

Oracle® Communications

Cloud Native Core, Service Communication Proxy REST Specification Guide



Release 23.4.4
F88459-05
October 2024

ORACLE®

Copyright © 2021, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1	Introduction	
1.1	References	1
2	SCP Configuration Using REST APIs	
2.1	Configuring SCP Features	2
2.2	Configuring Routing Options	25
2.3	Configuring Overload Configuration Information	73
2.4	Configuring Overload Configuration Information Threshold	79
2.5	Routing Options Configurations	83
2.6	Configuring System Options	98
2.7	Configuring NRF	102
2.8	OAuth2.0 Configurations	105
2.8.1	Configuring OAuth2.0 Access Token Granularity	105
2.8.2	Configuring OAuth2.0 Local PLMN Required	116
2.9	Configuring Error Profiles	122
2.10	Configuring CanaryRelease Options	132
2.11	Outlier Detection Configuration	134
2.12	Configuring NF Service Groups	138
2.13	Configuring NF Topology Groups	145
2.14	Fetching Release 15 Routing Rules	156
2.15	Configuring Ingress Rate Limiting	165
2.16	Configuring Egress Rate Limiting and Global Egress Rate Limiting	172
2.17	Configuring Dynamic Logging	181
2.18	Fetching Release 16 Routing Rules	186
2.19	Fetching Upgrade and Rollback Events	199
2.20	Updating HELM Configurable Parameters with REST APIs	202
2.21	Configuring Alternate NF Group	207
2.22	Configuring Server Header	216
2.23	Configuring SBI Message Priority	220
2.24	Pod Overload Control Configurations	229
2.24.1	Configuring Pod Overload Control Policy	229
2.24.2	Configuring Pod Overload Action Policy	235
2.24.3	Configuring Pod Overload Discard Policy	240

2.25	Configuring SEPP InterPlmn Info	244
2.26	Configuring App Routing Options	252
2.27	Configuring Mediation Trigger Point	261
2.28	Configuring Mediation Rule	273
2.29	Configuring Route Groups	285
2.30	Configuring Consumer NF Info	292
2.31	Configuring SCP Services	295
2.32	Configuring Load Control Information	324
2.33	Message Feed Configurations	328
2.33.1	Configuring Traffic Feed Data Director	328
2.33.2	Configuring Traffic Feed Trigger Point Config	333
2.34	Congestion Control Configurations	338
2.35	Circuit Breaking Configurations	346
2.36	Routing Config Set	352
2.37	NRF SRV Configuration	383
2.38	NRF FQDN InstanceId Mapping	390
2.39	Viewing SCP Feature Status	392

A HTTP Status Code and Applicability for Rerouting

B Error Code Generated by SCP

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

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

Table Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
API	Application Programming Interface
CCA	Client Credentials Assertion, 3gpp-Sbi-Client-Credentials header is defined by 3GPP. The header contains a client credentials assertion.
CNC Console	Oracle Communications Cloud Native Configuration Console
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
K8s	Kubernetes
LCI	Load Control Information
LC-H	Load Control based on LCI Header
MCC	Mobile Country Code
MNC	Mobile Network Code
NF	Network Function
NRF	Oracle Communications Cloud Native Core, Network Repository Function
OCI	Overload Control Information
OLC-H	Overload Control based on OCI Header
PLMN	Public Land Mobile Network
REST	Representational State Transfer
SBI	Service Based Interface
SCP	Oracle Communications Cloud Native Core, Service Communication Proxy
SCPC	Service Communication Proxy Control
SEPP	Oracle Communications Cloud Native Core, Security Edge Protection Proxy
SPN	Service Proto Name
SRV	Service Records
URI	Uniform Resource Identifier
XFCC	x-forwarded-client-cert is a proxy header that indicates TLS certificate information.

What's New in This Guide

This section introduces the documentation updates for release 23.4.x.

Release 23.4.4 - F88459-05, October 2024

There are no updates made to this document.

Release 23.4.3 - F88459-04, July 2024

There are no updates made to this document.

Release 23.4.2 - F88459-03, April 2024

- Added `ociEnabled` and `ociRuleName` parameters to [Routing Config Set](#) and [Configuring Routing Options](#) sections.
- Updated the value of `deliveryTimeoutMs` from 120000 to 5000 in the [Configuring Traffic Feed Data Director](#) section.

Release 23.4.1 - F88459-02, February 2024

- Added `kafkaPartitionSelectionLogic` and `deliveryTimeoutMs` parameters in the [Configuring Traffic Feed Data Director](#) section as part of the Message Feed enhancements.
- Updated the [Configuring SCP Features](#) section to enable or disable the NFProfile Processing enhancements supported by SCP.

Release 23.4.0 - F88459-01, December 2023

- Added NRF as supported NFtype to the egress rate limiter data in the [Configuring Egress Rate Limiting and Global Egress Rate Limiting](#) section.
- The following changes are made as part of the NRF Configuration using DNS SRV Resolution feature:
 - Updated the [Configuring SCP Features](#) section to enable or disable NRF configuration using the DNS SRV resolution feature.
 - Added the [NRF SRV Configuration](#) section to create or configure the new NRF SRV configuration for the given `nrfSrvFqdn`.
 - Added the [NRF FQDN InstanceId Mapping](#) section to fetch the NRF FQDN and corresponding `instanceId` mapping details.
 - Updated the [Configuring NRF](#) section with information about the support for load balancing feature for the delegated discovery request.
- The following changes are made as part of the Overload Control Based on the Overload Control Information Header feature:
 - Updated the [Configuring SCP Features](#) section to enable or disable the Overload Control Information (OCI) feature.
 - Added the [Configuring Overload Configuration Information](#) section with information about overload control configuration parameters required for sending OCI to peers.
 - Added the [Configuring Overload Configuration Information Threshold](#) section with information about overload control configurations required for the `OciThresholdConfig` threshold levels to generate self -OCI by SCP.

- Updated the [Configuring Routing Options](#) section as a part of the SCP Response Timeout Extension feature.
- Updated the default value for transport failures in SCP in [Configuring Routing Options](#) and [Routing Config Set](#) sections.
- Added the [Configuring Mediation Rule](#) section for creating, modifying, and deleting Mediation rules.

1

Introduction

This document provides information about how to configure the services and manageable objects in Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) using Representational State Transfer Application Programming Interfaces (REST APIs).

The core network in 5G follows a service-based architecture, where network functions provide services that can be utilized using REST APIs by other functions. This allows the adoption of web-scale technologies and software that are used by different organizations in the telecommunications network.

SCP provides routing, load balancing, rate limiting, static configuration, dynamic discovery, and so on, functionalities to other 5G Network Functions (NFs). For more information about SCP functionalities and features, see *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

Note

The performance and capacity of the SCP system may vary based on the call model, feature or interface configuration, network conditions, and underlying CNE and hardware environment.

1.1 References

- *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*
- *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*

2

SCP Configuration Using REST APIs

This chapter provides information about how to configure Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) using REST APIs.

SCP can be configured using Helm and REST configurations. Some configurations are performed during SCP installation using Helm and a few configurations are modified using REST APIs. REST configurations can also be performed using the Oracle Communications Cloud Native Configuration Console (CNC Console).

For more information about SCP configuration types, see the following guides:

- For Helm configuration: *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
- For REST configurations using the CNC Console: *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

SCP uses GET, PUT, DELETE, and so on HTTP methods to retrieve, update, and remove REST API configuration data.

Note

- The PUT method for multiple rules as a single payload through a single API is not allowed unless specified explicitly.
- If the query parameter is incorrect, SCP does not return an error response but considers an API call without any query parameter, and therefore the GET ALL output is returned in the response.

SCP Service Interfaces

SCP provides the following service interfaces:

- **Signaling Interface:** The signaling interface is exposed by SCP data plane called SCP-Worker. This interface is used to receive all 5G signaling traffic.
- **Config Interface:** The config interface is exposed by SCP control plane called SCPC-Config. This interface is used to receive all SCP configuration traffic.

SCP Signaling Service

SCP provides the following Signaling services:

- **FQDN**
 - Consumer NFs may use SCP Signaling service's FQDN to send 5G signaling traffic to SCP for routing. The Kubernetes service FQDN is of the following format:
 - * fqdn = scp-worker.<namespace>.<domain>. Where, namespace is Kubernetes namespace as provided during the Helm installation, and domain is as provided in the Helm chart (values.yaml) while installation.

- * If user NFs are deployed outside of Kubernetes cluster, then operator must ensure that this FQDN is resolvable by consumer NFs.
 - * Operator can specify the public or Kubernetes-cluster FQDN of SCP in the Helm chart (values.yaml, scpInfo.fqdn" = <releaseName>-scp-worker.<Namespace>.<domain>) during installation.
- **IP Address**
 - Consumer NFs may use SCP Signaling service's IP address to send the 5G signaling traffic to SCP for routing.
 - IP is <global.publicSignalingIP> as provided in the Helm chart (values.yaml) during SCP installation.

Note

Only IPv4 is supported.

- **Port**
 - Consumer NFs require port information along with FQDN or IP address to send 5G signaling traffic to SCP for routing.
 - Port is <global.publicSignalingPort> as provided in the Helm chart (values.yaml) during SCP installation.

SCP Config Service

SCP provides the following Config service:

- **FQDN**
 - Operator may use SCP Config service's FQDN to configure SCP for routing.
 - The Kubernetes service FQDN is of the following format:
 - * fqdn = scpc-config-svc.<namespace>.<domain>. Where, <namespace> is Kubernetes namespace as provided during the Helm installation, and <domain> is as provided in the Helm chart (values.yaml) during SCP installation.
 - * Operators must ensure that this FQDN is resolvable if operating from outside of the Kubernetes cluster.
- **IP Address**
 - Consumer NFs may use SCP Config service's IP Address to configure SCP for routing.
 - IP is <scpc-soothsayer.configService.publicConfigIP> as provided in the Helm chart (values.yaml) during SCP installation.
- **Port**
 - Operators require port information along with FQDN or IP address to configure SCP for routing.
 - Port is 8081 that is a fixed port and cannot be configured.

2.1 Configuring SCP Features

This section provides REST API configurations to enable SCP features.

Resources

The following table describes the resource name to retrieve, add, or update SCP features.

Table 2-1 Resource Name

Resource Name	Resource URI	HTTP Method	Description
scp-features	/ocscp/scpc-configuration/v1/scp-features	GET	Retrieves all the SCP features configured list at SCP or specific records based on the query parameters.
scp-features	/ocscp/scpc-configuration/v1/scp-features/{featureName}	GET	Retrieves records based on featureName as a path variable.
scp-features	/ocscp/scpc-configuration/v1/scp-features/{featureName}	PUT	Adds or updates the SCP feature interplmn routing configurations in SCP.

Data Model

Request Body

The following table describes the field names of the SCPFeaturesWrapper data type.

