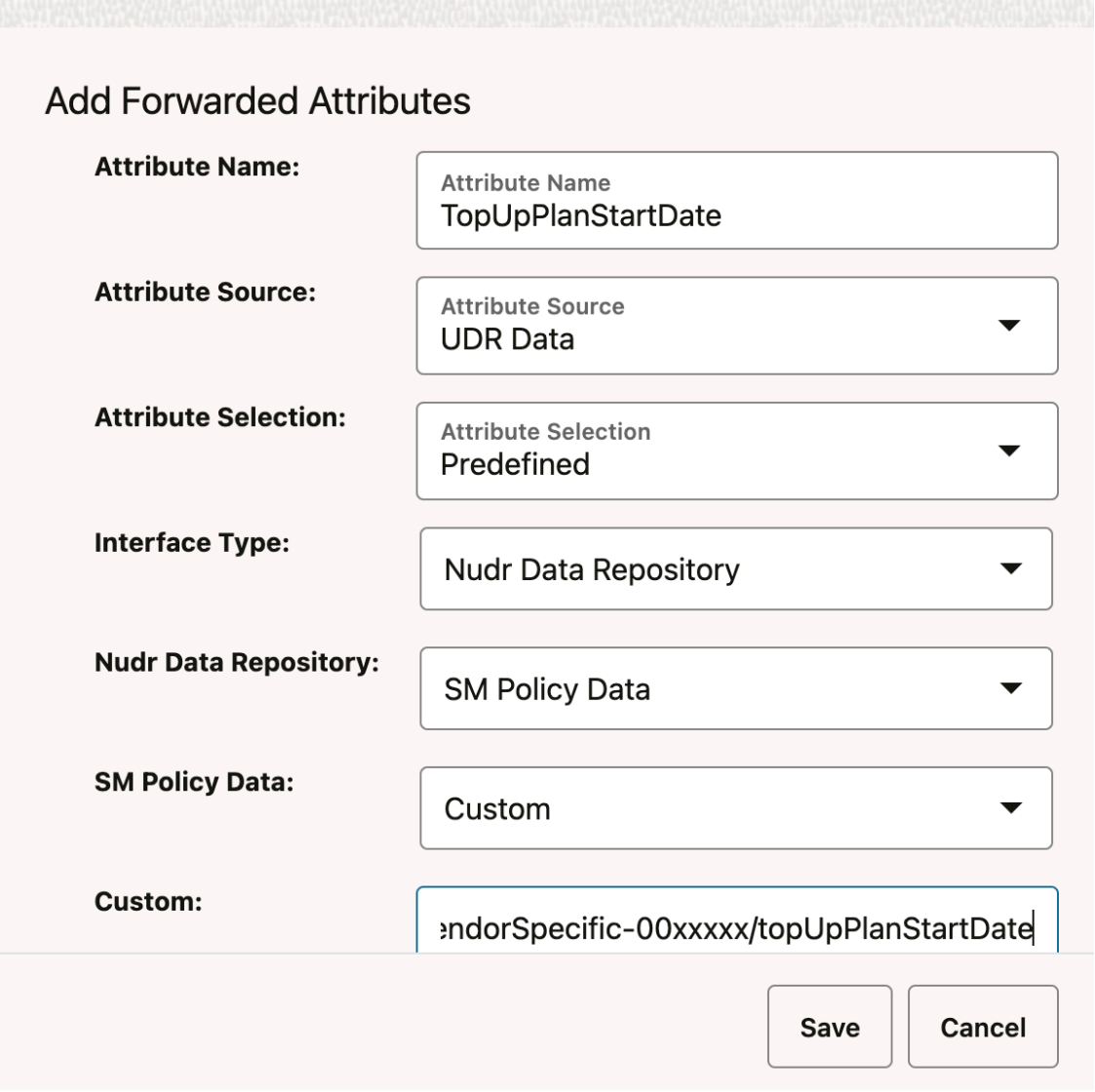


Figure 4-39 Forwarded Attributes for Home Monthly Plan with Top-up



PCRF Core Configuration
In CNC Policy, Navigate to Service Configurations → PCRF Core → Settings and set the following field(s) under Usage Monitoring Group:

- Enabled: true
- APN List: the list of APNs for which Usage Monitoring is required.
- Attribute Forwarding: the forwarding profile created for each desired interface/message type.

Usage Monitoring Service Configuration
In CNC Policy, Navigate to Service Configurations → Usage Monitoring and set the following field(s):

- Enable PRE: true

Configure other fields as necessary.

Match List

In CNC Policy, Navigate to Policy Data Configurations → Common → Match List and create a Match List to fill in the home MCC/MNCs.

Policy Table
Not required for this scenario.

Usage Monitoring Policy

Figure 4-40 Policy Project for Home Monthly Plan with Top-ups

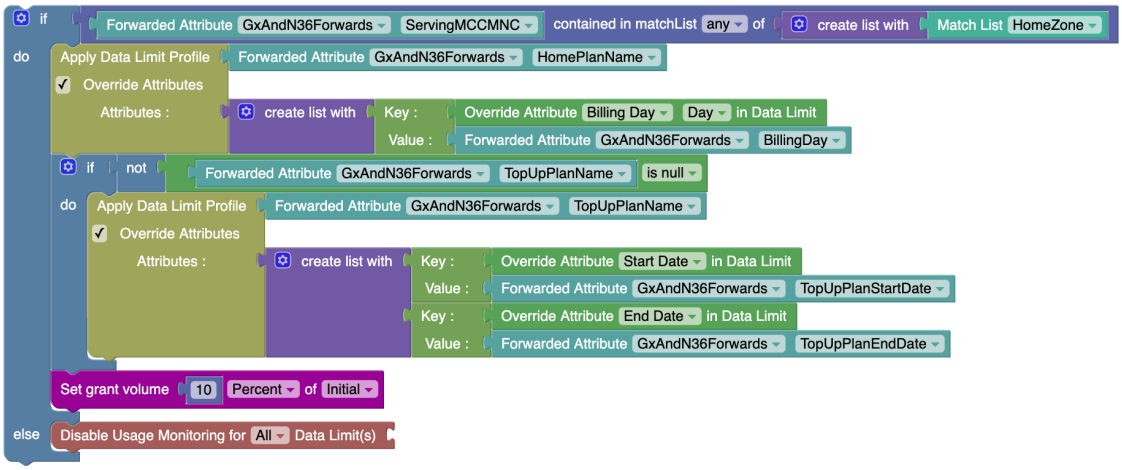
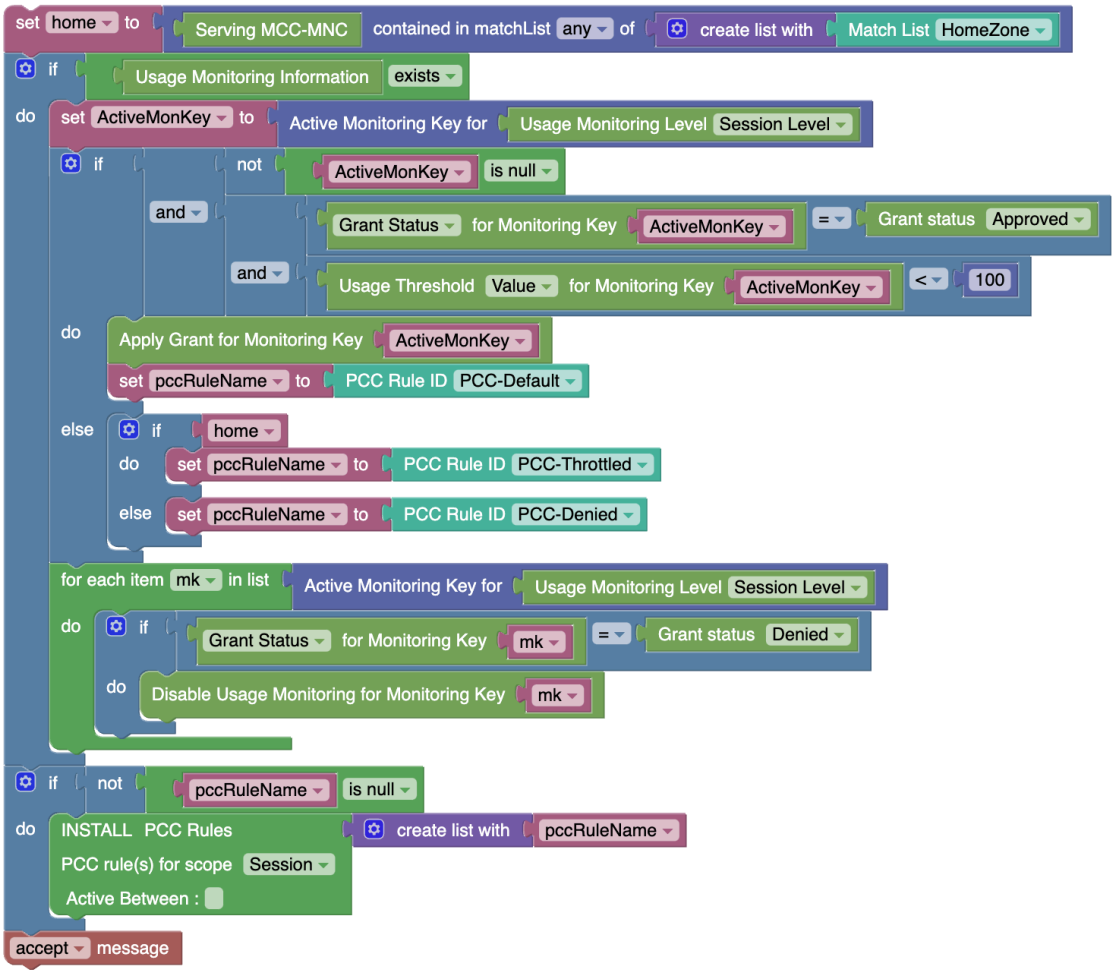


Figure 4-41 PCRF Core Project for Home Monthly Plan with Top-ups



Monthly Plan with Weekend Pass

Scenario

- Home Plan conditions as in the previous scenarios
- Subscriber has purchased a one-time (non-recurring) "Weekend" Pass.
  - The Pass is provided in the UDR UmDataLimits sections in SmData resource identified by custom attribute "passType"="weekend".
  - The Pass has a start date and an end date provided in respective UDR attributes.
  - The pass is applicable every week starting from "Friday 9:00PM" to "Monday 6:00AM".
- QoS and Charging for base and weekend pass plans are different.

ConfigurationData Limit Profile
In CNC Policy, Navigate to Policy Data Configurations → Usage Monitoring → Data Limit Profiles and create a Data Limit Profile for Home Plan.

The following fields are mandatory to be set:

- Name
- Usage Limit

- Reset Period

For the "Weekend" Pass, provision the same in the UDR using the provisioning interface for the targeted subscriber(s).

- Plan Type: Pass
- Custom Attribute: "passType=weekend"
- Reset Period: Empty

Attribute Forwarding Profile
In CNC Policy, Navigate to Service Configurations → Common Data → Attribute Forwarding Profile and create a Attribute Forwarding Profile with the field values as displayed in the below screenshot.