Table 2-2 SCPFeaturesWrapper

Field Name	Data Type	P	Description
featureName	String	M	Indicates the unique feature name as per the requirement. Supported values are: • <code>modeld_routing</code>: To enable or disable Release 16 Model D based routing. • <code>mediation</code>: To enable or disable Mediation. • <code>interplmn_routing</code>: To enable or disable the support for 5G SBI roaming. • <code>global_egress_ratelimit</code>: To enable or disable the Global Egress Rate Limiting and its specific configurations. • <code>enhanced_nf_status_processing</code>: To enable or disable the SUSPENDED NF Status processing. • <code>scp_user_agent_info</code>: To enable or disable addition of the "User-Agent" header in the SCP originated messages towards NRF. • <code>lci</code>: To enable or disable Load Control based on the Load Control Information (LCI) Header feature. • <code>Traffic Feed</code>: To enable or disable copying of both request and response messages routed through SCP towards Data Director • <code>egress_host_preference</code>: To enable or disable egress host preference. • <code>location_hdr_update_for_host_mismatch</code>: To enable or disable inter-SCP routing of subsequent 5G SBI request messages for unknown FQDNs as part of the Location Header for Host Mismatch feature. • <code>cca_header_validation</code>: To enable or disable Client Credentials Assertion (CCA) header validation. • <code>health_check</code>: Enables the Health Check API feature. By default, this feature is enabled. • <code>oauth2_support</code>: This parameter enables or disables the OAuth2.0 (Open Authorization) access tokens feature. • <code>nrf_bootstrap_info</code>: To enable or disable NRF configuration using the DNS SRV resolution feature and its configuration.

Table 2-2 (Cont.) SCPFeaturesWrapper

Field Name	Data Type	P	Description
			- oci: To enable or disable the Overload Control Information (OCI) feature. - ignore_unknown_nfservice: To enable or disable NFProfile Processing enhancements supported by SCP. - enhanced_error_rsp: To enable or disable Error Response enhancement supported by SCP.
enabled	Boolean	M	Enables or disables a feature. The values can be true or false. By default, this value is false.
featureSpecificConfig	customObject	O	Indicates feature specific configuration objects.

Table 2-3 Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
global_egress_ratelimit	featureSpecificConfig : { "remoteScpOneEnabled": "false", "remoteScpTwoEnabled": "false" }	This parameter enables or disables the Global Egress Rate Limiting feature. remoteScpOneEnabled: This parameter indicates whether SCP cache connectivity should be started for the remote SCP participant. Type: Boolean remoteScpTwoEnabled: This parameter indicates whether SCP cache connectivity should be started for the remote SCP participant.
modeld_routing	featureSpecificConfig: { "caching": "true", "enforceReqSpecificSvcDiscovery": "true" }	This parameter enables or disables the Model D Indirect 5G SBI Communication feature. caching: This parameter indicates whether local cache is enabled for Model D rules. enforceReqSpecificSvcDiscovery: This parameter enforces NF Service specific Discovery Request when possible.
mediation	NA	Not applicable for mediation. Keep this field blank.
interplmn_routing	NA	Not applicable for inter-plmn routing. Keep this field blank.

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
enhanced_nf_status_processing	<pre>featureSpecificConfig : { "enhancedSuspendedStateRo uting": ["AMF", PCF]" , "suspendedStateRouting": ["UDM"] }</pre>	This parameter enables or disables the NF Status Processing feature. enhancedSuspendedStateRouting: This parameter is used to indicate the list of NFTypes for which SCP would consider "SUSPENDED" NFs available for routing or alternate routing only when alternate is not available in the "REGISTERED" state. This parameter is used to list NFTypes eligible for Mode 3. An * means that all NFTypes are eligible for Mode 3. suspendedStateRouting: This parameter is used to indicate the list of NFTypes for which SCP would consider "SUSPENDED" NFs available for routing. This parameter is used to list the NFTypes eligible for Mode 2. An * means that all NFTypes are eligible for Mode 2. Type: array(NFType) Note: To specify all NFTypes for Mode-3, the list has to be specified with the wildcard *. Example: <pre>featureSpecificConfig : { "enhancedSuspendedStateRouting": ["*"] , "suspendedStateRouting": [] }</pre> Note: • Mode 1: If the enhanced_nf_status_processing is set to false, only NFs in the REGISTERED state are considered for routing. • Mode 2: If the enhanced_nf_status_processing is set to true and suspendedStateRouting is present, all configured NFs are considered for routing, irrespective of their NF state (REGISTERED or SUSPENDED). • Mode 3: If the enhanced_nf_status_processing is set to true and enhancedSuspendedStateRouting is present, SCP considers SUSPENDED NFs available for routing or alternate routing only when the alternate NF is not available in the REGISTERED state. • If enhancedSuspendedStateRouting is set to a subset of NF types such as AMF and PCF, SCP applies routing Mode 3 for AMF and PCF, and the remaining NF types will be routed to Mode 1. • If suspendedStateRouting is set to a subset of NF types such as AMF and PCF, SCP applies routing Mode 2 for AMF and PCF, and the remaining NF types will be routed to Mode 1. • If suspendedStateRouting and enhancedSuspendedStateRouting are

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		configured for mutually exclusive NF types such as UDM and PCF, then SCP will route UDM to Mode 2 and PCF to Mode 3, respectively, and the remaining NF types will be routed to Mode 1.
scp_user_agent_info	"featureSpecificConfig": { "userAgentHeaderFormat": "NFType-NFInstanceID FQDN", "uniqueID": "string/text input" }	This parameter enables or disables addition of "User-Agent" header in the SCP originated messages towards NRF. userAgentHeaderFormat: This parameter indicates the format of the "User-Agent" header that is added in the SCP originated message requests towards NRF. SCP supports the following formats of the "User-Agent" header: • NFType-NFInstanceID FQDN • NFType-NFInstanceID-FQDN • NFType-FQDN NFInstanceID • NFType-FQDN-NFInstanceID • NFType-NFInstanceID • NFType-FQDN • NFType • NFType-UNIQUEID uniqueID: This parameter is applicable only for NFType-UNIQUEID. If you configure userAgentHeaderFormat as NFType-UNIQUEID, you must configure uniqueID.

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
lci	<pre>"featureSpecificConfig": { "scpLciConveyanceEnable": false, "relayPeerLci": true, "scpLciConveyanceInterval": 5000, "scpLciConveyanceMinLoadChange": 5, "scpLciConveyanceMinLoadThreshold": 30, "scpLciConveyanceMinLoadThreshold": 30, "scpLciConveyanceMinLoadThreshold": 30, "peerLciProcessingMinLoadChange": 5, "unknownPeerLciExpiry": 300 }</pre>	scpLciConveyanceEnable: This parameter enables SCP to add its LCI in request and response. - Default value: false relayPeerLci: This parameter allows SCP to forward the received LCI header from producer NF. - Default value: true scpLciConveyanceInterval: This parameter indicates periodic intervals for reporting SCP LCI to a peer NF. For each interval, SCP's LCI is reported to the peer NF irrespective of any change to SCP LCI. Sending SCP LCI periodically ensures that the peer NF has not missed earlier reported SCP LCI. The SCP LCI load value is measured by SCP as the current load value of SCP if the load is more than configured scpLciConveyanceMinLoadThreshold or 0 if the load is less than scpLciConveyanceMinLoadThreshold. - Default value: 5000 milliseconds - Range: 1000 to 3600000 milliseconds Note: - This LCI conveyance is not limited by scpLciConveyanceMinLoadThreshold or scpLciConveyanceMinLoadChange parameter. - However, if the SCP load value is lesser than scpLciConveyanceMinLoadThreshold, then it reports 0 as a load considering SCP is not loaded. - LCI goes to peer NF if there is a message for that NF. scpLciConveyanceMinLoadChange: This parameter indicates the minimum delta change in load to convey LCI. It is applicable when SCP Load value goes beyond the scpLciConveyanceMinLoadThreshold value. - Default value: 5% - Range: 5% to 25% Example: - If the load changes from 30 to 35 or 35 to 30, LCI is conveyed. - if the load changes from 30 to 32, no LCI is conveyed. scpLciConveyanceMinLoadThreshold: This parameter indicates that SCP considers this parameter as a starting point for updating its original load value to peers. - Default value: 30% - Range: 0% to 60% Note: If the SCP load value is less than the scpLciConveyanceMinLoadThreshold, then

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		SCP reports zero as a LCI load, considering SCP is not loaded. A zero load value is conveyed as part of the <code>scpLciConveyanceInterval</code>. <code>scpLciConveyanceToUnknownPeer</code>: This parameter is boolean that denotes whether SCP should convey its LCI to unknown peers or not. When it is enabled, SCP includes its Load LCI in every message which is going to that unknown peer. - Default value: false Note: If the SCP load value is less than the <code>scpLciConveyanceMinLoadThreshold</code>, then SCP reports zero as a LCI load, considering SCP is not loaded. <code>peerLciProcessingMinLoadChange</code>: This parameter indicates minimum load change threshold in peer NF's load as indicated in LCI or from NRF notification that should trigger LCI processing at SCP for that peer NF. - Default value: 5% - Range: 0% to 25% <code>unknownPeerLciExpiry</code>: This parameter indicates the existence of unknown peer LCI in SCP. The unknown peer represents inter PLMN NFs. When SCP receives LCI load value from inter PLMN NFs, it caches this LCI load value for the period of <code>unknownPeerLciExpiry</code>. - Default value: 300 seconds - Range: 30 to 900 seconds
traffic_feed	NA	The <code>featureSpecificConfig</code> field is not applicable for <code>traffic_feed</code>. You must keep its value empty, for example, <code>featureSpecificConfig: {}</code>

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
egress_host_preference	<pre>"featureSpecificConfig": { "hostPreference": { "request": { "apiRootHdrPresent": "passThrough", "apiRootHdrNotPresent": "ip", "scpGeneratedNrfMsg": "ip" }, "response": { "headers": "followRequest" } }, "fqdnResolution": { "fqdn": "nfProfile", "interPlmnFqdn": "dns" } }</pre>	hostPreference.request.apiRootHdrPresent: This parameter indicates the Host (":authority" header) preference for egress request if "3gpp-Sbi-Target-apiRoot" header is present in the ingress request. • Default value: passThrough • Range: ip, fqdn, or passThrough If set as: — ip: IP is used in host of egress message requests. — fqdn: FQDN is used in host of egress message requests. — passThrough: Uses the same type of host in egress message requests as it is received in ingress message requests. hostPreference.request.apiRootHdrNotPresent: This parameter indicates the host preference (":authority" header) for egress request if "3gpp-Sbi-Target-apiRoot" header is not present in the ingress request. • Default value: ip • Range: ip or fqdn If set as: • ip: IP is used in host of egress message requests. • fqdn: FQDN is used in host of egress message requests. hostPreference.request.scpGeneratedNrfMsg: This parameter indicates the host preference (":authority" header) for SCP generated NRF messages. • Default value: ip • Range: ip or fqdn If set as: • ip: IP is used in host of egress message requests. • fqdn: FQDN is used in host of egress message requests. hostPreference.response.headers: This parameter indicates the host preference for headers in egress message responses. Host present in "location" header or "3gpp-Sbi-Target-apiRoot" header will be updated as per configuration. • Default value: followRequest • Range: followRequest, ip, or fqdn If set as: • ip: IP is used in host of location header or 3gpp-Sbi-Target-apiRoot header for egress message responses.