Figure 4-42 Forwarded Attributes for Monthly Plan with Weekend Passes

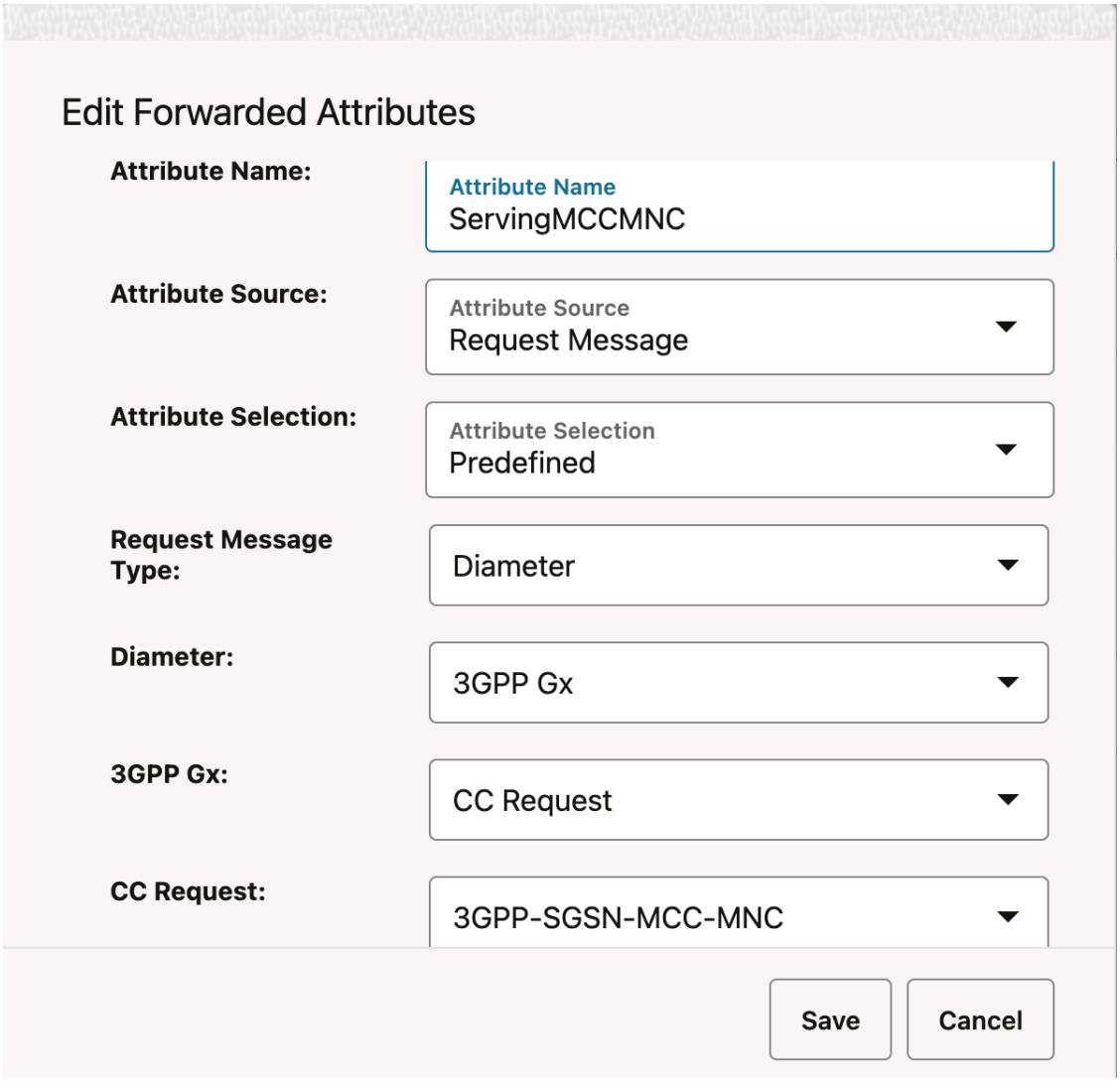


Figure 4-43 Forwarded Attributes for Monthly Plan with Weekend Passes

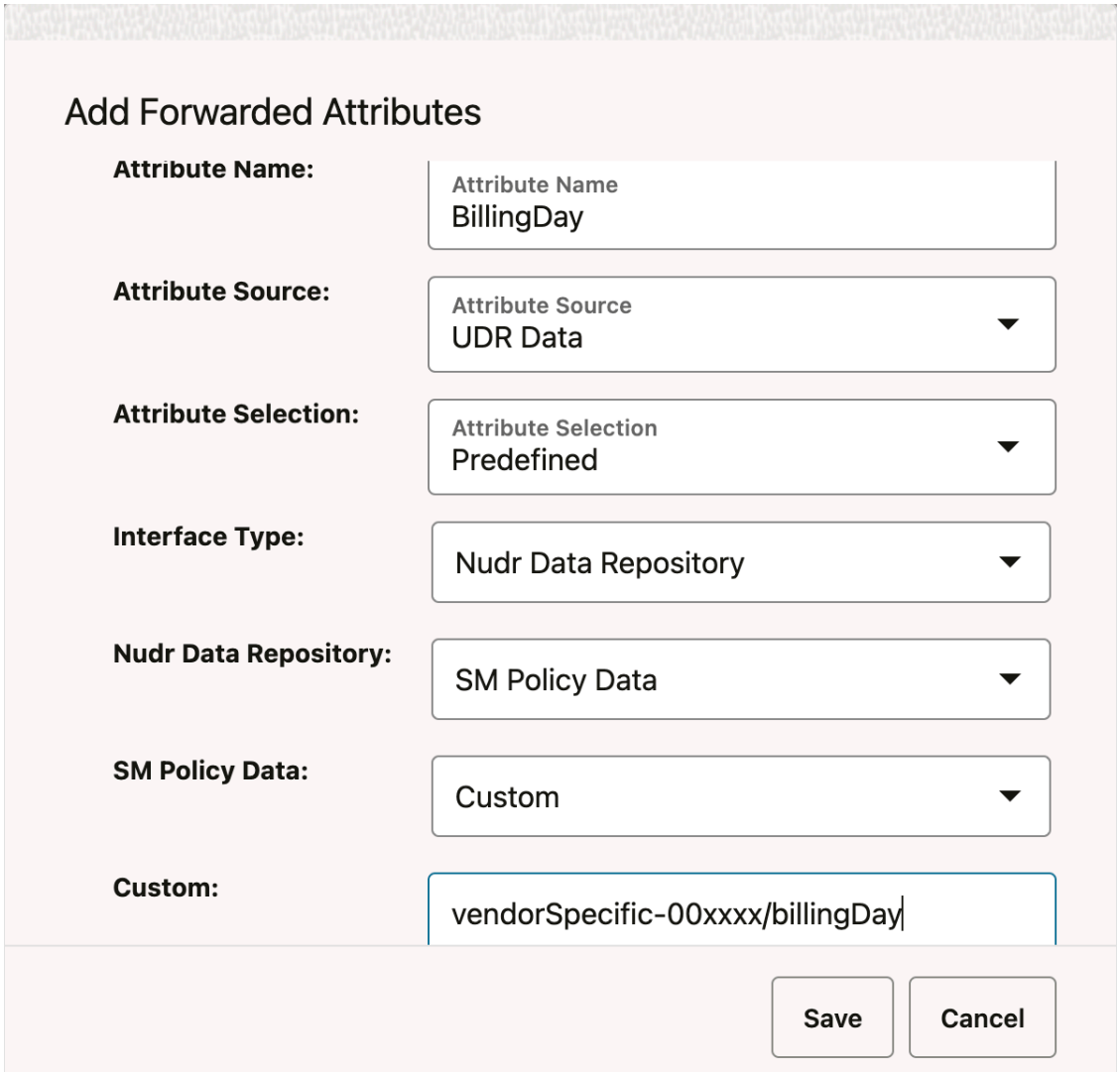
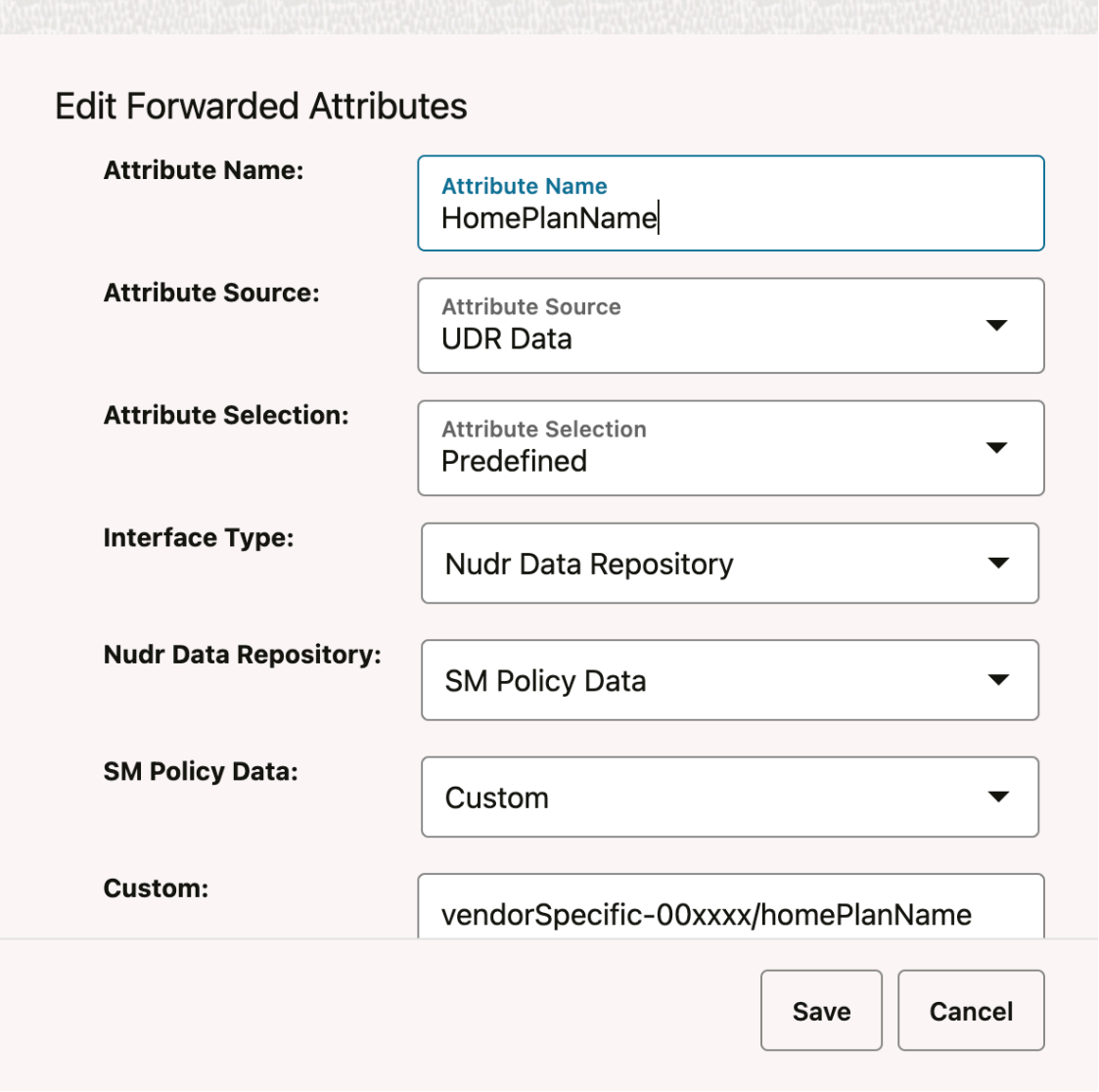


Figure 4-44 Forwarded Attributes for Monthly Plan with Weekend Passes



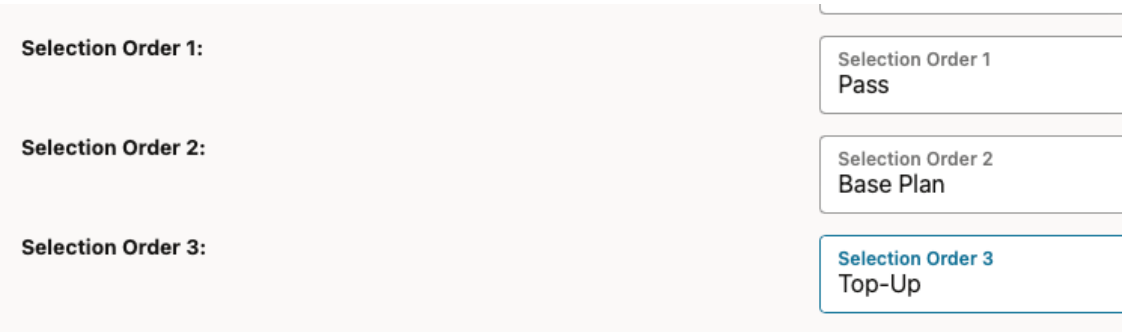
PCRF Core Configuration
In CNC Policy, Navigate to Service Configurations → PCRF Core → Settings and set the following field(s) under Usage Monitoring Group:

- Enabled: true
- APN List: the list of APNs for which Usage Monitoring is required.
- Attribute Forwarding: the forwarding profile created for each desired interface/message type.

Usage Monitoring Service Configuration
In CNC Policy, Navigate to Service Configurations → Usage Monitoring and set the following field(s):

- Enable PRE: true
- data plans Selection Order:

Figure 4-45 PCRF Core Configuration for Monthly Plan with Weekend Pass



Match List

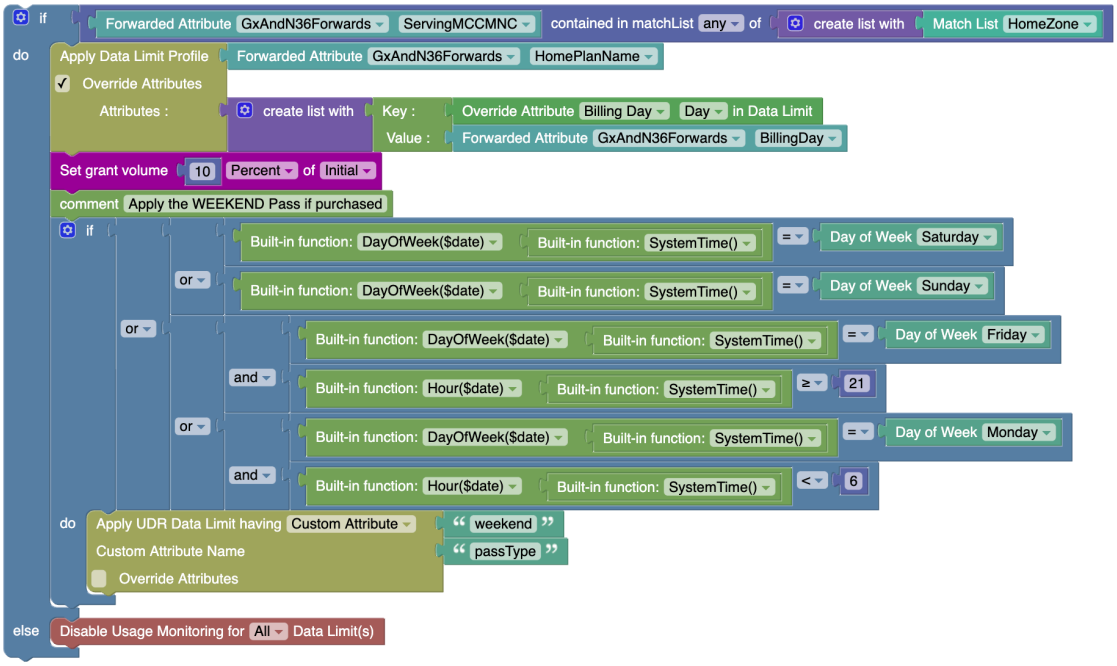
In CNC Policy, Navigate to Policy Data Configurations → Common → Match List and create a Match List to fill in the home MCC/MNCs.

Policy Table

Not required for this scenario.

Usage Monitoring Policy

Figure 4-46 Policy Project for Home Mobthly Plan with Weekend Passes



Monthly Plan with Multiple Top-ups

Scenario

- Subscriber has purchased a monthly plan. Name of the plan is provided in a vendor specific custom attribute "homePlanName" under SmData.
- As long as subscriber is in the home region and has data left, the subscriber can use this plan.

- The Billing Day is provided in a vendor specific custom attribute "billingDay" under SmData.
- Subscriber has purchased two Top-up Plans - the names of which are provided in the custom attributes "topup1Name" and "topup2Name" under SmData.
- The start and end dates for these top-up plans are also provided in vendor specific custom attributes "topUpPlan1StartDate", "topUpPlan1EndDate", "topUpPlan2StartDate", "topUpPlan2EndDate" under SmData. These are one-time plans and will expire when entirely consumed.
- The base plan will be consumed before the top-up as long as there is quota left in the base plan.
- "TOPUP1" will be consumed before "TOPUP2".
- QoS and Charging for base and top-up plans are same.
- When both base and top-up quota are exhausted, QoS throttling is applied
- Subscriber has purchased two Top-up Plans - "TOP1" and "TOP2"

ConfigurationData Limit Profile
In CNC Policy, Navigate to Policy Data Configurations → Usage Monitoring → Data Limit Profiles and create a Data Limit Profile for Home Plan.

The following fields are mandatory to be set:

- Name
- Usage Limit
- Reset Period

For Top-up, follow the same steps, however set the following field values:

- Plan Type: Top-up
- Reset Period: Empty

Attribute Forwarding Profile
In CNC Policy, Navigate to Service Configurations → Common Data → Attribute Forwarding Profile and create a Attribute Forwarding Profile as described in previous scenarios.

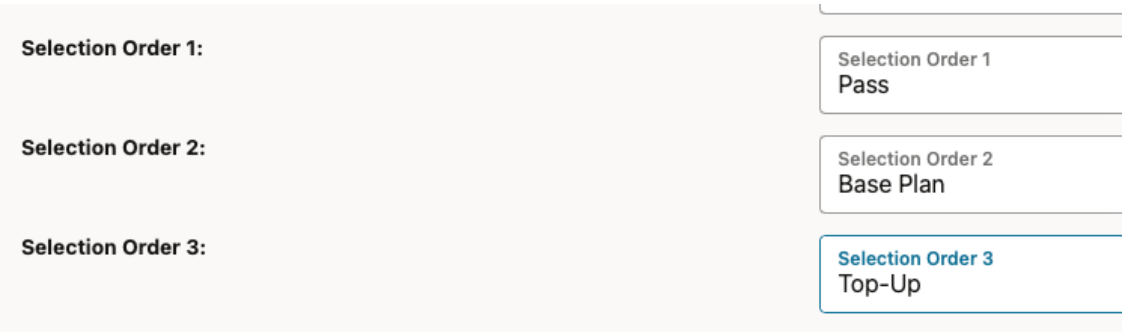
PCRF Core Configuration
In CNC Policy, Navigate to Service Configurations → PCRF Core → Settings and set the following field(s) under Usage Monitoring Group:

- Enabled: true
- APN List: the list of APNs for which Usage Monitoring is required.
- Attribute Forwarding: the forwarding profile created for each desired interface/message type.

Usage Monitoring Service Configuration
In CNC Policy, Navigate to Service Configurations → Usage Monitoring and set the following field(s):

- Enable PRE: true
- data plans Selection Order:

Figure 4-47 Configuration for Monthly Plan with Multiple Top-ups



Match List

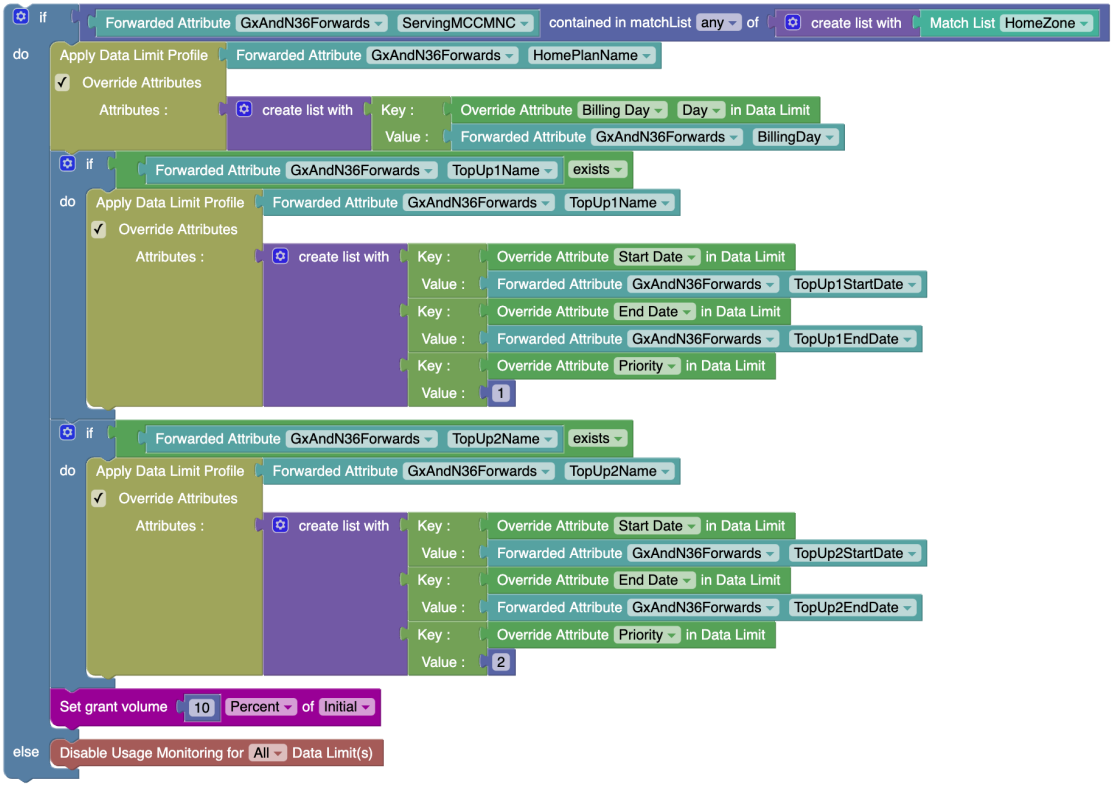
In CNC Policy, Navigate to Policy Data Configurations → Common → Match List and create a Match List to fill in the home MCC/MNCs.

Policy Table

Not required for this scenario.

Usage Monitoring Policy

Figure 4-48 Policy Project for Monthly Plan with Multiple Top-ups



Autoenrolled Roaming Subscriber with Multiple Roaming Passes

Scenario

- All data plans are configured In CNC Policy
- All roaming subscribers are given roaming plans based on the roaming zone, which is defined based on MCC-MNC.
  - If there is a match found for the Country Code and Network Code => Zone=RZ_WithAgreement
  - If there is a match found for the Country Code but not for Network Code => Zone=RZ_WithoutAgreement
  - If there is no match found for Country Code => Zone=0
- Each Subscriber is given two daily recurring Roaming Plans.
- When Roaming Plan 1 is exhausted, Roaming Plan 2 is applied.
- When Roaming Plan 2 is exhausted, subscribers belonging to Zone 0 are redirected to a Portal, rest are Throttled.

ConfigurationData Limit Profile
In CNC Policy, Navigate to Policy Data Configurations → Usage Monitoring → Data Limit Profiles and create Data Limit Profiles for Roaming Plan.

- Periodicity: Daily

Attribute Forwarding Profile
In CNC Policy, Navigate to Service Configurations → Common Data → Attribute Forwarding Profile and create a Attribute Forwarding Profile as described in previous scenarios.

PCRF Core Configuration
In CNC Policy, Navigate to Service Configurations → PCRF Core → Settings and set the following field(s) under Usage Monitoring Group:

- Enabled: true
- APN List: the list of APNs for which Usage Monitoring is required.
- Attribute Forwarding: the forwarding profile created for each desired interface/message type.

Usage Monitoring Service Configuration
In CNC Policy, Navigate to Service Configurations → Usage Monitoring and set the following field(s):

- Enable PRE: true

Configure other fields as necessary.

Match List
In CNC Policy, Navigate to Policy Data Configurations → Common → Match List and create a Match List to fill in the home MCC/MNCs.

Policy Table

Figure 4-49 Roaming Zones for Autoenrolled Roaming Subscriber with Multiple Roaming Passes

RoamingZones

Back | Create Column | Create Row | Delete Row | Refresh

MCC Number	RZ_WithAgreement Number	MCCMNC Match List	RZ_WithoutAgreement Number
300	1	300_List	51
400	2	400_List	52

Figure 4-50 Roaming Plans for Autoenrolled Roaming Subscriber with Multiple Roaming Passes

RoamingPlans

Back | Create Column | Create Row | Delete Row | Refresh

RoamingZone Number	QuotaPlan1 Data Limit Profile	QuotaPlan2 Data Limit Profile
1	RoamingPlan_1	RoamingPlan_3
0	RoamingPlan_0	RoamingPlan_0
51	RoamingPlan_2	RoamingPlan_4

Usage Monitoring Policy

Figure 4-51 Policy Porject for Autoenrolled Roaming Subscriber with Multiple Roaming Passes

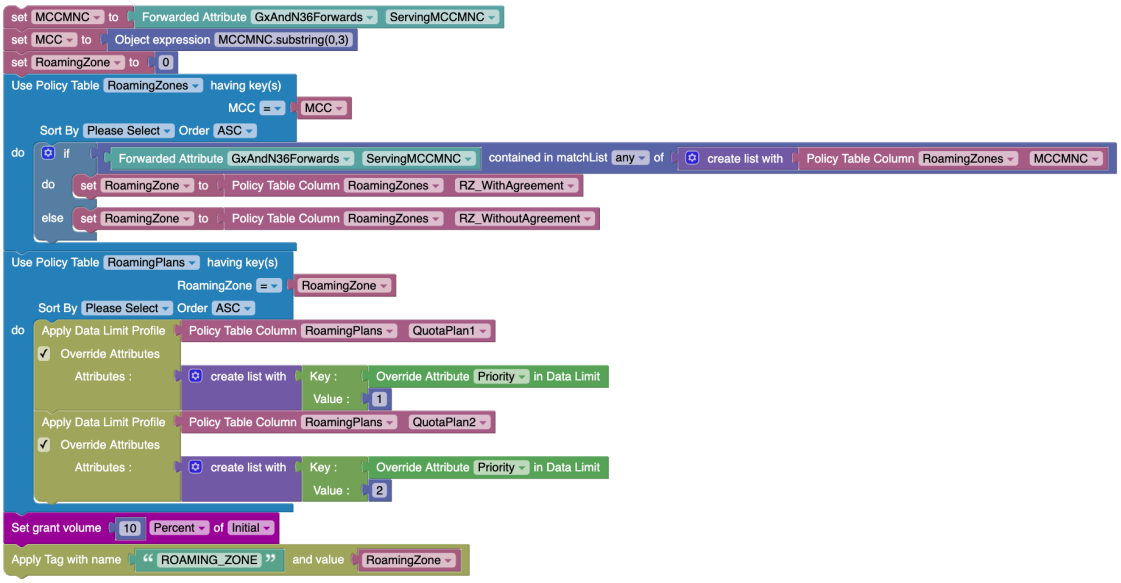
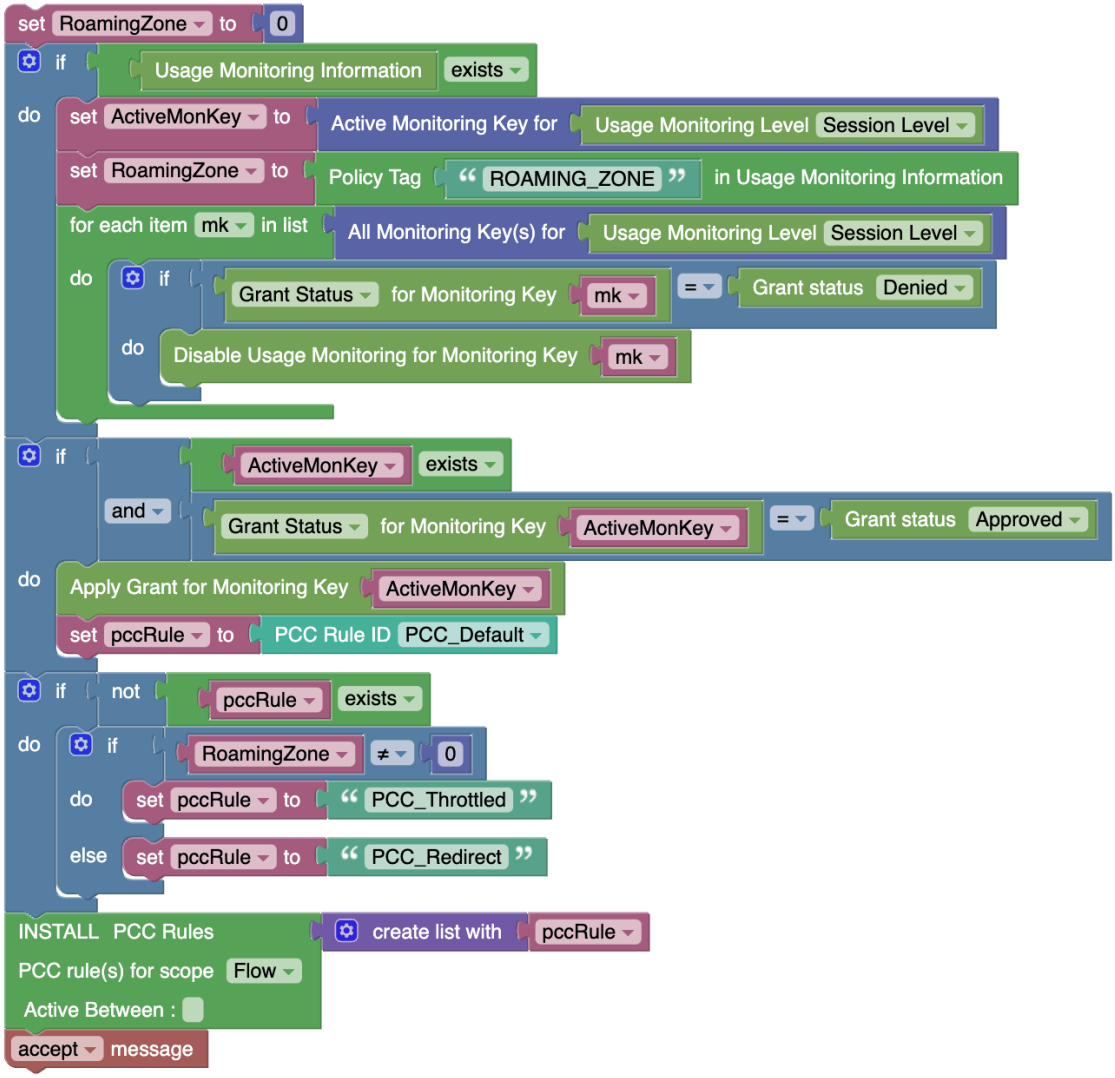


Figure 4-52 PCRF Core Porject for Autoenrolled Roaming Subscriber with Multiple Roaming Passes



4.7 Match List

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 List is used during a list creation to either select or omit the items from a list. The items in the list must be homogeneous.

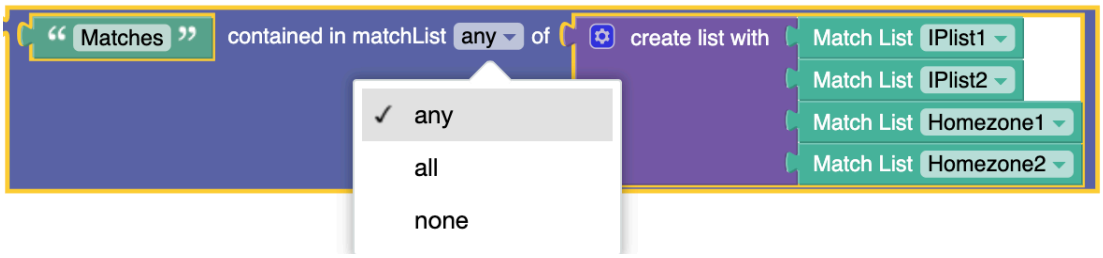
You can create the list of items using **Match List** page under **Common** section for **Policy Data Configuration** in CNC Console.

For more details, see *Match List* section in *Configuring CNC Console* in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

Policy Projects in CNC Console includes a **Contains in matchList** block, which indicates to select items specified in **Match List** block.

Match List specifies the list to be used for matching criteria.

Figure 4-53 Here is an example of match list functionality:



In the **Match List Block** Match List name is provided the right side and the value is provided on the left side. On the right side, multiple Match List can be given. But, it must contain only one value on the left side.

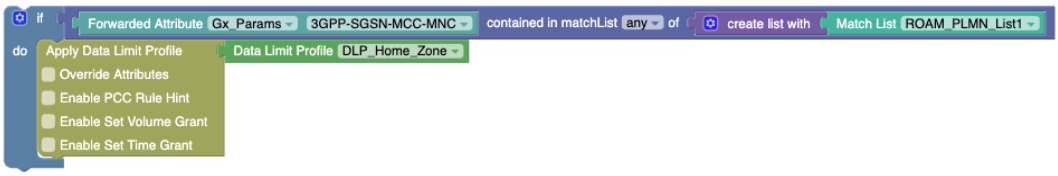
Possible values for **Contains in matchList** block are:

- `any` - If the attribute value from left side matches with any of the values of **Match List** in the right side, the output of **Contains in matchList** will be `true`. Otherwise, `false`.
- `all` - If the attribute value from left side is present in all the given values of **Match List** on the right side, the output of **Contains in matchList** will be `true`. Otherwise, `false`.
- `none` - If the attribute value from left side not present in any of the given values of **Match List** on the right side, the output of **Contains in matchList** will be `true`. Otherwise, `false`.

The values in the MatchList are matched based on data type:

- **String**: In this case, the match list name on the right side of the block is `String` type. The **Match List** screen on **Policy Data Configurations** can be verified to check that the data type for the match list string is `String`, that is the data type of the given value to match on the left side of the block. If **Match List** block contains the item which is `String` data tuype, same as the given value, then the output of the condition is `true`. Otherwise, the output is `false`.

Figure 4-54 Example for String Data Type in Match List



In this example, **Forwarded Attribute** block gets the value from the PRE body. If the PRE value for **Forwarded Attribute** block is `DNN1`, this value will be matched with `DNNString` match list to check whether the IP is the subnet or not.