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		- fqdn: FQDN is used in host of location header or 3gpp-Sbi-Target-apiRoot header for egress message responses. - followRequest: Uses the same host as used for corresponding egress message request. Note: If the location header contains absolute URI, SCP does not update the authority in absolute URI. fqdnResolution.fqdn: This parameter indicates the resolution preference of egress message requests host FQDN if present. - Default value: nfProfile - Range: dns or nfProfile If set as: - dns: DNS resolution is used to resolve fqdn selected for egress message request. - nfProfile: IP Endpoint is used to resolve fqdn selected for egress message request. fqdnResolution.interPlmnFqdn: This parameter indicates the resolution preference of egress message requests inter-plmn FQDN if present. - Default value: dns - Range: dns or nfProfile If set as: - dns: DNS resolution is used to resolve fqdn selected for egress message request. - nfProfile: IP Endpoint is used to resolve fqdn selected for egress message request.
location_hdr_update_for_host_mismatch	NA	It is applicable when the "Location" header in the "201 Created" response has authority (FQDN or IP) different from the producer's authority (FQDN or IP) where the message is sent. The featureSpecificConfig field is not applicable for location_hdr_update_for_host_mismatch Keep this field blank. For example, featureSpecificConfig: {}

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
cca_header_validation	<pre>{ "featureSpecificConfig": { "validations": [{ "type": "subject", "errorProfileName": "ccaVerificationError", "producerNfTypes": ["UDM", "AMF"] }, { "type": "headerPresence", "errorProfileName": "ccaHeaderNotPresentError", "producerNfTypes": ["UDM", "AMF"] }], "tls crt san": { "preferred_validation_order": ["URI-ID-URN", "DNS-ID"], "max_entries_to_process": 30 } } }</pre>	validations: This parameter indicates the list of all the validations that SCP performs on 3gpp-Sbi-Client-Credentials header. - Default value: {"type": "subject", "errorProfileName": "ccaVerificationError", "producerNfTypes": []} - Range: subject, headerPresence type: This parameter indicates the type of validation: - headerPresence: SCP checks the presence of the 3gpp-Sbi-Client-Credentials header in the ingress request. - Validation will pass if the header is present. - Validation will fail if the header is not present. - subject: SCP checks the NF instance ID from the "sub" parameter in the 3gpp-Sbi-Client-Credentials header with the NF instance ID from the list of SANs in the client's TLS certificate. SANs directly have the NF Instance Id or the client's other identity, like the FQDN or IP address, which will be used to get the NF Instance Id. If the 3gpp-Sbi-Client-Credentials header is not present, then this validation will not be performed. - Validation will pass if the NF instance ID from the "sub" parameter matches the NF instance ID from the SAN. - Validation will fail if the NF instance ID from the "sub" parameter doesn't match the NF instance ID from the SAN. - Default value: subject - Range: subject, headerPresence errorProfileName: This parameter is used to generate an error response if the corresponding validation fails. Error profiles can be configured using the REST API: /ocscp/scpc-configuration/{version}/errorProfileConfig. - Default value: ccaVerificationError - Range: NA producerNfTypes: This parameter mentions the name of the producer NF Type. - Default value: null - Range: NA tls crt san.preferred_validation_order: This parameter indicates the order format-wise from which SCP picks SAN from the client's TLS certificate for verification of the "subject" type of validation.

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		• Default value: URI-ID-URN, DNS-ID, IP-ADDRESS, URI-ID-APIROOT • Range: URI-ID-URN, DNS-ID, IP-ADDRESS, URI-ID-APIROOT tls_cert_san.max_entries_to_process: This parameter indicates the maximum number of SANs from the client's TLS certificate that SCP picks for validation. • Default value: 30 • Range: 1-100

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
health_check	<pre> featureSpecificConfig: "v1": scpHealthAPI: successRspType: "200WithEmptyPayload", overload: avgScpLoadThresholdValue: 75, overloadRspProfile: "healthCheckErrorProfile" nextHopSCP: isScpHealthCheckSvcEnabled: false requestTimeout: 1000 pollingInterval: 1000 consecutiveErrorResp: 3 conseutiveSuccessResp: 3 </pre>	This parameter enables the SCP Health Check API feature, which is the default configuration. avgScpLoadThresholdValue: This parameter provides the overall average SCP load threshold value. • Default value: 75% • Range: 75% - 90% successRspType: This parameter indicates successful responses for a healthy SCP. • Default value: 200StatusCodeAndEmptyPayload • Range: 200WithPayload, 200WithEmptyPayload, and 204WithNoContent errorProfileName: This parameter indicates the error profile configuration for the health query response in the exception conditions. • Default value: healthCheckErrorProfile. For more information about this parameter, see Configuring Error Profiles. Sample healthCheckErrorProfile: <pre> { "name": "healthCheckErrorProfile", "errorProfile": { "status": 503, "cause": "NF_CONGESTION", "title": "NF service is overloaded/congested", "detail": "NF service is overloaded/ congested" } </pre> isScpHealthCheckSvcEnabled: This parameter enables or disables the SCP health check API feature in inter-scp scenarios. • Default value: false • Range: true or false pollingInterval: This parameter indicates the duration to control the periodicity of health check requests in inter-scp scenarios. • Default value: 1000ms • Range: 300ms -60000ms requestTimeout: This parameter indicates the timer to monitor the waiting time for health check response in inter-scp scenarios. • Default value: 1000ms • Range: 300ms -60000ms noOfConsecutiveErrorResp: This parameter indicates the total number of consecutive failure responses that leads to failover in inter-scp scenarios. • Default value: 3 • Range: 1 - 20 noOfConsecutiveSuccessResp: This parameter indicates the total number of consecutive successful responses that leads to fallback in inter-scp scenarios. • Default value: 3

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		Range: 1 - 20

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
oauth2_support	<pre>"featureSpecificConfig": { "scpAccessTokenCapability": ": ["INDIRECT_COM_WITH_DELEG_DISC", "INDIRECT_COM_WITHOUT_DELEG_DISC"], "accessTokenConveyance": true, "oauth2AccessTokenValidation": false, "accessTokenValidationTypes": ["TYPE1"], "accessTokenRefreshGuardTime": 60000, "accessTokenValidityGuardTime": 30000, "accessTokenCleanUpPostExpiry": 900000, "accessTokenHistorySize": 10, "accessTokenCacheSize": 50000, "requesterInfo": ["DISCOVERY-HEADERS", "CCA-HEADER", "USER-AGENT-HEADER"], "cacheEnabled": false }</pre>	This parameter enables or disables the OAuth2.0 (Open Authorization) access tokens feature. scpAccessTokenCapability: This parameter indicates Access token support for the listed indirect communication modes at SCP. (ENUM) Possible values: [INDIRECT_COM_WITH_DELEG_DISC, INDIRECT_COM_WITHOUT_DELEG_DISC] - INDIRECT_COM_WITH_DELEG_DISC: SCP initiates access token request toward NRF in delegated discovery service request. - INDIRECT_COM_WITHOUT_DELEG_DISC: SCP is expected to forward the service request with or without access token as per configuration at SCP. SCP is not expected to initiate access token request toward NRF. accessTokenConveyance: This parameter conveys acquired access token in the "3gpp-Sbi-Access-Token" header in service response to consumer NFs. - Default value: true - Range: true or false oauth2AccessTokenValidation: This parameter enables or disables validation of OAuth2 access token from consumer NFs. - Default value: Disabled - Range: Disabled or Enabled accessTokenValidationTypes: This parameter configures the list of required validation types in the network. - Default value: empty as default, only TYPE1 is in scope. accessTokenRefreshGuardTime: This parameter initiates proactive refresh of cached access token when the configured time expires. The proactive refresh occurs if the relevant SBI messages are in exchange. - Default value: 60000ms - Range: 100ms - 300000ms accessTokenValidityGuardTime: This parameter indicates the time before the access token expiry when SCP considers not to use the existing access token and obtains new access token in the service request forwarded to producer NFs. - Default value: 30000ms - Range: 100ms - 300000ms accessTokenCleanUpPostExpiry : This parameter indicates the duration to purge the token from cache. - Default value: 900000ms

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		- Range: 0ms - 3600000ms accessTokenHistorySize: This parameter indicates the number of access tokens signature history to identify whether the access token initiated by SCP or not. - Default value: 10 records - Range: 0 - 20 records accessTokenCacheSize: This parameter indicates the number of access tokens that can be cached in SCP. - Default value: 50000 records - Range: 5000 - 100000 records requesterInfo: This parameter indicates access token requester (consumer NF) Info to generate the access token request. - Prioritized list of default values: 1. DISCOVERY-HEADERS 2. CCA-HEADER 3. USER-AGENT-HEADER cacheEnabled: This parameter enables or disables caching of access tokens. - Default value: true - Range: true or false
nrf_bootstrap_info	<pre>"featureSpecificConfig": "source": "DNS_SRV ", "deRegisterScpDuringMigration": "false"</pre>	source: This field is used to select whether the NRF Configuration Using DNS SRV Resolution feature should be enabled or disabled. SCP will enable the feature if the source is DNS_SRV. - Default value: DNS_SRV deRegisterScpDuringMigration: In the migration from static to DNS SRV task, if static and DNS SRV NRF configurations are the same, then this parameter will be used to deregister SCP with the old or static NRFset. - Default value: false - Range: true or false

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
olchSupportInd	<pre> "featureSpecificConfig": { "olchSupportInd": true, "scpOciConveyanceInterval" : 2000, "scpOciRecoveryValidityPer iod": 3600, "nextHopScpOciEnabled": true, "nextHopScpOciRuleName": NextHopScpOciRuleName", "nextHopSeppOciEnabled": true, "nextHopSeppOciRuleName": NextHopSeppOciRuleName", "scpOciConveyance": { "enable": true, "unknownPeer": { "request": true, "response": true } } } </pre>	If this parameter is set to true, SCP sends the olchSupportInd parameter in SCP NF profile when registering with NRF (NFRegister) or updating NRF (NFUpdate) to indicate that SCP supports Overload Control Information feature based on the 3gpp-Sbi-Oci header. - Default value: true - Range: true or false scpOciConveyanceInterval: This parameter is the interval for reporting SCP OCI to peer NFs. For every interval until the validity period, the last sent OCI is reported to peer NF, irrespective of any change to SCP OCI. Sending SCP OCI periodically ensures that the peer NF has not missed an earlier reported SCP OCI. The same OCI header as sent on the last OCI threshold change or validity period expiry is sent. - Default value: 2000 milliseconds - Range: 2000 to 3600000 milliseconds Note: OCI is sent to peer NFs only if there is a message for that NF. scpOciRecoveryValidityPeriod: This parameter indicates the validity period to send OCI headers to peers when SCP recovers from a congestion state. SCP sends OCI to peers with reduction metric as 0. - Default value: 3600 seconds - Range: 5 to 3600 seconds nextHopScpOciEnabled: If this parameter is set to true, the OCI feature is enabled for SCP scope OCI. - Default value: true - Range: true, false nextHopScpOciRuleName: If nextHopScpOciEnabled is set to true, OCI feature enforcement is done based on ociConfigRule configured with the name provided as value for this parameter. - Default value: NextHopScpOciRuleName - Range: NextHopScpOciRuleName Note: When ociConfigRule is configured for nextHopScpOciRuleName, set relayPeerOci to false and ociEnforcement to true. nextHopSeppOciEnabled: If this parameter is set to true, OCI enforcement is enabled for SEPP scope OCI. - Default value: true - Range: true, false nextHopSeppOciRuleName: If nextHopSeppOciEnabled is set to true, OCI feature enforcement is done based on ociConfigRule configured with the name provided as value for this parameter.

Table 2-3 (Cont.) Mapping of FeatureSpecificConfig per Feature

Feature(featureName)	featureSpecificConfig	Description
		- Default value: NextHopSeppOciRuleName - Range: NextHopSeppOciRuleName Note: When ociConfigRule is configured for nextHopSeppOciRuleName, set relayPeerOci to false and ociEnforcement to true. scpOciConveyance:enable: If this parameter is set to true, SCP starts conveying the 3gpp-Sbi-Oci header based on self-overload information. - Default value: true - Range: true or false scpOciConveyance:unknownPeer:request: If this parameter is set to true, SCP starts conveying self-OCI tagged to requests toward unknown peers. For unknown peers, identification of peer NFs is done based on message request's FQDN. - Default value:false - Range: true or false scpOciConveyance:unknownPeer:response: If this parameter is set to true, SCP starts conveying self-OCI tagged to responses toward unknown peers. - Default value:false - Range: true or false
ignore_unknown_nfservice	NA	The featureSpecificConfig field is not applicable for ignore_unknown_nfservice. You must keep its value empty, for example, featureSpecificConfig: {}
enhanced_error_rsp	<pre>"featureSpecificConfig": { "problemDetailsEnhancement": { "errorDetailMaxSize": 2100 } }</pre>	This parameter adds routing attempt information to ProblemDetails when SCP generates error responses. errorDetailMaxSize: This parameter manages the maximum length limit of the compiled error string in the detail parameter of problemDetails. SCP truncates the error string from end if the compiled string is greater than the maximum limit. - Default value: 2100 Bytes - Range: 1000 to 3100 Bytes

Response Body

The following table describes response body data models that varies based on the REST operation status.

Table 2-4 Response Body Data Type

Data Type	P	Cardinality	Response Codes	Description
array(SCPFeaturesWrapper)	M	1	200 OK	Indicates the list of SCP features (SCPFeaturesWrapper) matching criteria.
ProblemDetails	M	1	404 NOT FOUND	Returns when the data is not found for given query parameters.

JSON Format

```
[
{
  "featureName": "string",
  "enabled": false,
  "featureSpecificConfig": {

  }
}, {
  ....
  ...
}
]
```

Resource Definition**GET REST API**

This resource fetches the SCP feature details (SCPFeaturesWrapper) based on the query parameters.

If no query parameter is provided, all the SCP feature detail are returned.

Resource URI: /ocscp/scpc-configuration/v1/scp-features

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-5 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
featureName	String	O	Specifies the identity of featureName for which SCP features are fetched.

Note

featureName is a valid combination of query parameter or path variable.

Table 2-6 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
array(SCPFeaturesWrapper)	M	1	200 OK	Indicates the list of SCP features or specific record based on query parameters.
ProblemDetails	M	1	404 NOT FOUND	Returns when the data is not found for given query parameters.

Example

Successful response 1

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/scp-features" -H "accept: application/json"
```

```
[
  {
    "featureName": "interplmn_routing",
    "enabled": false,
    "featureSpecificConfig": {
    }
  }
]
```

Successful response 2

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/scp-features/interplmn_routing" -H "accept: application/json"
```

```
{
  "featureName": "interplmn_routing",
  "enabled": false,
  "featureSpecificConfig": {
  }
}
```

Successful response 3

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/scp-features?featureName=interplmn_routing" -H "accept: application/json"
```

```
{
  "featureName": "interplmn_routing",
  "enabled": false,
  "featureSpecificConfig": {
  }
}
```

Successful response 4

```
curl -X GET "http://10.75.212.104:32287/ocscp/scpc-configuration/v1/scp-features/egress_host_preference"-H "accept: application/json"
```

Code: 200

```
{
  "featureName": "egress_host_preference",
  "enabled": false,
  "featureSpecificConfig": {
    "fqdnResolution": {
      "fqdn": "nfProfile",
      "interPlmnFqdn": "dns"
    },
    "hostPreference": {
      "request": {
        "apiRootHdrPresent": "passThrough",
        "scpGeneratedNrFMsg": "ip",
        "apiRootHdrNotPresent": "ip"
      },
      "response": {
        "headers": "followRequest"
      }
    }
  }
}
```

Failure case 1

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/scp-features?featureName=routing_options" -H "accept: application/json"
```

Response Body:

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "SCP Features configuration data not found against given query parameter(s), Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/scp-features?"
}
```

```
featureName=routing_options",
  "cause": "DATA_NOT_FOUND"
}
```

Failure case 2

```
curl -X GET "http://10.75.212.104:32287/ocscp/scpc-configuration/v1/scp-features/egress_host_preferenceheader1" -H "accept: application/json"
```

Response Body:

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "SCP Features configuration data not found against given query parameter(s), Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/scp-features/egress_host_preferenceheader1",
  "cause": "DATA_NOT_FOUND"
}
```

PUT REST API

This resource adds or updates the SCP feature interplmn routing configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/scp-features/{featureName}

Table 2-7 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
SCPFeaturesWrapper	M	1	200 OK	Indicates the SCP feature configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571 section 5.2.4.1.

Example

Successful response 1:

```
$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/scp-features" -H "accept: application/json" -H "Content-Type: application/json" -d '{"featureName":"interplmn_routing","enabled":"false","featureSpecificConfig":{"}}'"
```

```
{
  "featureName": "interplmn_routing",
  "enabled": false,
  "featureSpecificConfig": {
```



```
    }
  }
200 OK
```

Successful response 2:

```
curl -X PUT "http://10.75.212.104:32287/ocscp/scpc-configuration/v1/scp-features/egress_host_preference" -H "accept: */*" -H "Content-Type: application/json" -d '{\
"featureName\":"egress_host_preference",\
"enabled\:false,\
"featureSpecificConfig\":{\
"fqdnResolution\":{\
"fqdn\":"nfProfile",\
"interPlmnFqdn\":"dns"},\
"hostPreference\":{\
"request\":{\
"apiRootHdrPresent\":"passThrough",\
"scpGeneratedNrFMsg\":"ip",\
"apiRootHdrNotPresent\":"ip"},\
"response\":{\
"headers\":"followRequest"}}}}}'
```

```
{
  "featureName": "egress_host_preference",
  "enabled": false,
  "featureSpecificConfig": {
    "fqdnResolution": {
      "fqdn": "nfProfile",
      "interPlmnFqdn": "dns"
    },
    "hostPreference": {
      "request": {
        "apiRootHdrPresent": "passThrough",
        "scpGeneratedNrFMsg": "ip",
        "apiRootHdrNotPresent": "ip"
      },
      "response": {
        "headers": "followRequest"
      }
    }
  }
}
200 OK
```

Failure case:

Note

In case SCP is not configured with local or foreign PLMNs and invalid NF type is configured for this feature, you receive a Bad Request 400 with error message.

```
$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/scp-features" -H "accept: application/json" -H "Content-Type: application/json" -d '{\
"featureName\":"interplmn_routing",
```

```
\\"enabled\\":\\"false\\",\\"featureSpecificConfig\\":\\"{}\\\\"}"
```

Response Body:

```
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Missing mandatory configuration. Atleast one local PLMN (SCP
Profile) and one remote PLMN (SeppConfig) should be configured for enabling
this feature.",
  "instance": "/ocscp/scpc-configuration/v1/scp-features",
  "cause": "MANDATORY_IE_INCORRECT"
}
```

2.2 Configuring Routing Options

Parameters for Configuring Routing Options

The following table describes the parameters for configuring routing options.

Table 2-8 Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
odEnabled	M	Enables or disables the Outlier Detection feature.	false	true, false	Yes	Yes	Yes	Yes
odRuleName	M	Indicates the name of the rule holding the configuration of outlier detection. The outlier detection feature works based on configuration under this rule.	defaultRule	NA	Yes	Yes	Yes	Yes
ociEnabled	M	Enables and disables the Overload Control Information feature.	false	true, false	Yes	Yes	Yes	Yes
ociRuleName	M	Indicates the name of the rule holding the configuration of Overload Control Information. The Overload Control Information feature works based on the configuration under this rule.	defaultOciConfig Rule	NA	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
responseTimeout	M	Indicates the allotted time to respond to a message request. When the response timeout expires, SCP initiates alternate routing to the available alternate NF or pod. Note: Even though SCP supports configuring responseTimeout up to 15 seconds, users must take caution when configuring high response timeout values. A larger number of requests with delayed responses will have a negative impact on the scp-worker's overall performance. Therefore, users should only set larger responseTimeout values, for instance, more than 10 seconds, for those services that really need them. SCP can only support up to 200 queries per second with a response time of more than 10 seconds.	1 second	100-15000 ms The supported values can be in 's' or 'ms'. Where, 's' is seconds and 'ms' is milliseconds.	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
totalTransactionLifetime	M	Indicates the total time allowed to forward a request, including the initial and all subsequent routing attempts. Note: The totalTransactionLifetime value should be greater than the value obtained by multiplying responseTimeout by the total maximum number of attempts (pod level + service level).	6 seconds	100 - 240000 ms	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
Max Routing Attempts	M	Indicates the maximum number of forward routing attempts at a service level. - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both service and pod level, the total transaction lifetime field value is not required. If the Max Routing attempts value is set to greater than 1 for both service and pod level, then the total transaction lifetime field value is considered for rerouting processing. - Rerouting of request messages is always considered as Max Routing attempts value minus one (-1), that is, Rerouting of request messages = (Max Routing	1 for Pod Level. 3 for Service Level	1-5	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
		attempts value) -1 The default routing attempt is 1.						
reRouteConditionList	M	- This parameter lists the HTTP status codes that SCP uses to attempt alternative routing. If the upstream server responds with any of these configured response codes, SCP will try rerouting based on the configured alternate routing mechanism. - In the event of a response timeout, connect failure, refused stream, or GOAWAY frame received on any connection, SCP attempts to reroute the request. These options (events) are not configurable and are supported by SCP.	"reRouteConditionList": [{ "statusCode": "5xx" }, { "statusCode": "429" }, { "statusCode": "307" }, { "statusCode": "308" }]	301, 302, 303, 304, 307, 308, 400, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 425, 426, 428, 429, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 510, 511, 5xx	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
actions	M	Supported actions: - Forwards the ingress service request to selected egress producer NF. - Sends Response with configured result code and message.	Forward	NA	Yes	NA	Yes	Yes
loadBalancingAlgorithm	M	Priority Only: Use priority as the first level criteria. Use capacity as second level criteria.	Priority_only	NA	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
defaultPriority	M	- Priority (relative to other NF Services of the same type) in the range of 0-65535, to be used for NF Service selection; lower values indicate a higher priority. If priority is present in either NF profile or nfServiceList parameters, those profiles or parameters take precedence over this value. - This default priority value is used for NF service instance selection if priority is not published by producer NFs while registration with NRF in NF profile, including both NF profile and nfServiceList parameters.	1	0-65535	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
defaultCapacity	M	- Capacity information in the range of 0-65535, expressed as a weight relative to other NF service instances of the same type; if capacity is also present in either NF profile or nfServiceList parameters, those profiles or parameters take precedence over this value. - This default capacity value shall be used for NF service instance selection if capacity is not published by producer NFs while registration with NRF in NF profile, including both NF profile and nfServiceList parameters.	65535	0-65535	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
reverseProxySupport	M	Enables reverse proxy support for a service. In reverse proxy mode, all the requests have the authority as SCP. SCP forwards those requests to respective Producers after making required authority changes in the requests (both initial and subsequent). Currently, reverse proxy mode is supported only for some interfaces. If the parameter is set to false, then transparent proxy mode is enabled. If the reverseProxySupport parameter is set to true, it supersedes initialServiceRequest.routePolicy even if it is set to 'Forward_Route' and creates rules for initial messages in the Load_balance way.	false	true, false	Yes	No	Yes	No