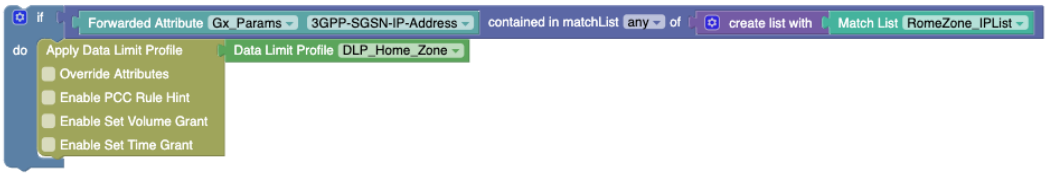
- **WildCard**: In this case, the match list name on the right side of the block is `WildcardString`. The **Match List** screen on **Policy Data Configurations** can be verified

to check the data type for the match list `ipv4` is IPv4 Subnet, the given value to match on the left side of the block. In the given example, the value is `string333444`. If the match list `WildcardString` contains item with wildcard characters (example - "string*", "str*" or "string3?3444"), then the output of this condition is `true`. Otherwise, the output is `false`.

Figure 4-55 Example for Widdcard Data Type in Match List

- **IPv4**: In this case, the match list name is `ipv4`. The **Match List** screen under **Policy Data Configurations** section can be verified to check the data type for the match list ipv4 is IPv4 Subnet, which is the data type of the value mentioned on the right side of the block. In this case the value is "`193.12.32.12`". If match list IPv4 contains the item that is IPv4 Subnet (example - "193.12.23.18/14", "193.12.32.25/24"), the output of this condition is `true`. Otherwise, the outpus is `false`.

Figure 4-56 Example for IPV4 Data Type in Match List



In this example, the **Forwarded Attribute** block receives the value from the PRE. For example, if the PRE value for **Forwarded Attribute** block is "`193.12.32.12`", with this value, it will try to match with `IPList` match list to check whether the IP is the subnet or not.

- **IPv6**: In this case, the match list name is **IPv6**. The **Match List** screen under **Policy Data Configurations** can be verified to check that the data type for the match list IPv6 is IPv6 Subnet, that is the data type of the value mentioned on the right side of the block. The given value to match is given on the left side of the block, in this case that is "`FE80:CD00:0:CDE:1257:0:211E:729C`". If the match list `IPv6` contains the item that is IPv6 Subnet (example - "FE80:CD00:0:CDE::/30", "FE80:CD00::/14", "FE80:CD00:0:CDE:1257::/48"), then the output of this condition is `true`. Otherwise, the output is `false`.

Figure 4-57 Example for IPV6 Data Type in Match List

In this example, the **Forwarded Attribute** block receives the value from the PRE. For example, if the PRE value for the **Forwarded Attribute** block is

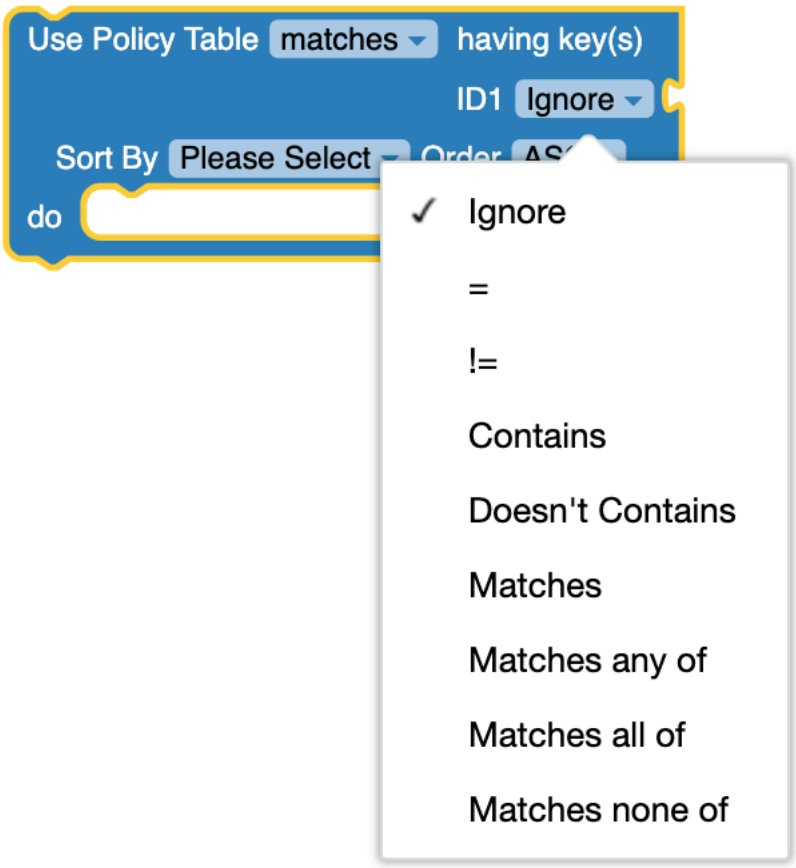
`"FE80:CD00::CDE:1257::211E::",`, with this value it will try to match with `"IPv6List"` match list to check whether the IP is the subnet or not.

- **Regular Expression**: In this case, the Match List name is `RegularExpression`. The **Match List** screen under **Policy Data Configurations** section can be verified to check that the data type for the match list is `RegularExpression`, that is the data type of the value on the right side of the block. The given value to match is given on the left side of the block. In this example, the value is `"hello@gmail.com"`. If the match list `RegularExpression` contains the item that is RegularExpression Subnet (example - "/^[\w-\.]+@([\w-]+\.)+[\w-]{2,4}$/g"), then the output of this condition is `true`. Otherwise, the output is `false`.

Using Match List with Policy Tables

When there are multiple Policies with similar structure, Policy tables can be used to consolidate and capture the differences in structure. The **Use Policy Table** block can be used to specify a parameter in a rule that uses a Policy table. The parameter name must be the column (field) name in the Policy table.

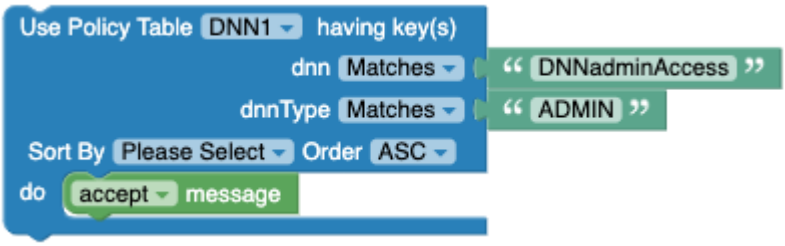
Figure 4-58 Exmple for Use Policy Table



The possible values of **Use Policy Table** block are:

- `Matches`: For `Matches` to be used in Policy Table, the data type must be `String`.

Figure 4-59 Example: Use Policy Table with Matches option

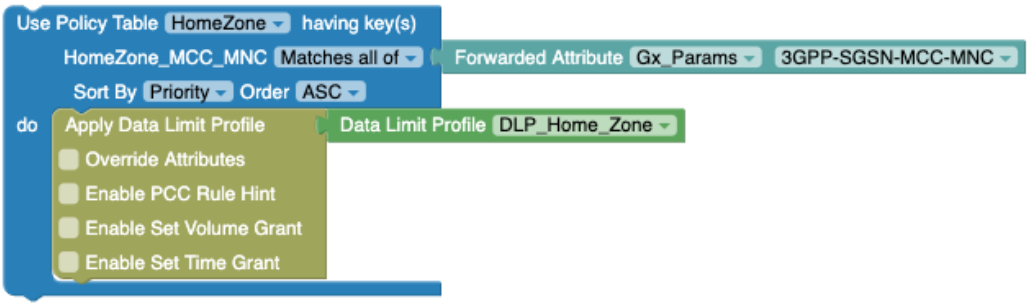


In the above example, in table DNN1, the value of column dnn is matched with "DNNAdminAccess: and the value of column dnnType is matched with "ADMIN".

- `Matches all of`: The data type of the Policy table should be `MatchList` or `MatchLists` (array of matchlist)

  If the data type is `MatchLists`, the array of `MatchList` can be present per row (in policy table) and in this case all the `MatchList` should be matched in a single row (policy table) to return `true` and pass that row.

Figure 4-60 Example: Use Policy Table with Matches All Of option

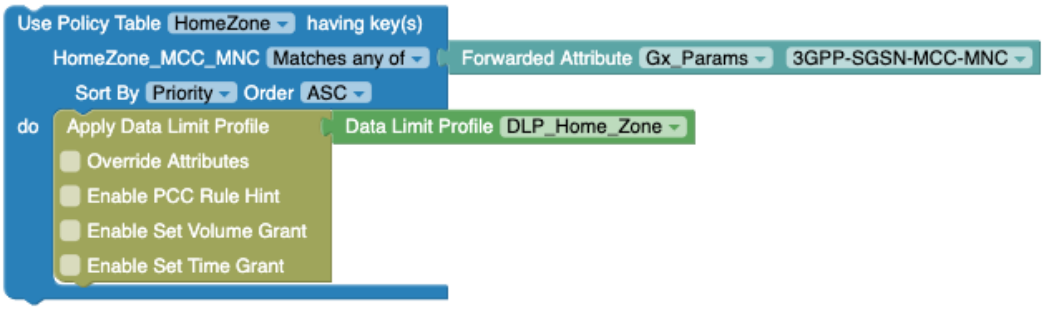


In the above example, the value of **Forwarded Attribute** block (such as "333444") is matched with both "DNN2" and "DNN" or "IPList" and "HomeZone" to return the respective row.

- `Matches any of`: The data type of the Policy table should be `MatchList` or `MatchLists` (array of `MatchList`)

  If the data type is `MatchLists`, the array of `MatchList` can be present per row (in policy table) and in this case any `MatchList` should be matched in a single row (Policy table) to return true and pass that row.

Figure 4-61 Example: Use Policy Table with Matches Any Of option



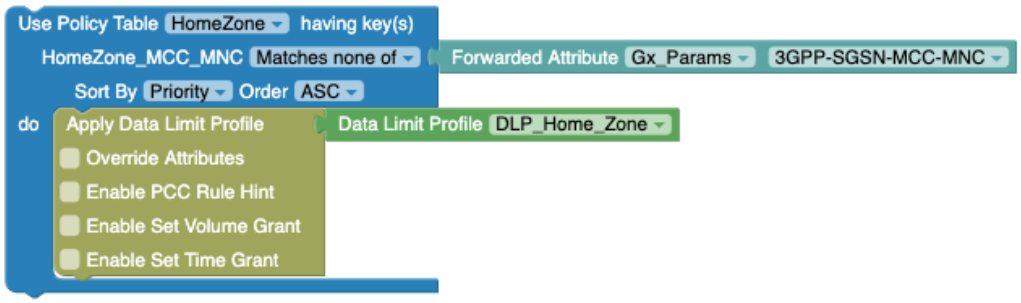
In the above example, **Forwarded Attribute** the value is (such as "333444") is matched with any of "DNN2" and "DNN" or "IPList" and "HomeZone" to return the respective row.

> **Note**
>
> The data type of the policy table column `MatchList` is same for both the operators `Matches all of` and `Matches any of`, as there will be only one `MatchList` present per row.

- `Matches none of`: The data type of the Policy table should be `MatchList` or `MatchLists` (array of `MatchList`).

  If the data type is `MatchLists`, the array of `MatchList` can be present per row (in policy table) and in this case all `MatchList` should not be matched in a single row (policy table) to return `true` and pass that row.

Figure 4-62 Example: Use Policy Table with Matches None Of option



In the above example, the value of **Forwarded Attribute** block (such as "333444") must not match with both "DNN2" and "DNN" or "IPList" and "HomeZone" to return the respective row

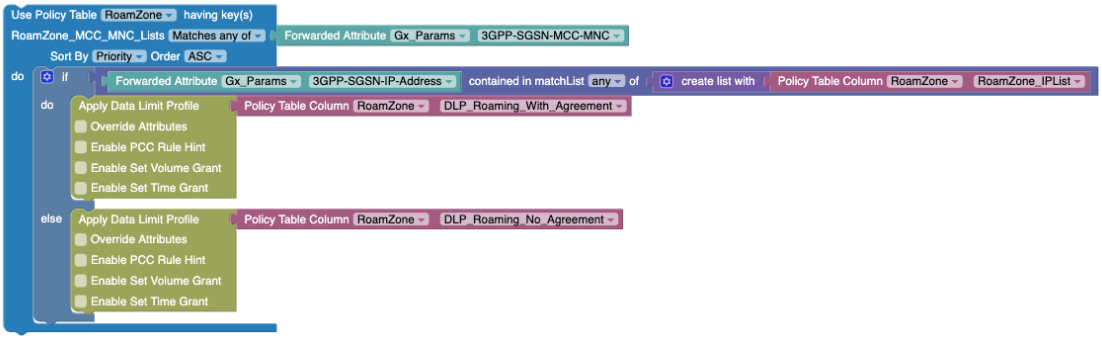
.

Using Policy Table Columns

Policy supports matching the value of a particular column similar to Match Lists.

Figure 4-63 Policy Table Column

Figure 4-64 Example: Use of Policy Table Column block



In the above example, If PRE value for the **Forwarded Attribute** block should be an exact match or the wildcard match with column `DNNString` in the table `HomeZone1`, then in the **if** condition block, the PRE value for the **Forwarded Attribute** block should match with the match list defined in the column `IPList` under the table `HomeZone1`.

If the given value "311", which exactly matches with the column name MCC, then in the `MatchList` block the given value "311490" will match with any of the value in the table column `MCCMNC`.

It can have any `MatchList` data type such as string, wildcard, IPv4, IPv6, or Regular expression.

5
Deprecated and Removed Blocks

With the evolving Cloud Native Core Policy blocks, we are identifying existing blocks that should be replaced with new blocks with enhanced functionality to improve overall customer experience. However, to ensure backward compatibility, the blocks are first marked as deprecated.

Deprecated Blocks

This section lists blocks that have been marked as deprecated with latest release. Users are recommended to review usage of these blocks in their current deployment, and make plans to upgrade to the suggested replacements.

The following table lists the deprecated blocks:

Table 5-1 List of deprecated blocks

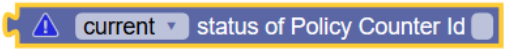
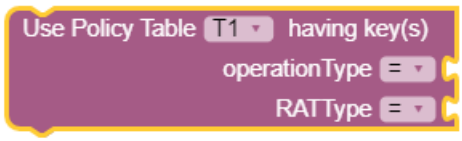
Block	Deprecated	Support Removed	Suggested Replacement
	1.9.0	TBD	NA
	1.7.0	TBD	This **Call policy** block has been replaced with new call policy block.
	1.8.0	TBD	This **Log:level** block has been replaced with new Log: level block.
	1.7.0	TBD	This request attribute in SMF block is deprecated only for two dropdown values - **requesterNFType** or **operationType**. If you wish to select any of these values, select request attributes block.
	1.10.0	TBD	This block under PCF-SM policy projects is deprecated. It has been replaced with Status of **Policy Counter ID** block available under Public category.

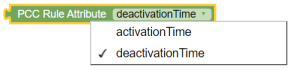
Table 5-1 (Cont.) List of deprecated blocks

Block	Deprecated	Support Removed	Suggested Replacement
	1.11.0	TBD	This block under the Policy Table sub-category of policy projects is deprecated. It has been replaced with **Use Policy Table** block available under Public category.

Removed Blocks

The following table lists the removed blocks:

Table 5-2 List of removed blocks

Block	Removed	Replacement
	1.8.0	This **PCC rule attribute** block has been replaced with new PCC rule dynamic override block.