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
exceptionErrorResponse	M	Resource Exhausted Action: - Action taken when a request cannot be processed due to an internal resource being exhausted - Option: Send Answer with configured HTTP status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Abandon with no Answer	NA	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
exceptionErrorResponse	M	No Producer Response Action - Action taken when the routing of a request is abandoned due to a response timeout. - Option: Send Answer with configured http status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Send Answer with configured http status code (Default 504).	NA	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
exceptionErrorResponse	M	Connection Failure Action: - Action taken when the routing of a request is abandoned when the last egress connection selection fails - Option: Send Answer with configured HTTP status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Send Answer with configured http status code (Default 504).	NA	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
exceptionErrorResponse	M	Host not found Action: - Action taken when the routing of a request is abandoned due to FQDN of the host not being found - Option: Send Answer with configured http status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Send Answer with configured http status code (Default 504).	NA	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
deploymentModel	M	Indicates deployment model of the NF or NF service. - Default, SITE_WIDE is supported for all NF services. - REGIONAL deployment is supported only for CHF NF in addition to SITE_WIDE. - Limitation: PRIMARY_SECONDARY_PAIR deployment is not supported.	SITE_WIDE	NA	Yes	Yes	Yes	No
assignPreferredLocality	M	SCP assigns its own locality as a preferred locality for NF discovery if assignPreferredLocality is enabled and the 3gpp-Sbi-Discovery-preferredlocality header is absent in ingress service requests.	false	true, false	Yes	NA	Yes	No
overridePreferredLocality	M	SCP overrides the 3gpp-Sbi-Discoverypreferred-locality header received in the service request and uses its own locality as preferred-locality for NF discovery if overridePreferredLocality is enabled, and the 3gpp-Sbi-Discoverypreferred-locality header is present in ingress service requests	false	true, false	Yes	NA	Yes	No

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
forward Revised PreferredLocality	M	Controls the forwarding of assigned or overridden values of 3gpp-Sbi-Discovery-preferred-locality headers to the next hop SCP.	false	true, false	Yes	NA	Yes	No
initialServiceRequest	M	Considers routePolicy and reroutePolicy for the initial service request.	NA	NA	Yes	NA	Yes	Yes
subsequentServiceRequest	M	Considers routePolicy and reroutePolicy for subsequent service requests. Note: This parameter is not applicable for notification message	NA	NA	NA	NA	Yes	No
service	M	Name of the NF service.	SCP level config	NA	Yes	Yes	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHop SCP.service.max Routing Attempts	M	Indicates the maximum number of reroute attempt (retries) at service level. - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both service and pod level, the total transaction lifetime field value is not required. If the Max Routing attempts value is set to greater than 1 for both service and pod level, then the total transaction lifetime field value is considered for rerouting processing. - Rerouting of request messages is always considered as Max Routing attempts value minus one (-1), that is, Rerouting of request messages = (Max Routing	2 attempts	1-5	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
		attempts value) -1 The default routing attempt is 1.						

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHop SCP.serviceEndPoint.maxRoutingAttempts	M	Indicates the maximum number of reroute attempts (retries) at NF or pod level. - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both service and pod level, the total transaction lifetime field value is not required. If the Max Routing attempts value is set to greater than 1 for both service and pod level, then the total transaction lifetime field value is considered for rerouting processing. - Rerouting of request messages is always considered as Max Routing attempts value minus one (-1), that is, Rerouting of request messages = (Max Routing	1 attempt	1-5	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
		attempts value) -1 The default routing attempt is 1.						
nextHop SCP.responseTimeout	M	Indicates the allotted time to respond to a message request. When the response timeout expires, SCP performs alternate rerouting to the available alternate NF or pod, or sends an error message.	4 seconds	100-15000 ms	Yes	Yes	No	Yes
nextHop SCP.totalTransactionLifetime	M	Indicates the total time allowed to forward a request to Next Hop SCP. Note: - The total time consumed in processing all retries should not exceed the total transaction lifetime. - totalTransactionLifetime value should be greater than the value obtained by multiplying responseTime out by total maximum number of attempts (pod level + service level).	7 seconds	100 - 240,000 ms	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSCP.exceptions	M	Host not found Action - Action taken when the routing of a request is abandoned due to FQDN of the host not found. - Options: - Abandon with no Answer - Send Answer with configured http status code. Refer to HTTP Status Code and applicability for rerouting.	Send Answer with configured http status code (Default 504).	-	Yes	-	No	Yes
nextHopSCP.loadBasedCongestionControlEnabled	M	Enables and disables Load Based Congestion Control for nextHopSCP.	true	true, false	Yes	No	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSCP.nfServiceLoadBasedCongestionControlCfg	M	Name of the rule holding the configuration of congestion control for nextHopSCP. Based on the configuration under this rule, congestion control works.	defaultRuleForNextHopScp { "ruleName": "defaultRuleForNextHopScp", "congestionControlConfigData": { "v1": { "alternateRoutingOnsetThresholdPercent": 80, "alternateRoutingAbatementThreshold"				No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			<code>shouldPercent": 75,</code> <code>"throttleOnsetThresholdPercent": 90,</code> <code>"throttleAbatementThresholdPercent": 85,</code> <code>"sbimsgPriorityDiscardFrom": 24,</code> <code>"errorProfileConfiguration": {</code> <code>"errorCode</code>					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			"": 503, "errorCause": "NF_CONGESTION" , "errorTitle": "NF service is overloaded / congested" , "errorDescription": "NF service is overloaded / congested" , "retr					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			<pre> yAfter": "5", "redirectUrl": "" } } } </pre>					
nextHopSEPP:totalTransactionLifetime	M	- Time consumed in processing of all retries should not exceed the total transaction life time. - The total time allowed to forward a request, including initial and all subsequent routing attempts Note: totalTransactionLifetime value should be greater than the value obtained by multiplying responseTimeout by total maximum number of attempts (pod level + service level).	7 seconds	100 - 240000	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSEPP.responseTimeout	M	Indicates the allotted time to respond to a message request. When the response timeout expires, SCP performs alternate rerouting to the available alternate NF or pod, or sends an error message.	4 seconds	100-15000 ms	Yes	Yes	No	Yes
nextHopSEPP.service.maxRoutingAttempts	M	- Number of reroute attempt (retries) at NF/Pod level - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both Service and Pod level, the total transaction lifetime field value is not needed and If the Max Routing attempts value (including both service and pod level) is greater than 1, total transaction lifetime value is considered in rerouting processing.	2	1 to 5	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSEPP.serviceEndpoint.maxRoutingAttempts	M	- Number of re-route attempt (retries) at NF/Pod level - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both Service and Pod level, the total transaction lifetime field value is not needed and If the Max Routing attempts value (including both service and pod level) is greater than 1, total transaction lifetime value is considered in rerouting processing.	1	1 to 5	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSEPP.routeConditionList	M	- This parameter lists the HTTP status codes that SCP uses to attempt alternative routing. If the upstream server responds with any of these configured response codes, SCP will try rerouting based on the configured alternate routing mechanism. - In the event of a response timeout, connect failure, refused stream, or GOAWAY frame received on any connection, SCP attempts to reroute the request. These options (events) are not configurable and are supported by SCP.	"reRouteConditionList": [{ "statusCode": "5xx" }, { "statusCode": "429" }, { "statusCode": "307" }, { "statusCode": "308" }]	301, 302, 303, 304, 307, 308, 400, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 425, 426, 428, 429, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 510, 511, 5xx	Yes	Yes	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSEPP.exceptions	M	Host not found Action - Action taken when the routing of a request is abandoned due to FQDN of the host not found. - Options: - Abandon with no Answer - Send Answer with configured http status code. Refer to HTTP Status Code and applicability for rerouting.	Send Answer with configured http status code (Default 504).	Send Answer with configured http status code (Default 503).	Yes	No	No	Yes
nextHopSEPP.loadBasedCongestionControlEnabled	M	Enables and disables Load Based Congestion Control for nextHopSEPP.	true	true, false	Yes	No	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nextHopSEPP.nfServiceLoadBasedCongestionControlCfg	M	Name of the rule holding the configuration of congestion control for nextHopSEPP. Based on the configuration under this rule, congestion control will work.	defaultRuleForNextHopSEPP { "ruleName": "defaultRuleForNextHopSEPP", "congestionControlConfigData": { "v1": { "alternateRoutingOnsetThresholdPercent": 80, "alternateRoutingAbatementThre	-	Yes	-	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			<code>shouldPercent": 75,</code> <code>"throttleOnsetThresholdPercent": 90,</code> <code>"throttleAbatementThresholdPercent": 85,</code> <code>"sbimsgPriorityDiscardFrom": 24,</code> <code>"errorProfileConfiguration": {</code> <code>"errorCode</code>					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			"": 503, "errorCause": "NF_CONGESTION" , "errorTitle": "NF service is overloaded / congested" , "errorDescription": "NF service is overloaded / congested" , "retr					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			<pre>yAfter": "5", "redirectURL": "" } } }</pre>					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
alternateNFGroupRoutingOptions	M	This parameter decides the alternate routing mode, depending on which scp-worker derives the alternate producer NF - Different modes are described below NF_SET: SCP performs alternate routing based on the Model C Indirect 5G SBI Communication format. This is the default mode. DNS_SRV: SCP performs alternate routing based on the DNS SRV query. NF_SET_FOLLOWED_BY_DNSSRV: SCP performs alternate routing based on NF Set and then with DNS SRV. STATIC_CONFIG:	NF_SET	NF_SET DNS_SRV NF_SET_FOLLOWED_BY_DNSSRV STATIC_CONFIG NF_SET_FOLLOWED_BY_STATIC_CONFIG	Yes	No	No	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
		SCP performs alternate routing based on the static configuration. — NF_SET_FOLLOWED_BY_STATIC_CONFIG: SCP performs alternate routing based on NF Set, and then using static configuration.						
cbEnabled	M	Enables and disables circuit breaking.	false	true, false	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
cbRuleName	M	Name of the rule holding the configuration of Circuit Breaking. Based on configuration under this rule, Circuit Breaking works.	defaultRule { "ruleName": "defaultRule", "data": { "v1": { "http2MaxRequests": 1000 } } }	-			Yes	Yes
loadBasedCongestionControlEnabled	M	Enables and disables Load Based Congestion Control	true	true, false	Yes	No	Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
nfServiceLoadBasedCongestionControlCfg	M	Name of the rule holding the configuration of congestion control. Based on the configuration under this rule, congestion control works.	defaultRule { "ruleName": "defaultRule", "congestionControlConfigData": { "v1": { "alternateRoutingOnsetThresholdPercent": 80, "alternateRoutingAbatementThresholdPercent": 75,				Yes	Yes

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			"throttleOnsetThresholdPercent": 90, "throttleAbatementThresholdPercent": 85, "sbimsgPriorityDiscardFrom": 24, "errorProfileConfiguration": { "errorCode": 503,					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			"errorCause": "NF_CONGESTION", "errorTitle": "NF service is overloaded / congested", "errorDescription": "NF service is overloaded / congested", "retryAfter": "5",					

Table 2-8 (Cont.) Parameters for Routing Options

Parameter Name	P	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF	Applicable for R15 Mode	Applicable for R16 Mode
			<pre> "redirectUrl": "" } } } </pre>					

Table 2-9 deploymentCHF

Enumeration value	CHF Deployment
REGIONAL	Regional CHF deployment, that is, CHF's, are deployed in primary region and secondary regions. A region may consist of one or more locality.
SITE_WIDE	Site specific CHF deployment, that is, CHF instances, are deployed as per SCP's site deployment.
PRIMARY_SECONDARY_PAIR	Primary and Secondary CHF deployment using ChfServiceInfo. Primary and Secondary CHF instance information is published in ChfServiceInfo while registering with NRF.

Table 2-10 initialServiceRequest

routePolicy	reroutePolicy
Load_Balance	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite. This enables SCP to perform alternate routing from one service to another. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion (Applicable for Release 15 only) • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup (Applicable for Release 15 only)

Table 2-10 (Cont.) initialServiceRequest

routePolicy	reroutePolicy
Forward_Route	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite. This enables SCP to perform alternate routing from one service to another. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion (Applicable for Release 15 only) • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup (Applicable for Release 15 only)

Table 2-11 subsequentServiceRequest

routePolicy	reroutePolicy
Load_Balance	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite. This enables SCP to perform alternate routing from one service to another. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion (Applicable for Release 15 only) • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup (Applicable for Release 15 only)
Forward_Route	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite. This enables SCP to perform alternate routing from one service to another. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion (Applicable for Release 15 only) • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup (Applicable for Release 15 only)

Configuring Operations for Routing Options

You can configure routing options by using these operations: LIST, GET, PUT, and PATCH.

The following section provides sample details of the operations to configure routing options.

Request_Type: GET

URI: /ocscp/scpc-configuration/v1/routingoptions/

Port: 8081

Message

```
curl --header 'Content-type: application/json' --header 'accept: application/
json' --request GET http://<SCP configuration FQDN>:8081/ocscp/scpc-
configuration/v1/routingoptions/<serviceName>
```

```
"odEnabled": false,
  "cbEnabled": false,
  "ociEnabled": false,
  "odRuleName": "defaultRule",
  "cbRuleName": "defaultRule",
  "ociRuleName": "defaultOciConfigRule",
  "pod": {
    "maxRoutingAttempts": 1,
    "alternateRouting": true,
    "loadBalancingAlgorithm": "Round_Robin"
  },
  "alternateNFGroupRoutingOptions": {
    "mode": "NF_SET"
  },
  "srv": {
    "name": "nudm-uecm",
    "maxRoutingAttempts": 3,
    "actions": "Forward",
    "loadBalancingAlgorithm": "Priority_only",
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRule",
    "defaultPriority": 1,
    "defaultCapacity": 65535,
    "reverseProxySupport": true,
    "initialServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    },
    "subsequentServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    }
  },
  "totalTransactionLifetime": "6s",
  "reRouteConditionList": [
    {
      "statusCode": "307"
    },
    {
      "statusCode": "308"
    },
    {
      "statusCode": "429"
    },
    {
      "statusCode": "5xx"
    }
  ],
  "responseTimeout": "1s",
```

```

"exceptionErrorResponses": [
  {
    "name": "Resource_Exhausted",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "No_Response",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "Connect_Failure",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "No_Host",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "Db_LookUp_Error",
    "action": "Send_Answer",
    "error_code": 500,
    "error_response": "Session/Subscriber binding not found/look-up failure
at OCSCP-SDS Service"
  }
],
"deploymentModel": "SITE_WIDE",
"name": "nudm-uecm",
"assignPreferredLocality": false,
"overridePreferredLocality": false,
"forwardRevisedPreferredLocality": false,
"nextHopSEPP": {
  "totalTransactionLifetime": "7s",
  "responseTimeout": "4s",
  "service": {
    "maxRoutingAttempts": 2
  },
  "serviceEndpoint": {
    "maxRoutingAttempts": 1
  },
  "loadBasedCongestionControlEnabled": true,
  "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
  "reRouteConditionList": [
    {
      "statusCode": "307"
    },
    {
      "statusCode": "308"
    }
  ],

```

```

        {
          "statusCode": "429"
        },
        {
          "statusCode": "5xx"
        }
      ],
      "exceptions": [
        {
          "name": "No_Host",
          "action": "Send_Answer",
          "error_code": 504,
          "error_response": "Gateway Timeout"
        }
      ]
    },
    "nextHopScp": {
      "totalTransactionLifetime": "7s",
      "responseTimeout": "4s",
      "service": {
        "maxRoutingAttempts": 2
      },
      "serviceEndpoint": {
        "maxRoutingAttempts": 1
      },
      "loadBasedCongestionControlEnabled": true,
      "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
      "exceptions": [
        {
          "name": "No_Host",
          "action": "Send_Answer",
          "error_code": 504,
          "error_response": "Gateway Timeout"
        }
      ]
    }
  }
}

```

Request_Type: PUT**URI:** /ocscp/scpc-configuration/v1/routingoptions**Port:** 8081**Message**

```

curl -X PUT http://<SCP configuration FQDN>:8081/ocscp/scpc-configuration/v1/
routingoptions/namf-comm/ \
-H 'Content-Type: application/json' \
-d

```

```

'{
  "odEnabled": false,
  "cbEnabled": false,
  "ociEnabled": false,

```

```

"odRuleName": "defaultRule",
"cbRuleName": "defaultRule",
"ociRuleName": "defaultOciConfigRule",
"pod": {
  "maxRoutingAttempts": 1,
  "alternateRouting": true,
  "loadBalancingAlgorithm": "Round_Robin"
},
"alternateNFGroupRoutingOptions": {
  "mode": "NF_SET"
},
"srv": {
  "name": "namf-comm",
  "maxRoutingAttempts": 3,
  "actions": "Forward",
  "loadBalancingAlgorithm": "Priority_only",
  "loadBasedCongestionControlEnabled": true,
  "nfServiceLoadBasedCongestionControlCfg": "defaultRule",
  "defaultPriority": 1,
  "defaultCapacity": 65535,
  "reverseProxySupport": true,
  "initialServiceRequest": {
    "routePolicy": "Forward_Route",
    "reroutePolicy": "RerouteWithinSite"
  },
  "subsequentServiceRequest": {
    "routePolicy": "Forward_Route",
    "reroutePolicy": "RerouteWithinSite"
  }
},
"totalTransactionLifetime": "6s",
"reRouteConditionList": [
  {
    "statusCode": "307"
  },
  {
    "statusCode": "308"
  },
  {
    "statusCode": "429"
  },
  {
    "statusCode": "5xx"
  }
],
"responseTimeout": "1s",
"exceptionErrorResponses": [
  {
    "name": "Resource_Exhausted",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "No_Response",
    "action": "Send_Answer",

```

```

        "error_code": 504,
        "error_response": "Gateway Timeout"
    },
    {
        "name": "Connect_Failure",
        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
    },
    {
        "name": "No_Host",
        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
    },
    {
        "name": "Db_LookUp_Error",
        "action": "Send_Answer",
        "error_code": 500,
        "error_response": "Session/Subscriber binding not found/look-up failure
at OCSCP-SDS Service"
    }
],
"deploymentModel": "SITE_WIDE",
"name": "namf-comm",
"assignPreferredLocality": false,
"overridePreferredLocality": false,
"forwardRevisedPreferredLocality": false,
"nextHopSEPP": {
    "totalTransactionLifetime": "7s",
    "responseTimeout": "4s",
    "service": {
        "maxRoutingAttempts": 2
    },
    "serviceEndpoint": {
        "maxRoutingAttempts": 1
    },
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
    "reRouteConditionList": [
        {
            "statusCode": "307"
        },
        {
            "statusCode": "308"
        },
        {
            "statusCode": "429"
        },
        {
            "statusCode": "5xx"
        }
    ],
    "exceptions": [
        {
            "name": "No_Host",

```

```

        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
    }
]
},
"nextHopScp": {
    "totalTransactionLifetime": "7s",
    "responseTimeout": "4s",
    "service": {
        "maxRoutingAttempts": 2
    },
    "serviceEndpoint": {
        "maxRoutingAttempts": 1
    },
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
    "exceptions": [
        {
            "name": "No_Host",
            "action": "Send_Answer",
            "error_code": 504,
            "error_response": "Gateway Timeout"
        }
    ]
}
}
}'

```

Request_Type: PUT**URI:** /ocscp/scpc-configuration/v1/routingoptions/**Port:** 8081**Message**

```

curl -X 'PUT' \
'http://<SCP configuration FQDN>:30446/ocscp/scpc-configuration/v1/
routingoptions/nnef-eventexposure' \
-H 'accept: application/json' \
-H 'Content-Type: application/json' \
-d

```

```

'{
  "odEnabled": false,
  "cbEnabled": false,
  "ociEnabled": false,
  "odRuleName": "defaultRule",
  "cbRuleName": "defaultRule",
  "ociRuleName": "defaultOciConfigRule",
  "pod": {
    "maxRoutingAttempts": 1,
    "alternateRouting": true,
    "loadBalancingAlgorithm": "Round_Robin"
  },