A

Sample Policy Projects for Usage Monitoring

Important

This section provides a sample legacy OCPM policy in blockly design. The data in this section is meant for reference and may not be an optimized design. Oracle recommends you to use this information as reference only. To understand the overall Usage Monitoring use cases that a policy designer can use for optimized implementation, see Usage Monitoring Use Cases.

Figure A-1 Policy Project for Roaming Use Cases

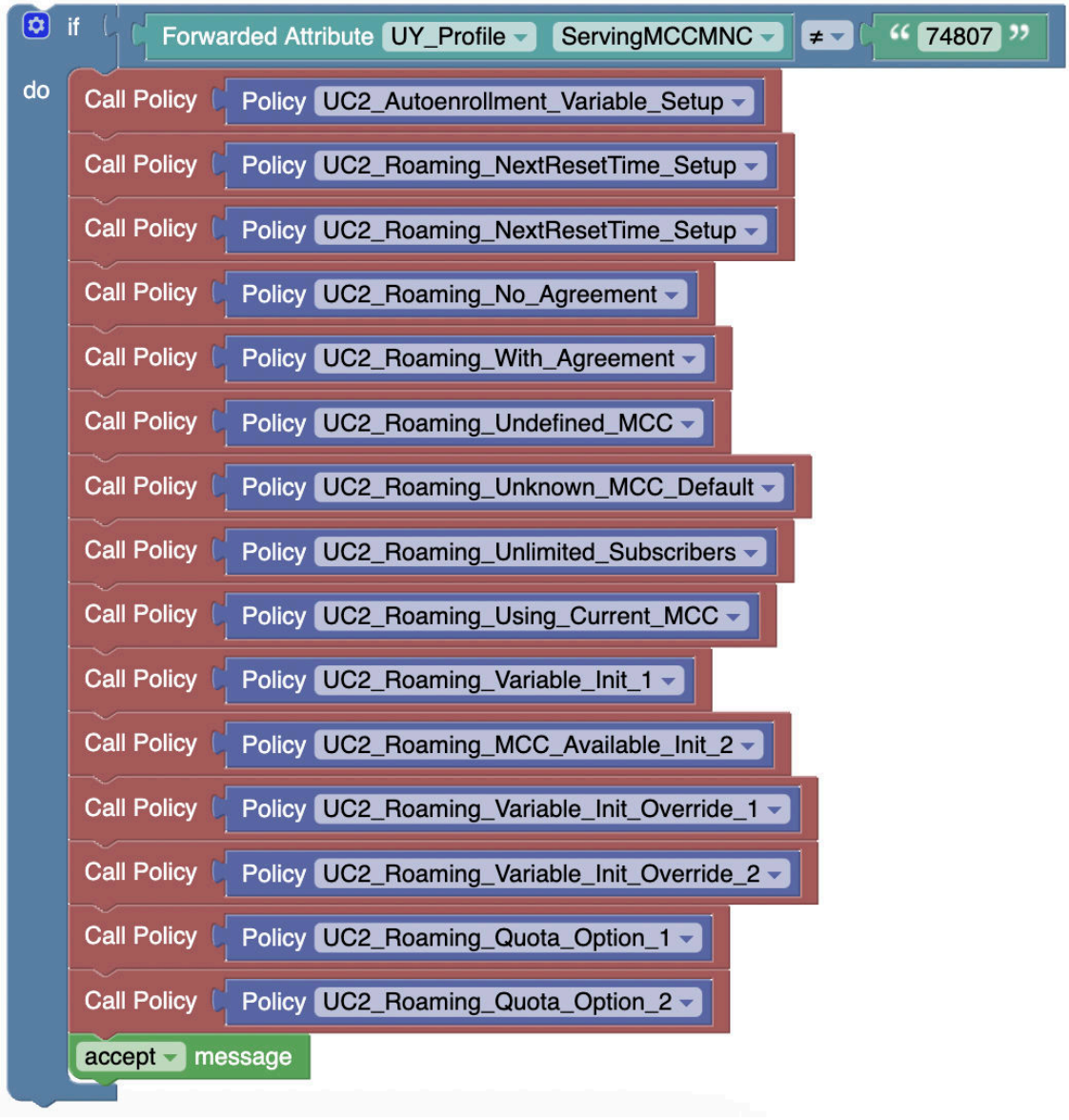


Figure A-2 Policy Project for Autoenrollment Variable Setup

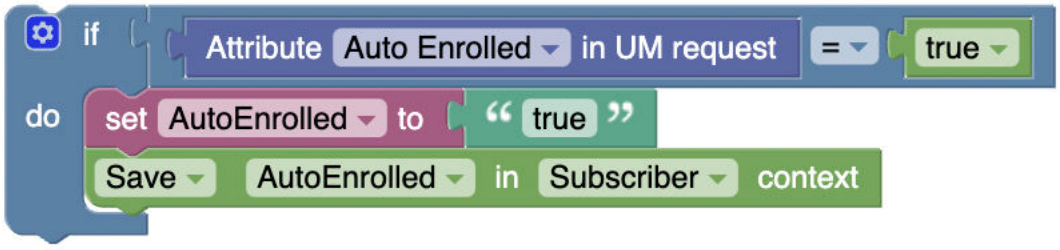


Figure A-3 Policy Project for Roaming NextResetTime Setup

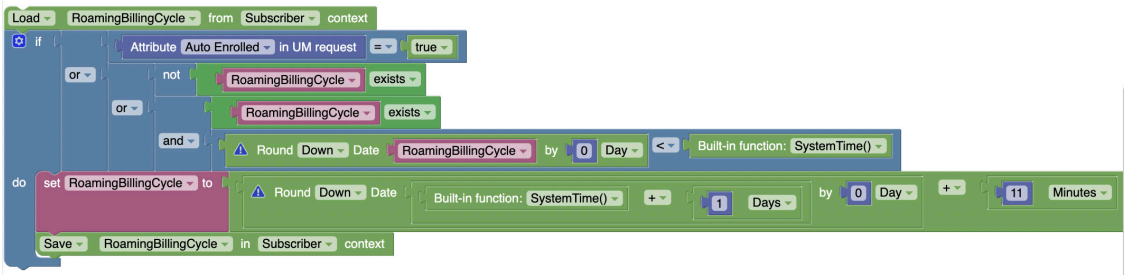


Figure A-4 Policy Project for Roaming No Agreement

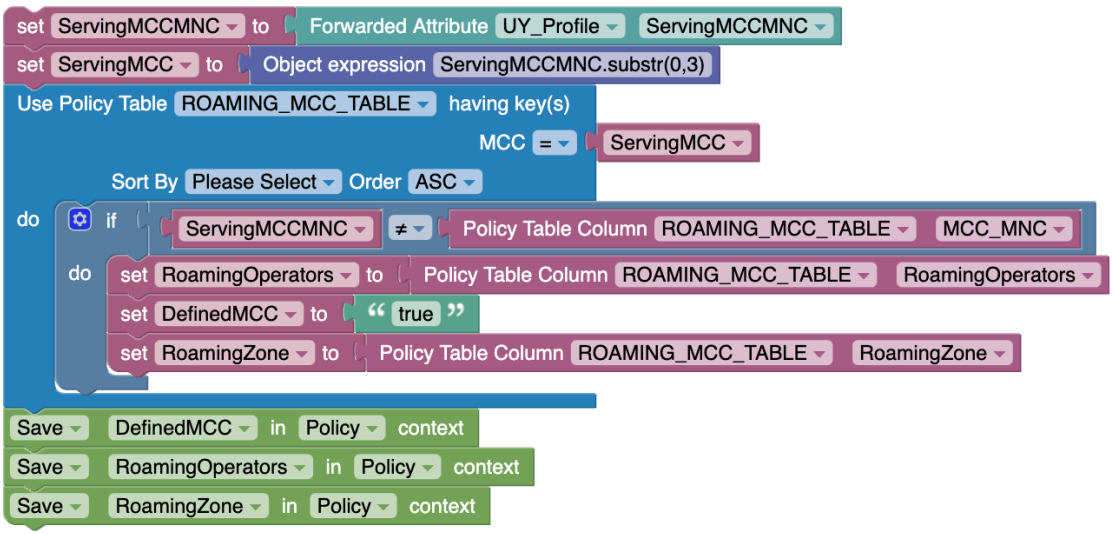


Figure A-5 Policy Project for Roaming With Agreement

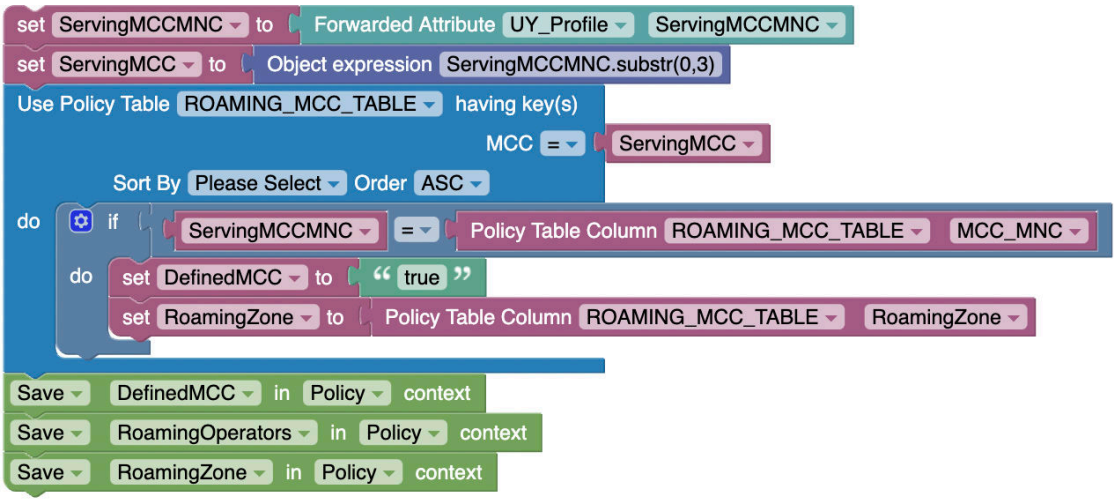


Figure A-6 Policy Project for Roaming Undefined MCC

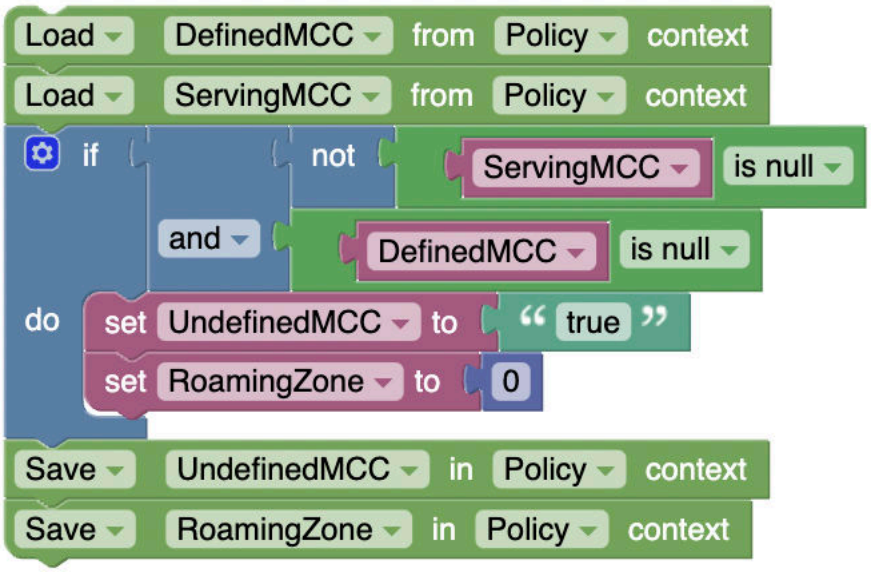


Figure A-7 Policy Project for Roaming Unknown MCC Default

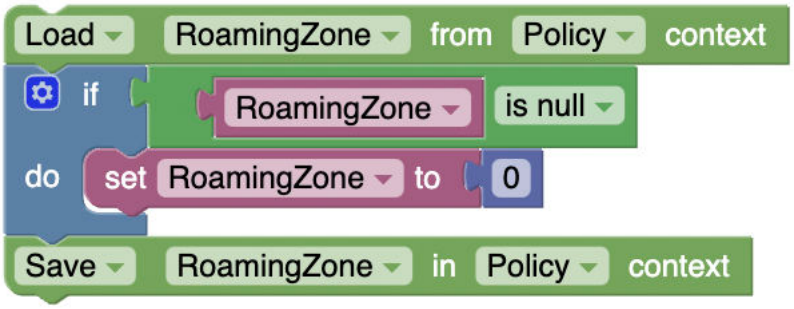


Figure A-8 Policy Project for Roaming Using Current MCC

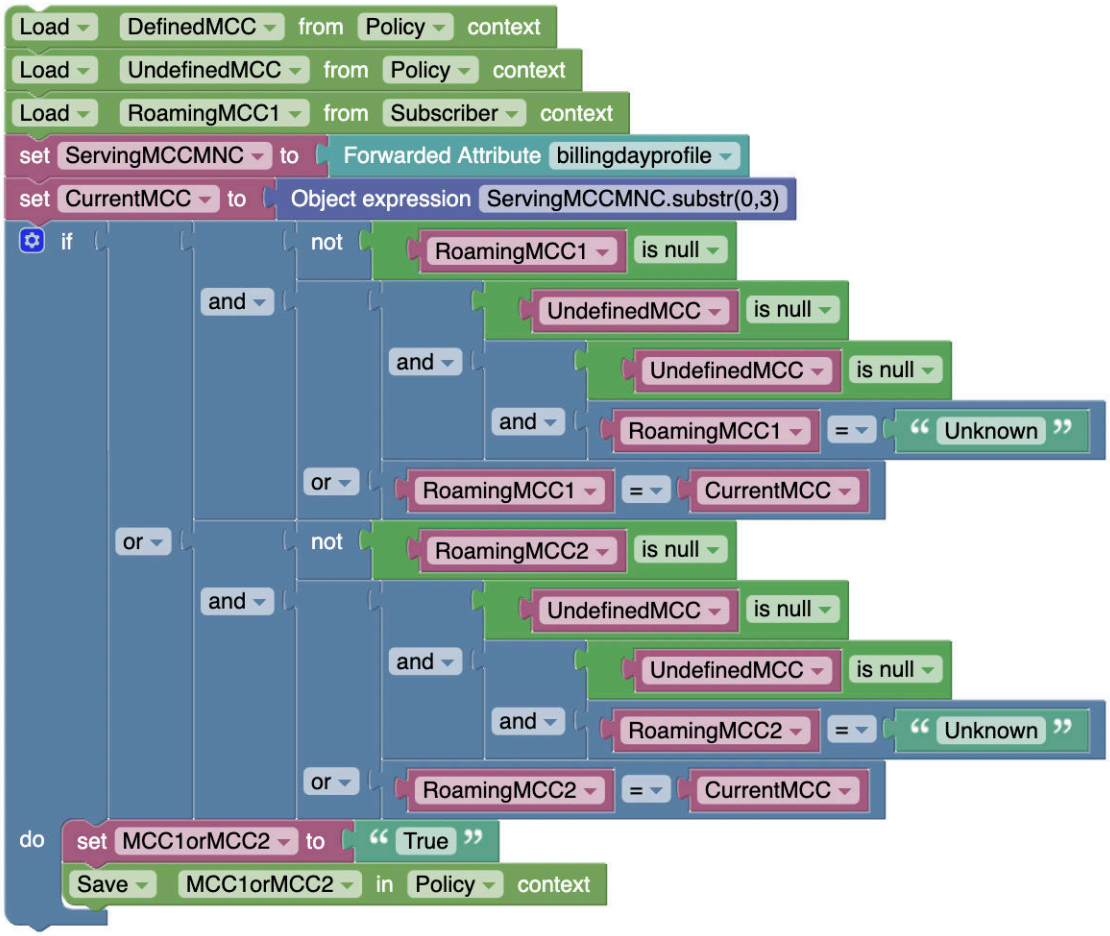