```

```

"alternateNFGroupRoutingOptions": {
  "mode": "NF_SET"
},
"srv": {
  "name": "namf-comm",
  "maxRoutingAttempts": 3,
  "actions": "Forward",
  "loadBalancingAlgorithm": "Priority_only",
  "loadBasedCongestionControlEnabled": true,
  "nfServiceLoadBasedCongestionControlCfg": "defaultRule",
  "defaultPriority": 1,
  "defaultCapacity": 65535,
  "reverseProxySupport": true,
  "initialServiceRequest": {
    "routePolicy": "Forward_Route",
    "reroutePolicy": "RerouteWithinSite"
  },
  "subsequentServiceRequest": {
    "routePolicy": "Forward_Route",
    "reroutePolicy": "RerouteWithinSite"
  }
},
"totalTransactionLifetime": "6s",
"reRouteConditionList": [
  {
    "statusCode": "307"
  },
  {
    "statusCode": "308"
  },
  {
    "statusCode": "429"
  },
  {
    "statusCode": "5xx"
  }
],
"responseTimeout": "1s",
"exceptionErrorResponses": [
  {
    "name": "Resource_Exhausted",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "No_Response",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "Connect_Failure",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  }
]

```



```

    },
    {
      "name": "No_Host",
      "action": "Send_Answer",
      "error_code": 504,
      "error_response": "Gateway Timeout"
    },
    {
      "name": "Db_LookUp_Error",
      "action": "Send_Answer",
      "error_code": 500,
      "error_response": "Session/Subscriber binding not found/look-up failure
at OCSCP-SDS Service"
    }
  ],
  "deploymentModel": "SITE_WIDE",
  "name": "namf-comm",
  "assignPreferredLocality": false,
  "overridePreferredLocality": false,
  "forwardRevisedPreferredLocality": false,
  "nextHopSEPP": {
    "totalTransactionLifetime": "7s",
    "responseTimeout": "4s",
    "service": {
      "maxRoutingAttempts": 2
    },
    "serviceEndpoint": {
      "maxRoutingAttempts": 1
    },
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
    "reRouteConditionList": [
      {
        "statusCode": "307"
      },
      {
        "statusCode": "308"
      },
      {
        "statusCode": "429"
      },
      {
        "statusCode": "5xx"
      }
    ],
    "exceptions": [
      {
        "name": "No_Host",
        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
      }
    ]
  },
  "nextHopScp": {
    "totalTransactionLifetime": "7s",

```

```

    "responseTimeout": "4s",
    "service": {
      "maxRoutingAttempts": 2
    },
    "serviceEndpoint": {
      "maxRoutingAttempts": 1
    },
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
    "exceptions": [
      {
        "name": "No_Host",
        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
      }
    ]
  }
}'

```

Request_Type: PATCH**URI:** /ocscp/scpc-configuration/v1/routingoptions/**Port:** 8081**Message**

```

curl -X PATCH http://<SCP configuration FQDN/External IP>:8081/ocscp/scpc-
configuration/v1/routingoptions/<service name> \
-H 'Content-Type: application/merge-patch+json' \
-d '{
  "srv": {
    "name": "nudm-uecm",
    "reverseProxySupport": true
  },
  "exceptionErrorResponses": [
    {
      "name": "Db_LookUp_Error",
      "action": "Send_Answer",
      "error_code": 500,
      "error_response": "Session/Subscriber binding not found/
look-up failure at OCSCP-SDS Service"
    }
  ]
}'

```

2.3 Configuring Overload Configuration Information

This section provides information about overload control configuration parameters required for sending OCI to peers.

Resources

The following table describes the resource name to retrieve, add, or update overload control configuration data:

Table 2-12 Resources

Resource Name	Resource URI	HTTP Method or Custom Operation	Description
oci-config	/ocscp/scpc-configuration/v1/oci-config	GET	Retrieves OCI config at SCP.
oci-config	/ocscp/scpc-configuration/v1/oci-config	PUT	Updates OCI config parameters.
oci-config	/ocscp/scpc-configuration/v1/oci-config	DELETE	Removes OCI config rule.

Resource Definition

GET

This resource fetches the OCI Config details (OCIConfigWrapper) based on the query parameters.

If no query parameter is provided, all the SCP feature details are returned.

Resource URI: /ocscp/scpc-configuration/v1/oci-config

Response Body

Response body data model varies based on the REST operation status.

Table 2-13 Response Body Parameters

Data Type	P	Cardinality	Response Codes	Description
OCIConfigWrapper	M	1	200 OK	Indicates the list of OCI Config (OCIConfigWrapper) matching criteria.
ProblemDetails	M	1	404 NOT FOUND	Returns when data is not found for given query parameters.

Example of a successful response:

```
curl -X GET "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/oci-config" -H "accept: application/json"
```

```

Code: 200
{
  [
    {
      "ociConfigRule": "defaultOciConfigRule",
      "data":
      {
        "relayPeerOci": false,
        "ociEnforcement": true,

```

```

        "ociEnforcementAction": "REROUTE",
        "ociSendErrorProfile": "defaultErrorProfile",
        "interPlmnOciEnforcement": false,
        "ociTrafficRecoveryPolicy":
        {
            "recoveryPolicy": "INCREMENTAL",
            "stepInPercentage": 10,
            "stepDurationInMs": 100
        },
        "ociEnforcementPolicy":
        {
            "enforcementPolicy": "PERCENTAGE_WITH_PRIORITY",
            "maxSbiMessagePriorityForOciEnforcement": 15
        }
    }
}
]
}

```

Example of a failure response:

```
curl -X GET "http://10.75.214.171:30970/ocscp/scpc-configuration/v2/oci-config" -H "accept: application/json"
```

```

{
    "title": "Not Found",
    "status": "404",
    "detail": "Oci_Config data not found against given query parameter(s). Please refer to the User Guide.",
    "instance": "/ocscp/scpc-configuration/v1/oci-config?ociConfigRule=abc",
    "cause": "DATA_NOT_FOUND"
}

```

PUT

This resource updates the OCI config using the request body.

Resource URI: ocscp/scpc-configuration/v1/oci-config

Table 2-14 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinalit y	Response codes	Description
OCIConfigWrapp er	M	1	200 OK	Indicates the list of OCI Config (OCIConfigWrapper) matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns error with problem details structure as defined in 3GPP TS 29.571 Section 5.2.4.1.

Example of a successful response:

```
curl -X PUT "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/oci-
config" -H "accept: application/json"
```

Code: 200

```
{
  [
    {
      "ociConfigRule": "defaultOciConfigRule",
      "data": {
        "relayPeerOci": false,
        "ociEnforcement": true,
        "ociEnforcementAction": "REROUTE",
        "ociSendErrorProfile": "defaultErrorProfile",
        "interPlmnOciEnforcement": false,
        "ociTrafficRecoveryPolicy": {
          "recoveryPolicy": "INCREMENTAL",
          "stepInPercentage": 10,
          "stepDurationInMs": 100
        },
        "ociEnforcementPolicy": {
          "enforcementPolicy": "PERCENTAGE_WITH_PRIORITY",
          "maxSbiMessagePriorityForOciEnforcement": 15
        }
      }
    }
  ]
}
```

DELETE

This resource deletes the OCI config using the request body.

Resource URI: ocscp/scpc-configuration/v1/oci-config

Table 2-15 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinalit y	Response Codes	Description
OCIConfigWrapp er	M	1	200 OK	Indicates the list of OCI Config (OCIConfigWrapper) matching criteria.
ProblemDetails	M	1	403 Forbidden	Returns when data is not found for given query parameters.

Example of a successful response:

Request:

```
curl -X 'DELETE'\ 'http://10.75.225.82:30636/ocscp/scpc-configuration/v1/oci-
config?ociConfigRule=defaultOciConfigRule'\ -H 'accept: application/json'
```

Response:

```
{
  "title": "Forbidden",
  "status": "403",
  "detail": "Given oci config rule is used in routing options hence cannot
be deleted",
  "instance": "/ocscp/scpc-configuration/v1/oci-config?
ociConfigRule=defaultOciConfigRule",
  "cause": "OPERATION_NOT_ALLOWED"
}
```

Data Model

Table 2-16 OCConfigWrapper

Field Name	Data Type	Default Value	Description
relayPeerOci	Boolean	false	If this parameter is set to true, SCP forwards the OCI header received from downstream peer in the ingress messages to upstream peers with the egress messages. - Default value: false - Range: true, false
ociEnforcement	Boolean	true	Enables or disables overload corrective action on the OCI information received from peer. Overload corrective actions can send error responses or reroute based on ociEnforcementAction. - Default value: true - Range: true, false
ociEnforcementAction	Enum	REROUTE	Decides OCI enforcement action, such as send error or reroute. SENDERROR: SCP immediately sends error responses without trying for alternate peers. REROUTE: SCP attempts to reroute to available alternate peers. If it is not able to reroute, SCP sends error responses back. - Default value: REROUTE - Range: SENDERROR and REROUTE
OciSendErrorProfile	String	defaultErrorProfile	In reference to the error response profile, SCP sends error responses because of overload correction action based on OCI. Default value: defaultErrorProfile
interPlmnOciEnforcement	Boolean	false	Enables or disables OCI enforcement toward remote PLMN peers. - Default value: false - Range: true, false

Table 2-17 ociTrafficRecoveryPolicy

Field Name	Data Type	Default Value	Description
recoveryPolicy	Enum	INCREMENTAL	Decides the traffic recovery policy after OCI enforcement action. INCREMENTAL: Increments traffic in steps to 100% based on "stepInPercentage" and "stepDurationInMs" parameters. IMMEDIATE: Increments traffic to 100% immediately. - Default value: INCREMENTAL - Range: INCREMENTAL, IMMEDIATE
stepInPercentage	Integer	10	Defines the size of a step in percentage of reduced traffic when the INCREMENTAL policy is configured. - Default value: 10 - Range: 5 - 15
stepDurationInMs	Integer	100	Defines the duration of a step when the INCREMENTAL policy is configured. Traffic is incremented after this duration for every step during traffic recovery after OCI enforcement action. - Default value: 100 - Range: 50 - 10000

Table 2-18 ociEnforcementPolicy

Field Name	Data Type	Default Value	Description
enforcementPolicy	Enum	PERCENTAGE_WITHPRIORITY	Decides the traffic recovery policy toward a peer after OCI enforcement action. PERCENTAGE_WITH_PRIORITY: Enforces OCI action on percentage of messages as received in reduction metric if priority of message is greater than "maxSbiMessagePriorityForOciEnforcement". PERCENTAGE_ONLY: Enforces OCI action on percentage of messages as received in the reduction metric. - Default value: PERCENTAGE_WITH_PRIORITY - Range: PERCENTAGE_WITH_PRIORITY, PERCENTAGE_ONLY
maxSbiMessagePriorityForOciEnforcement	Integer	15	Defines maximum priority value below which OCI enforcement action will not be applied. - Default value: 15 - Range: 0 - 31

JSON Format**Current JSON Format:**

```
[
  {
    "ociConfigRule": "defaultOciConfigRule",
    "data": {
      "relayPeerOci": false,
      "ociEnforcement": true,
      "ociEnforcementAction": "REROUTE",
      "ociSendErrorProfile": "defaultErrorProfile",
```

```
        "interPlmnOciEnforcement": false,
        "ociTrafficRecoveryPolicy":
        {
            "recoveryPolicy": "INCREMENTAL",
            "stepInPercentage": 10,
            "stepDurationInMs": 100
        },
        "ociEnforcementPolicy":
        {
            "enforcementPolicy": "PERCENTAGE_WITH_PRIORITY",
            "maxSbiMessagePriorityForOciEnforcement": 15
        }
    }
}
```

Error Profile:

```
{
    "name": "ociErrorProfile",
    "errorProfile":
    {
        "status": 500,
        "cause": "NF_SERVICE_FAILOVER",
        "customCause": null,
        "title": "INTERNAL SERVER ERROR",
        "detail": "SCP is unable to route because peer NF overload as per
reported OCI",
        "retryAfter": 0,
        "redirectURL": null
    }
}
```

2.4 Configuring Overload Configuration Information Threshold

This section provides information about overload control configurations required for the `OciThresholdConfig` threshold levels to generate self-Overload Control Information (OCI) by SCP.