Figure A-9 Policy Project for Roaming Variable Init_1

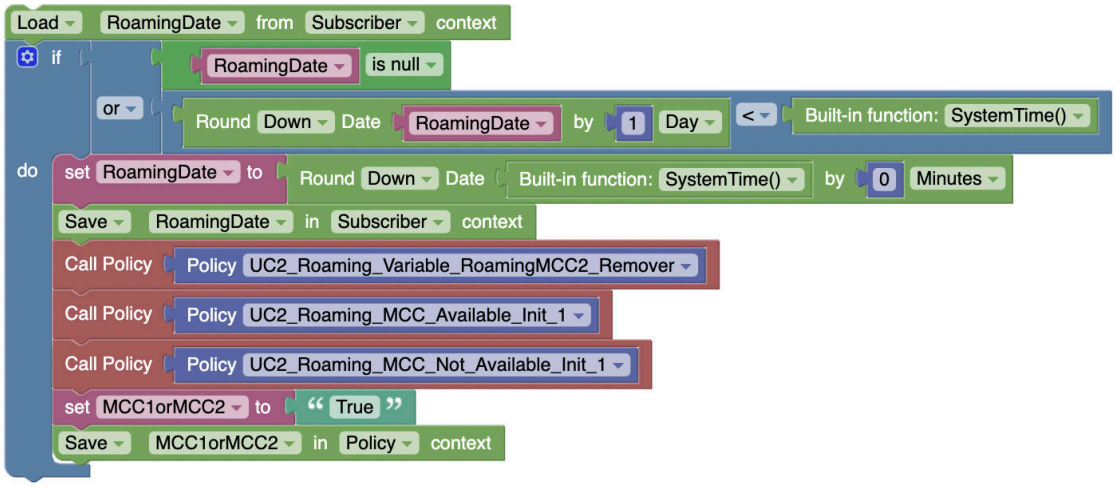


Figure A-10 Policy Project for Roaming Variable RoamingMCC2 Remover

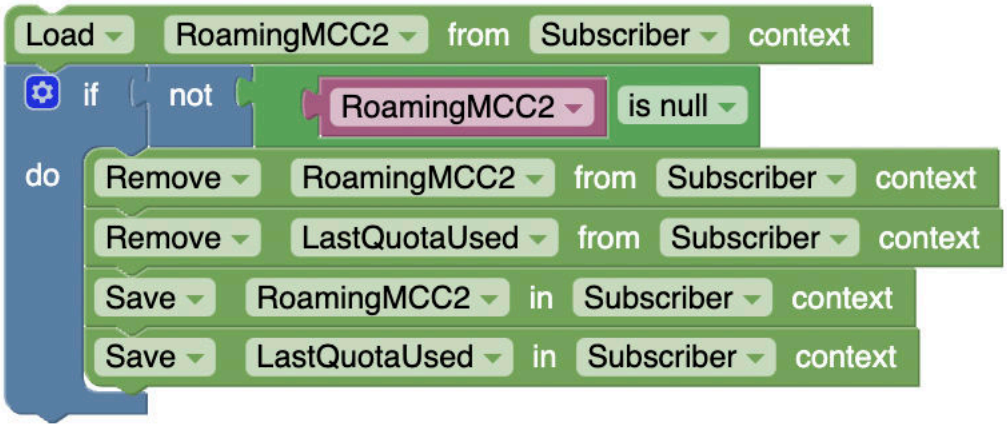


Figure A-11 Policy Project for Roaming MCC Available Init_1

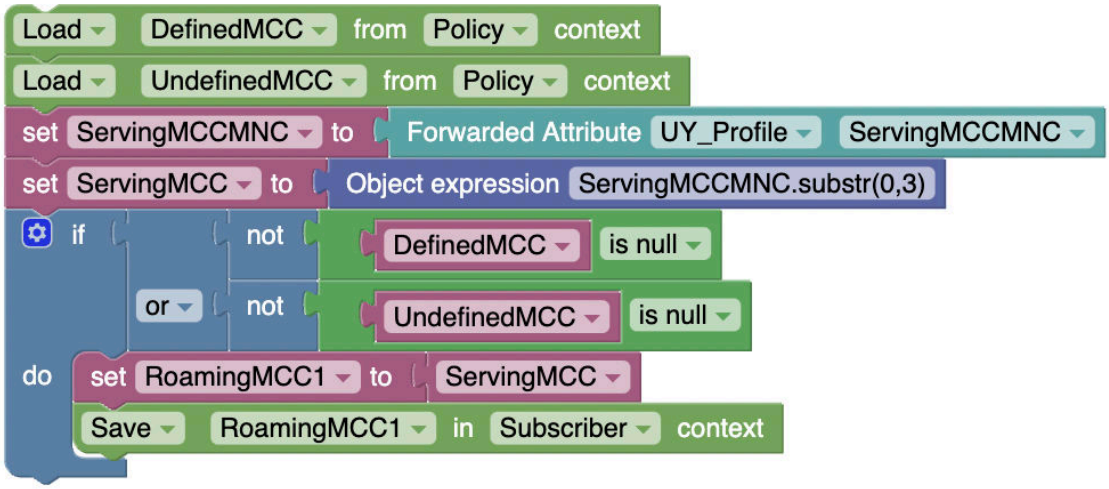


Figure A-12 Policy Project for Roaming MCC Not Available Init_1

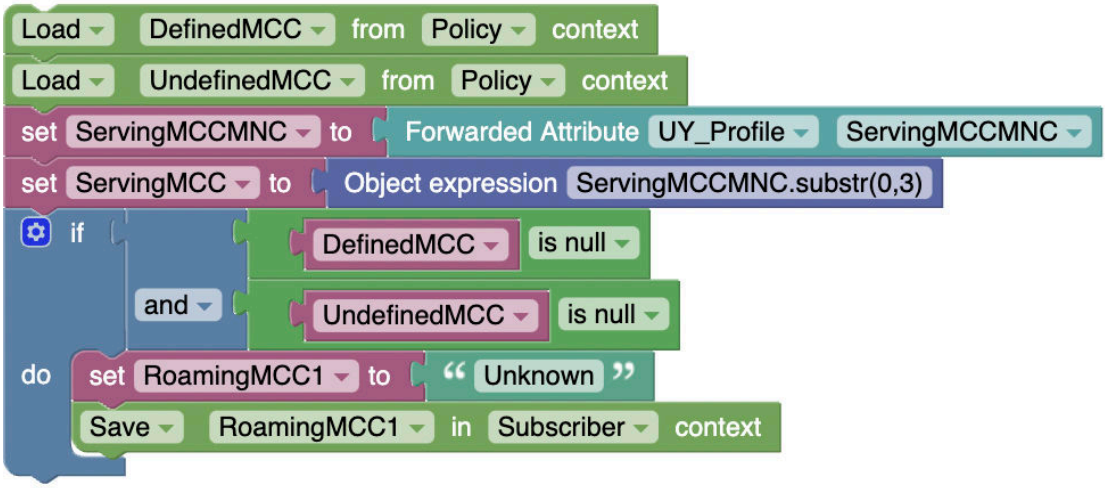


Figure A-13 Policy Project for Roaming Variable Init_2

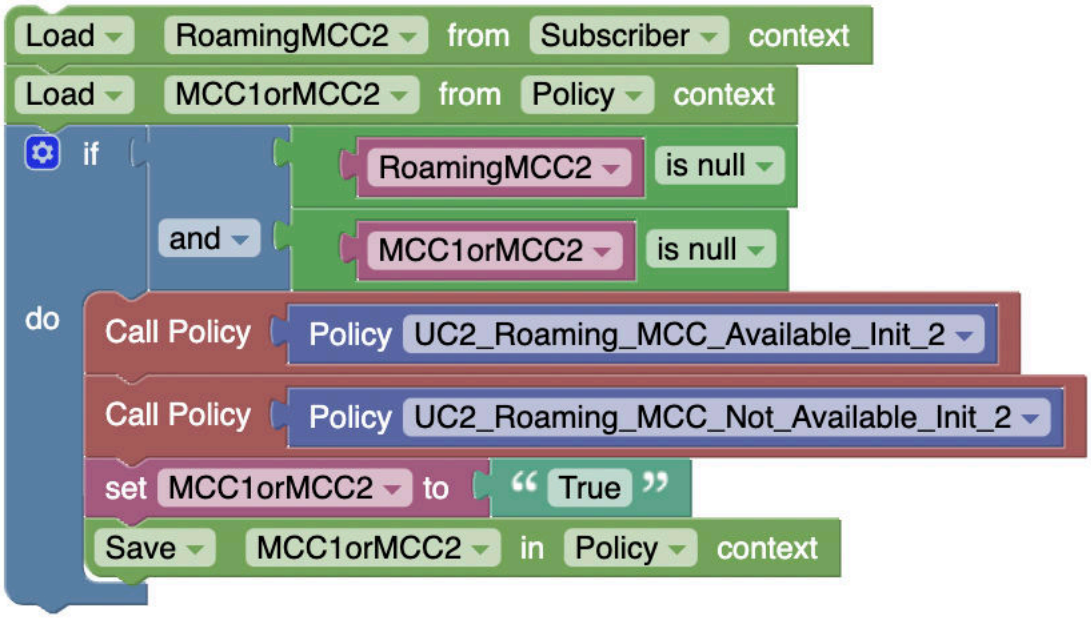


Figure A-14 Policy Project for Roaming MCC Available Init_2

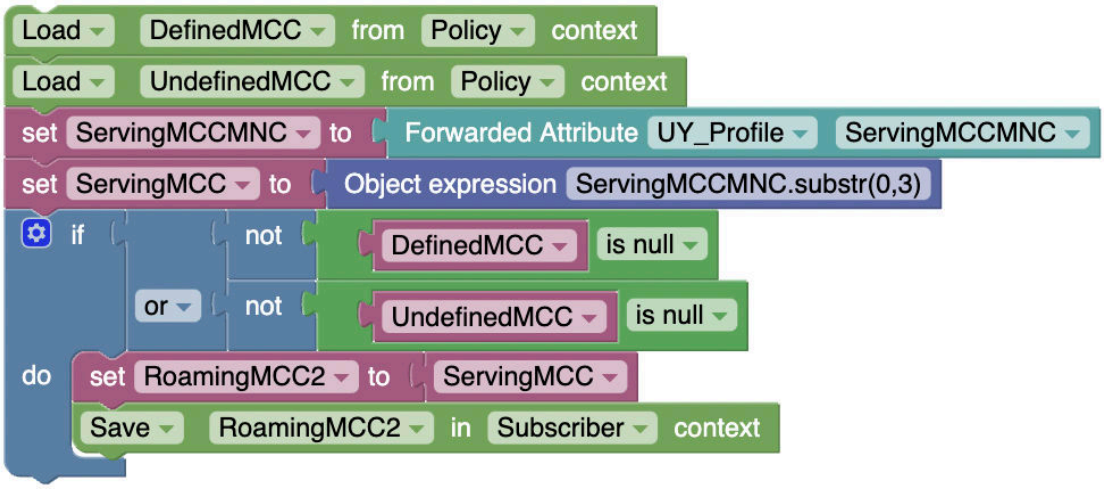


Figure A-15 Policy Project for Roaming MCC Not Available Init_2

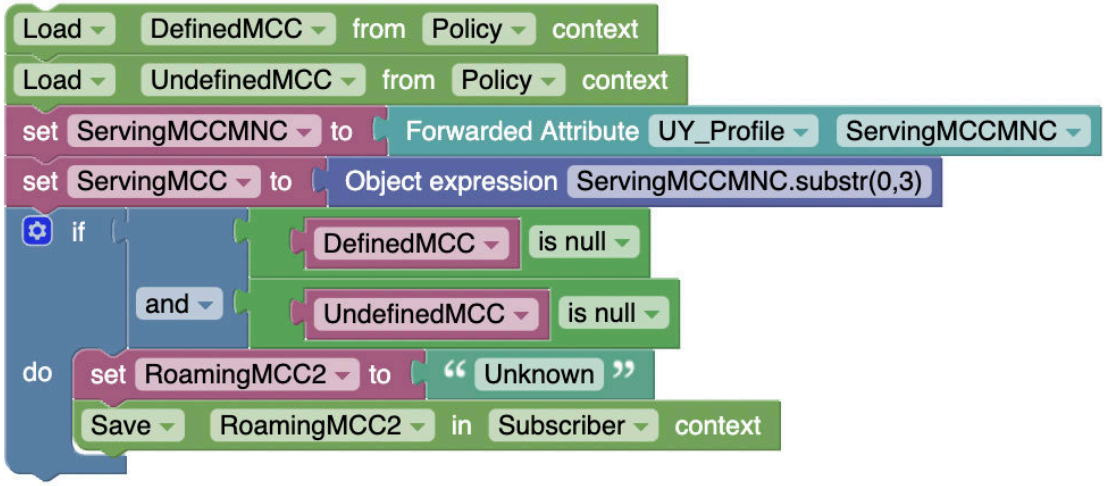


Figure A-16 Policy Project for UC2 Roaming Variable Init Override

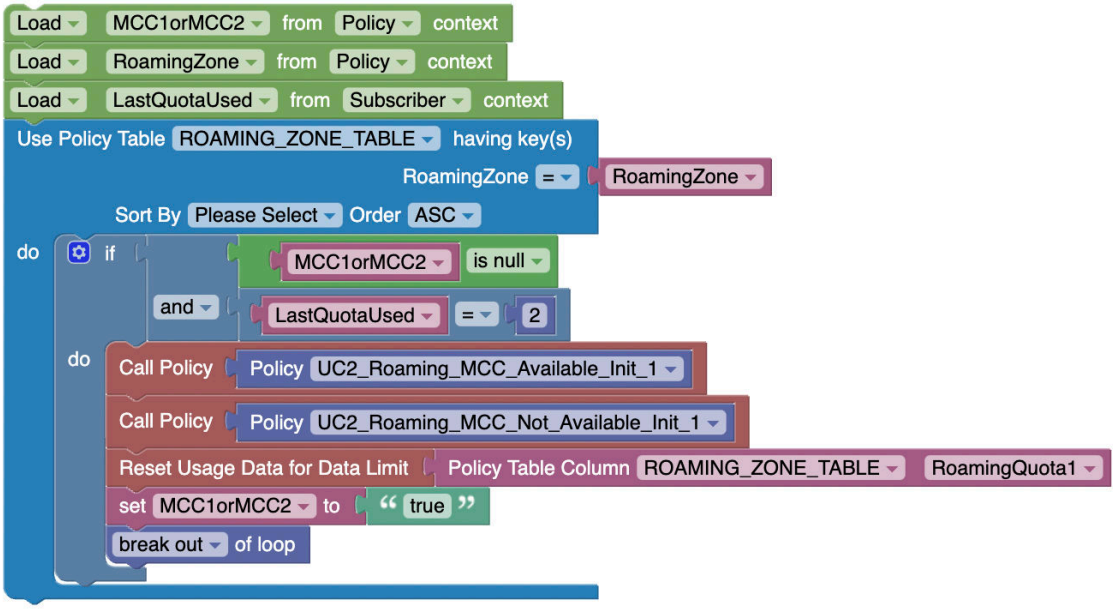


Figure A-17 Policy Project for Roaming Variable Init Override

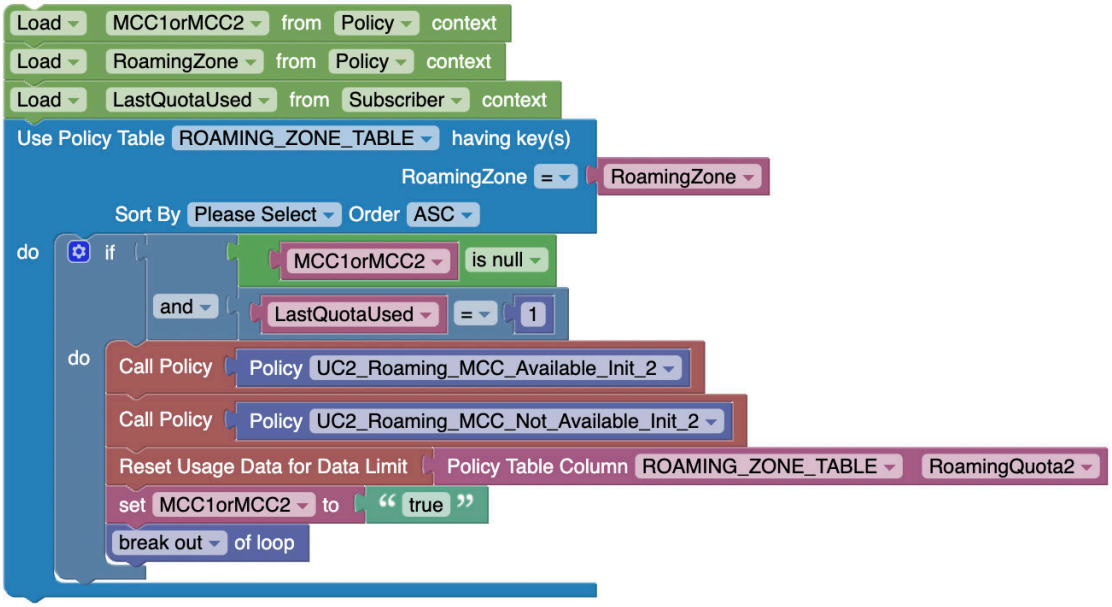


Figure A-18 Policy Project for Roaming Quota Option

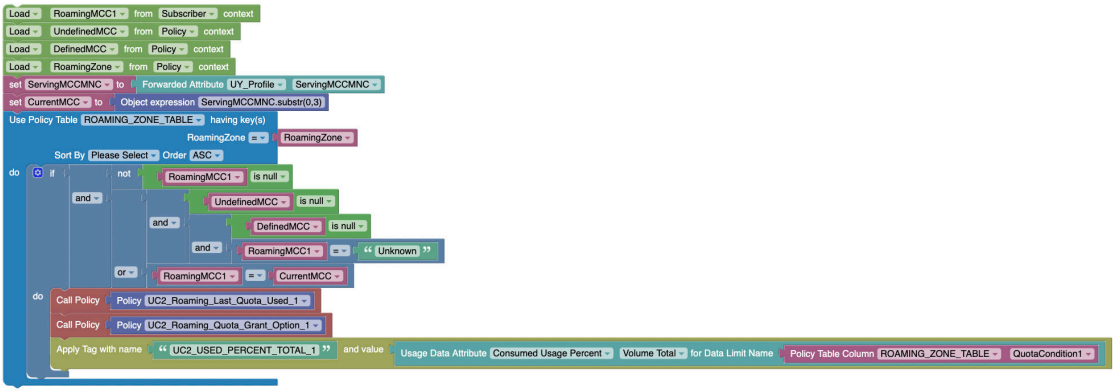


Figure A-19 Policy Project for Roaming Last Quota Used

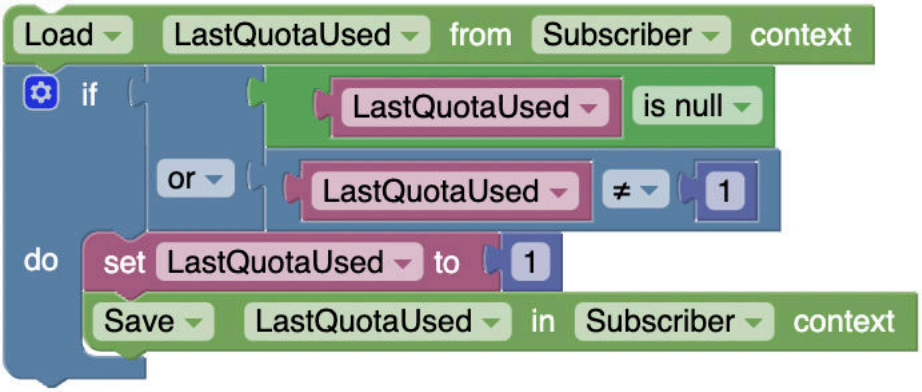
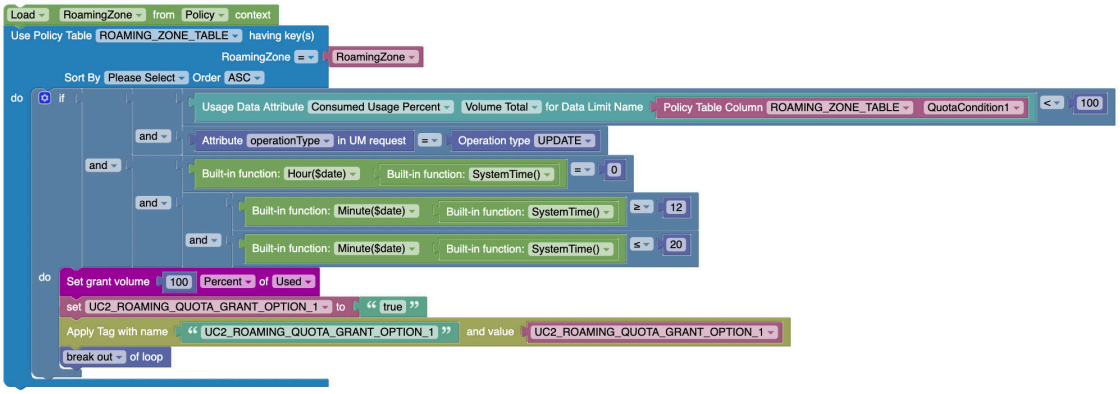


Figure A-20 Policy Project for Roaming Quota Grant Option



Sample Projects for PCRF Core

Figure A-21 Main

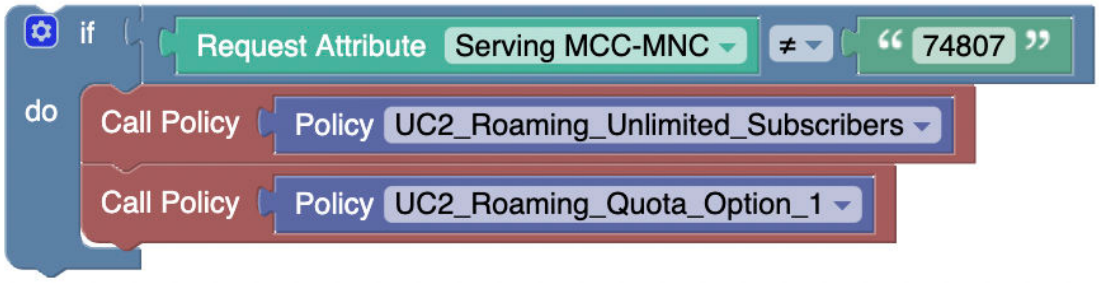


Figure A-22 Roaming Unlimited Subscribers

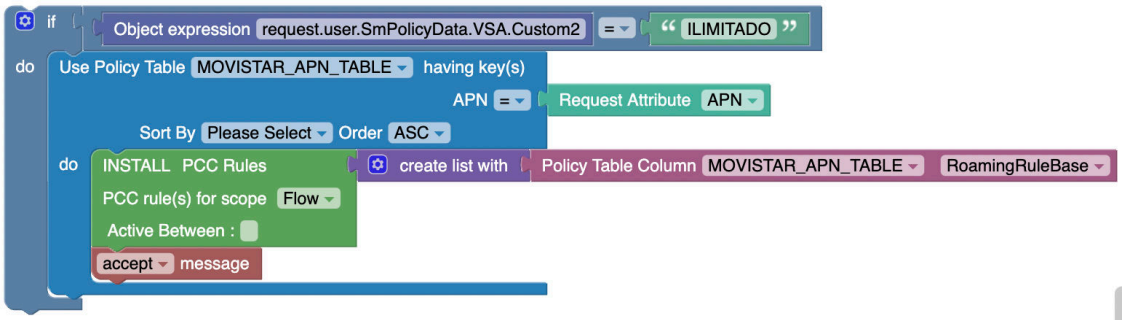


Figure A-23 Roaming Quota Option

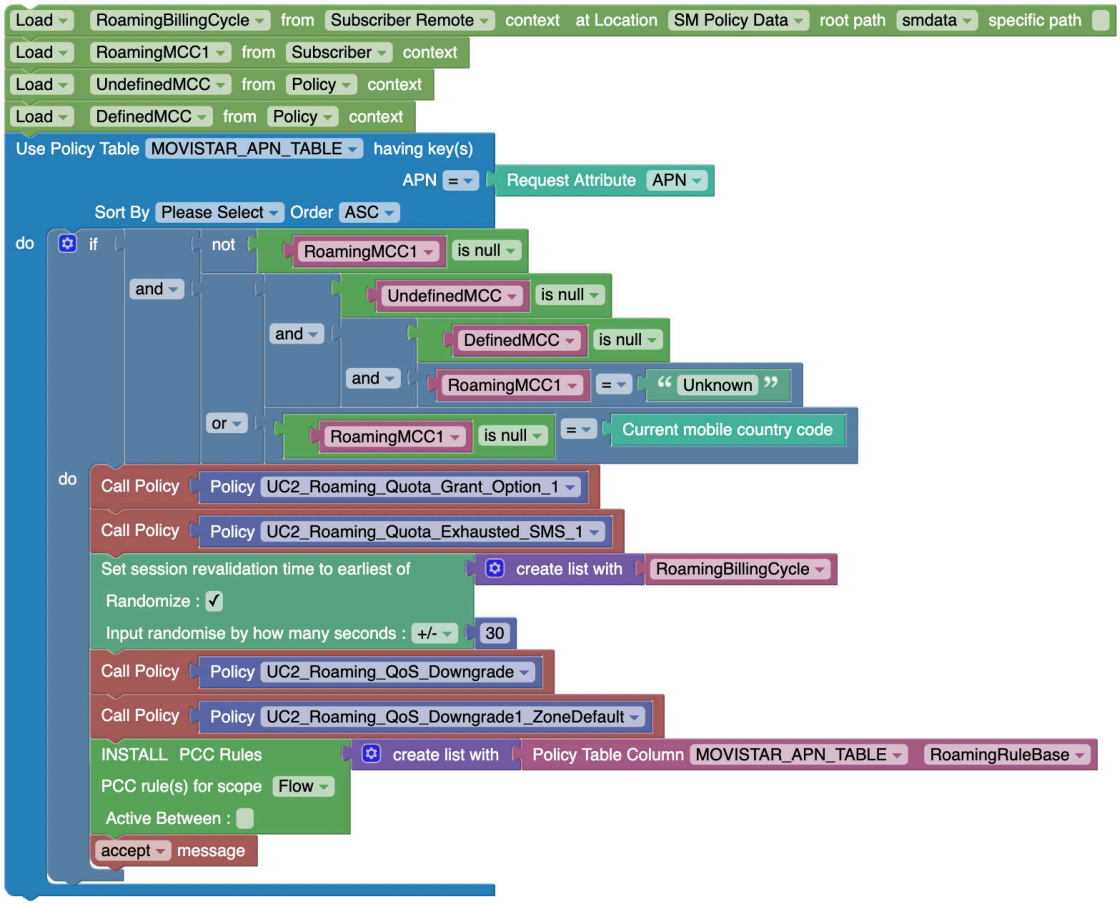


Figure A-24 Roaming Quota Grant Option

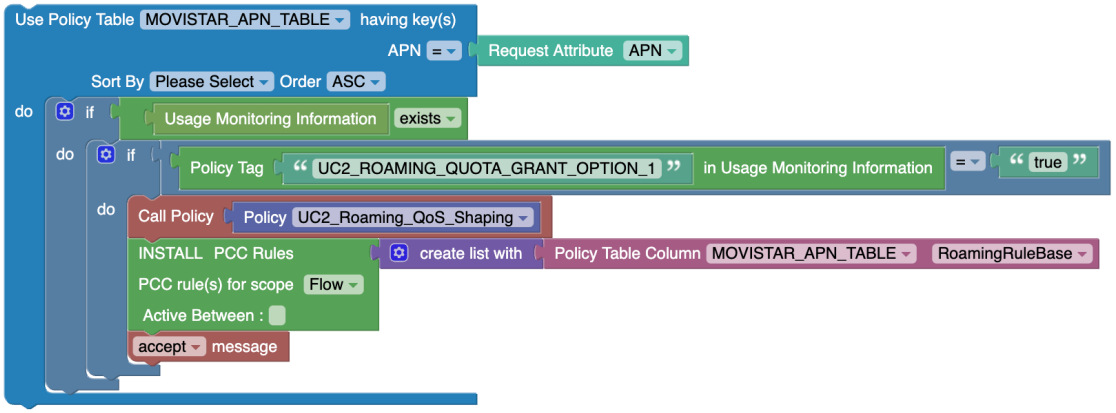


Figure A-25 Roaming QoS Shaping

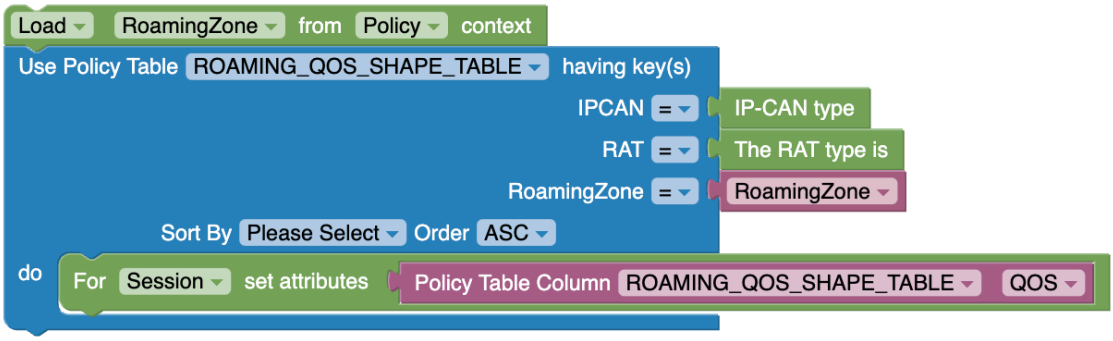


Figure A-26 Roaming Quota Exhausted SMS_1

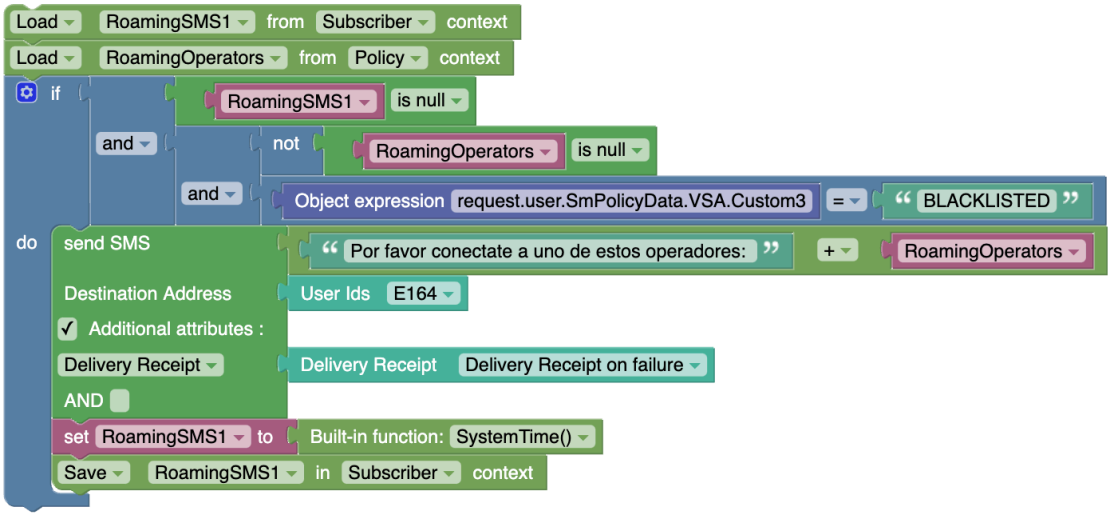


Figure A-27 Roaming QoS Downgrade

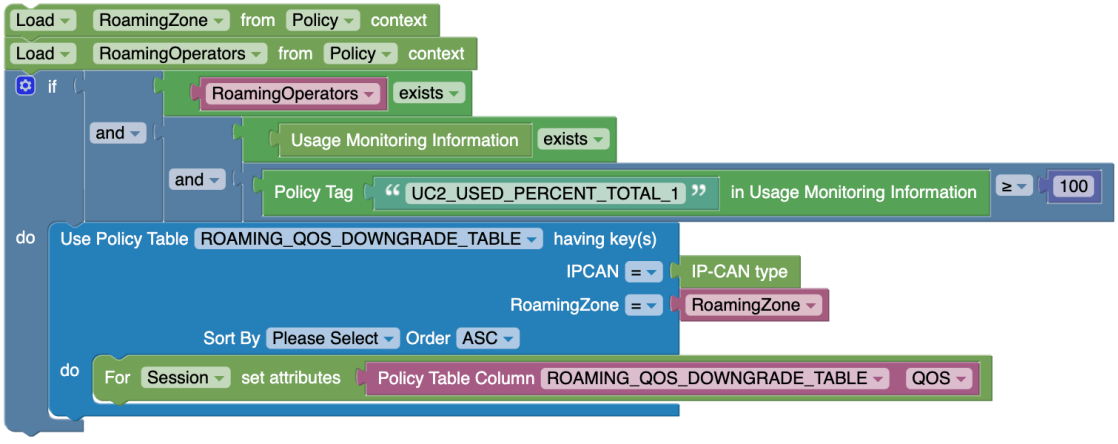
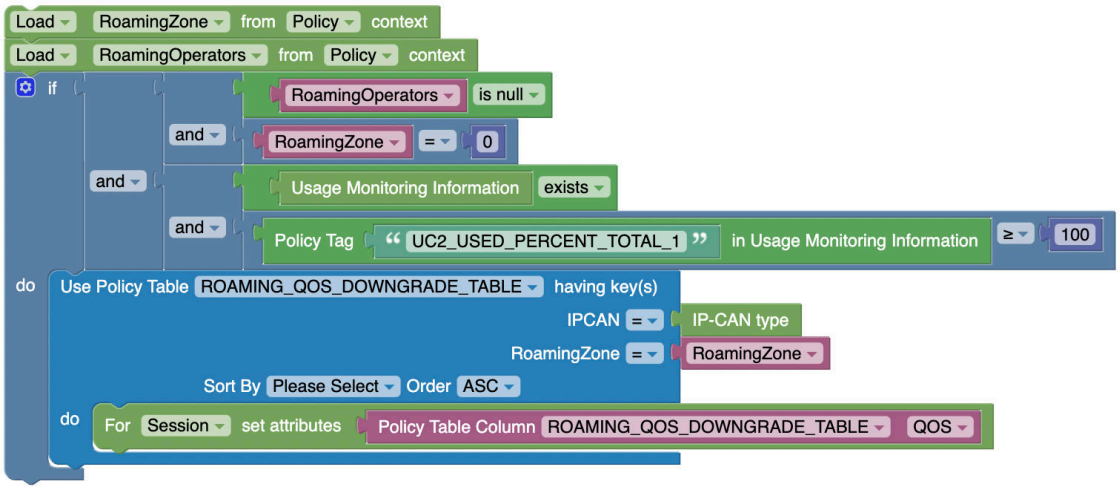


Figure A-28 Roaming QoS Downgrade1 ZoneDefault

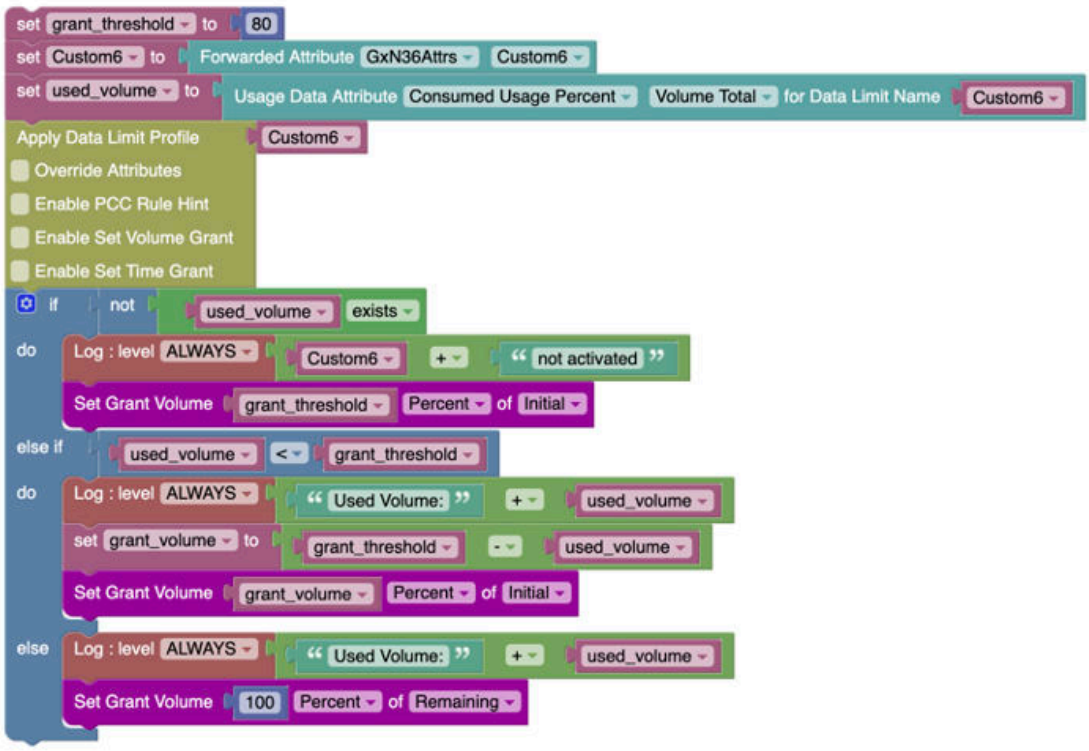


Granting Quota

Scenario:

- User plan is provided as subscriber VSA by UDR
- Grant 80% of Total (Initial) Quota at activation of plan.
- If user consumes less than 80%, then grant the delta quota again.
- Once user crosses 80%, grant remaining quota.
- At any time if user detaches, subsequent attach should grant quota as per last reported in CCR-T.

Figure A-29 Sample project:



Initial Condition: Plan is not activated.

Total Quota: 100K

Step #	Ingress Diameter Message	Quota Reported	Cumulative Quota Consumed	Quota Grant	Notes
1	CCR-I	-	-	80K	• User data fetched from UDR • Plan activated • Initial grant of 80%
2	CCR-U	20K	20K	60K	• Consumed Quota ((20K) updated on UDR. • Grant = 80K – 20K

Step #	Ingress Diameter Message	Quota Reported	Cumulative Quota Consumed	Quota Grant	Notes
3	CCR-T	30K	50K	-	• Consumed Quota (50K) updated on UDR. • Session Terminated
4	CCR-I	-	-	30K	• User data fetched from UDR • Grant = 80K – 50K
5	CCR-U	20K	70K	10K	• Consumed Quota (70K) updated on UDR. • Grant = 80K – 70K
6	CCR-U	10K	80K	20K	• Initial Grant of 80% consumed so grant remaining 20% • Grant = 100K – 80K
7	CCR-T	10K	90K	-	• Consumed Quota (90K) updated on UDR. • Session Terminated
8	CCR-I	-	-	10K	• User data fetched from UDR • Grant = 100K – 90K
9	CCR-U	10K	100K	-	• Total Quota Exhausted • No further Grant • Quota Disabled • Consumed Quota (100K) updated on UDR.

Step #	Ingress Diameter Message	Quota Reported	Cumulative Quota Consumed	Quota Grant	Notes
10	CCR-T	-	100K	-	• No Quota Reported as no Grant was given in previous decision.

PCC Rule Level Usage Monitoring

Figure A-30 Sample Policy Project for PCC Rule Level Usage Monitoring

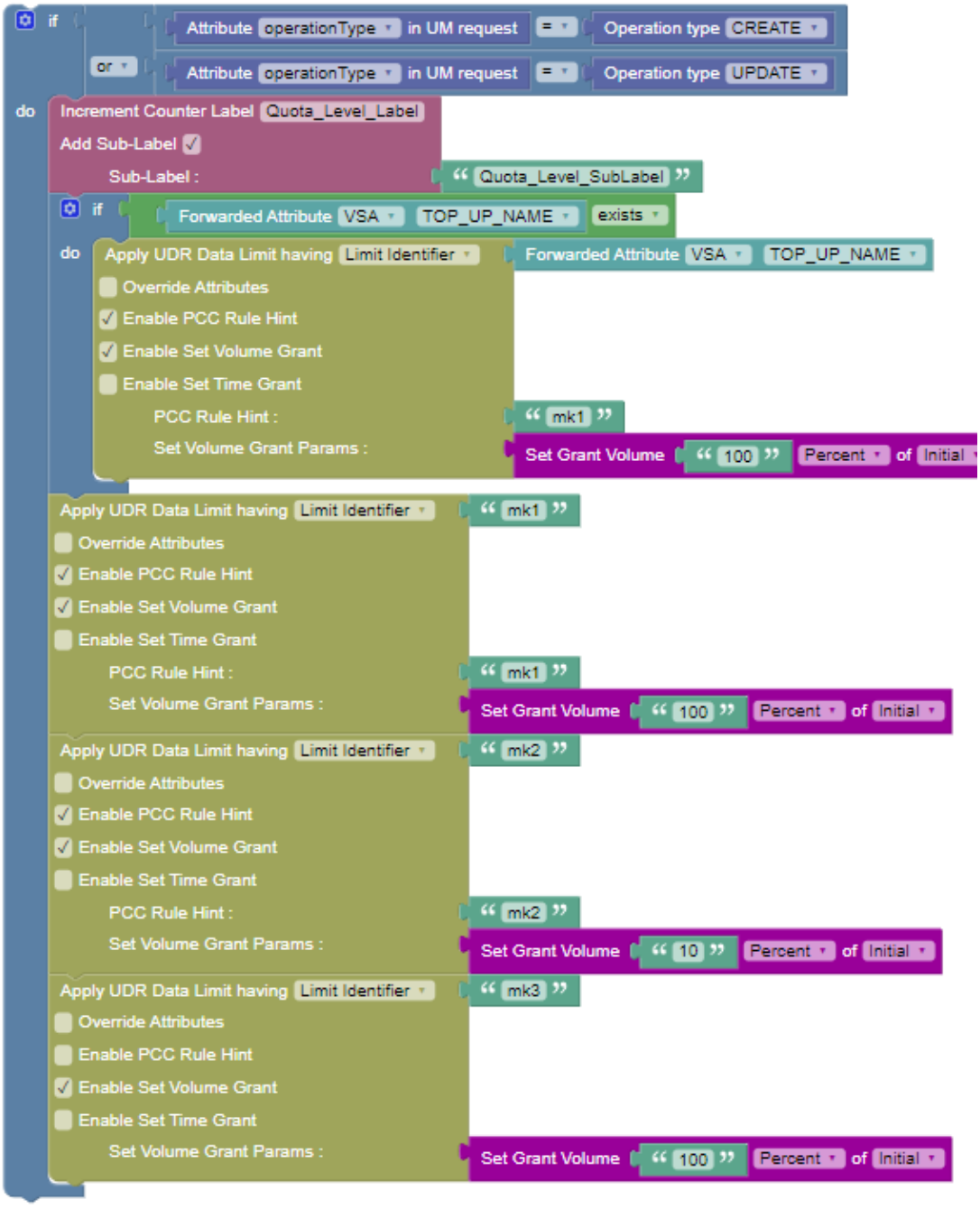
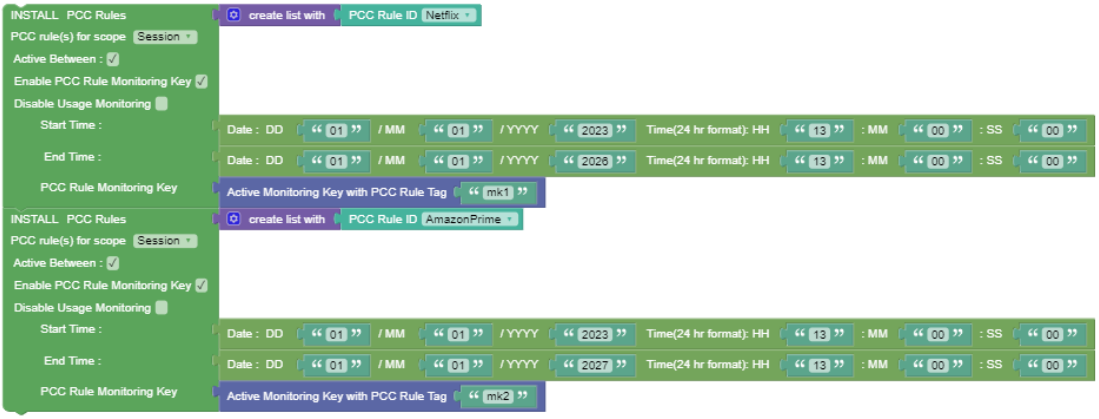


Figure A-31 Sample Policy Project for PCC Rule Level Usage Monitoring for PCRF Core



You must configure **PCC Rule** and **Predefined PCC Rule** in **Traffic Rule** page for **PCRF Core** under **Policy Data Configuration** in CNC Console.