Resources

The following table describes the resource name to retrieve, add, or update overload control configuration data:

Table 2-19 Resources

Resource Name	Resource URI	HTTP Method or Custom Operation	Description
oci-threshold-config	/ocscp/scpc-configuration/v1/scp-worker/oci-threshold-config	GET	Retrieves all SCP OCI threshold config data configured at SCP.

Table 2-19 (Cont.) Resources

Resource Name	Resource URI	HTTP Method or Custom Operation	Description
oci-threshold-config	/ocscp/scpc-configuration/v1/scp-worker/oci-threshold-config	GET	Retrieves an SCP OCI threshold config data configured based on the threshold level at SCP when the threshold level is provided as query parameters. However, this query parameter is optional. If it is absent, then it retrieves all SCP OCI threshold config data configured at SCP.
oci-threshold-config	/ocscp/scpc-configuration/v1/scp-worker/oci-threshold-config	PUT	Adds or updates SCP OCI threshold config data at SCP.

Resource Definition**GET REST API**

This resource fetches the SCP OCI threshold config data based on the query parameters.

If no query parameter is provided, all the SCP OCI threshold config data is returned.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/oci-threshold-config

Table 2-20 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the names of supported threshold levels such as WARN, MINOR, MAJOR, and CRITICAL.

PUT REST API

This resource adds or updates the SCP OCI threshold config configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/oci-threshold-config

Table 2-21 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
OciThresholdConfigWrapper	M	1	200 OK	Indicates the names of supported threshold levels such as WARN, MINOR, MAJOR, and CRITICAL.
ProblemDetails	M	1	400 BAD REQUEST	Returns error with problem details structure as defined in 3GPP TS 29.571 Section 5.2.4.1.

Table 2-22 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
thresholdLevel	String	M	1	Indicates all the custom threshold levels apart from WARN, MINOR, MAJOR, and CRITICAL.

Note

- A valid combination of query parameters is provided as follows:
 - thresholdLevel
- Only custom threshold levels can be removed. The default levels such as WARN, MINOR, MAJOR, or CRITICAL, cannot be removed.

Table 2-23 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Codes	Description
None		1	200 OK	In successful cases, only response code is returned.
ProblemDetails	M	1	404 NOT FOUND	When no matching entry is found.

Data Model

The following table describes the field names of the OciThresholdConfigWrapper data type:

Table 2-24 OciThresholdConfigWrapper

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the supported threshold levels such as WARN, MINOR, MAJOR, and CRITICAL.
OciThresholdConfig	Object	M	Indicates the OciThresholdConfig data.

Table 2-25 OciThresholdConfig

Field Name	Data Type	P	Range	Description
generateOciHeader	Boolean	M	true, false	Controls the generation of self-OCI, which is created by SCP, for different threshold levels. If this parameter is set to true. The OCI header for self-overload is added to HTTP messages on load update for this OCI level.
onSetThreshold	Integer	M	2-100	Indicates the onset overload threshold value based on the CPU usage.
abatementThreshold	Integer	M	1-99	Indicates the abatement overload threshold value based on the CPU usage.

Table 2-25 (Cont.) OciThresholdConfig

Field Name	Data Type	P	Range	Description
overloadReductionMetric	Integer	M	0-100%	Indicates the value of the Overload-Reduction-Metric attribute in the 3gpp-Sbi-Oci header that is configured at each overload level, for example, the percentage (%) of traffic that the consumer NF must reduce toward SCP.
periodOfValidity	Integer	M	5 - 3600 seconds	Indicates the value of the Period-of-Validity attribute in the 3gpp-Sbi-Oci header that is configured at each overload level.
abatementTimeInMilliseconds	Integer	M	50 ms to 5000 ms	Indicates the abatement time for overload level change.

The following table provides the default values of the OciThresholdConfig parameter:

Table 2-26 OciThresholdConfig

thresholdLevel	onsetThreshold	abatementThreshold	overloadReductionMetric	periodOfValidity	abatementTime
WARN	68	65	10	5 seconds	200 ms
MINOR	75	70	20	5 seconds	200 ms
MAJOR	80	78	30	5 seconds	200 ms
CRITICAL	86	82	40	5 seconds	200 ms

JSON format for SCP OCI threshold config

```
[
  {
    "thresholdLevel": "CRITICAL",
    "data": {
      "onSetThreshold": 86,
      "abatementThreshold": 82,
      "abatementTimeInMilliseconds": 200,
      "generateOciHeader": false,
      "overloadReductionMetric": 40,
      "periodOfValidity": 5
    }
  },
  {
    "thresholdLevel": "MAJOR",
    "data": {
      "onSetThreshold": 80,
      "abatementThreshold": 78,
      "abatementTimeInMilliseconds": 200,
      "generateOciHeader": false,
      "overloadReductionMetric": 30,
      "periodOfValidity": 5
    }
  },
]
```

```

    {
      "thresholdLevel": "MINOR",
      "data":
      {
        "onSetThreshold": 75,
        "abatementThreshold": 70,
        "abatementTimeInMilliseconds": 200,
        "generateOciHeader": false,
        "overloadReductionMetric": 20,
        "periodOfValidity": 5
      }
    },
    {
      "thresholdLevel": "WARN",
      "data":
      {
        "onSetThreshold": 68,
        "abatementThreshold": 65,
        "abatementTimeInMilliseconds": 200,
        "generateOciHeader": false,
        "overloadReductionMetric": 10,
        "periodOfValidity": 5
      }
    }
  ]

```

2.5 Routing Options Configurations

This REST API is used to configure routing options at the NFType, NFServiceName, and message type levels. The API takes input as NFType, NFServiceName, and so on.

The user can specify only the granularity levels using this API; the actual routing options are configured in another table named Routing Config Set. For more information, see [Routing Config Set](#). The name of the routing option is provided in the Routing Options Configurations API as a value for the routingConfigSetName parameter.

Resources

The following table describes the resource name to retrieve, add, update, and remove routing option configurations based on the query parameters.

Resource URI : `http://<authority>:<port>/ocscp/scpc-configuration/{version}/routing-options-config/{routingOptionsConfigName}`

Authority: loadbalancer or fqdn

Port: nodeport(lp address) or internal port (For fqdn)

loadbalancerip: 10.75.225.111

Table 2-27 Resource Name

Resource Name	Resource URI	HTTP Method	Query Parameter	Description
routing-options-config	ocscp/scpc-configuration/{version}/routing-options-config	GET	• nftype : Get Routing Options config for given nftype. • nfservicename : Get Routing Options config for given nfservicename. • isnotification: Get notification Routing Options Valid Query Parameter combinations: • nftype • nftype + nfservicename • nfType + nfservicename + messagetype • nftype+messagetype • no parameters • nfservicename+messagetype • messagetype • nfservicename	Retrieves routing option name configurations for given filters; if no query parameter is specified, it will return all the data present in the table.
routing-options-config	ocscp/scpc-configuration/{version}/routing-options-config/{routingOptionsConfigName}	GET	-	Retrieve the routing option configuration name for the given name.
routing-options-config	ocscp/scpc-configuration/{version}/routing-options-config/{routingOptionsConfigName}	PUT	-	Updates or creates routing options configurations for parameters.
routing-options-config	ocscp/scpc-configuration/{version}/routing-options-config/{routingOptionsConfigName}	DELETE	-	Deletes routing option configurations for given names.

Data Model**Request Body (PUT)**

The following table describes the field names of the RoutingOptionsConfiguration data type.

Table 2-28 RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
routingOptionsConfigName	String	M	-	-	Unique name to identify the routing options configurations.
routingConfigSetName	String	M	-	-	Name of the routing configuration used to retrieve routing options from another table (Routing Config Set); if a rule with this name is not present in the Routing Config Set table, then the request is rejected.
nftype	NFType: • TS29.510 section Table 6.1.6.3.3-1: Enumeration • custom NF type	C	All	5G_EIR, AMF, AUSF, BSF, CHF, LMF, NEF, NRF, NSSF, NWDAF, PCF, SEPP, SCP, SMF, SMSF, UDM, UDR	The NF type for which routing options are configured.

Table 2-28 (Cont.) RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
nfservicename	Name of the 5G SBI service: 3GPP services defined as per TS29.510 section 6.1.6.3.11 - Enumeration: ServiceName and 5g-sbi-notification for all notification messages - Add custom service name	C	All	n5g-eir-eic, namf-comm, namf-evts, namf-loc, namf-mt, nausf-auth, nausf-sorprotection, nausf-upuprotection, nbsf-management, nchf-converged charging, nchf-spendinglimitcontrol, nchf-spendinglimitcontrol, nlmf-loc, nnef-pfdmanagement, nnef-eventexposure, nnef-afsessionwithqos, nnrf-disc, nnrf-nfm, nssf-nssaiavailability, nnssf-nselection, nnwdaf-analyticsinfo, nnwdaf-eventsubscription, npcfa-policy-control, npcfa-bdtpolicycontrol, npcfa-eventexposure, npcfa-policyauthorization,	The NF service name for which routing options are configured

Table 2-28 (Cont.) RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
				npcf-smpolicycontrol, npcf-ue-policy-control, ampolicy, bdtpolicycontrol, smpolicy, ue-policy, nscp-5g-sbi-proxy, nsmf-event-exposure, nsmf-pdusession, nsmsf-sms, nudm-ee, nudm-pp, nudm-sdm, nudm-ueau, nudm-uecm, nudr-dr, nudr-group-id-map, 5g-sbi-notification, nmediation-http, ocscp-sds	
messagetype	List	C	notification-message	notification-message	The list indicates which message type the configuration is applicable to.

Note

- A defaultRule is created during a fresh deployment or upgrade. This rule cannot be deleted or updated.

```
{
  "routingOptionsConfigName": "defaultConfig",
  "nfType": "ALL",
  "serviceName": "ALL",
  "messageTypeList": ["notification-message"],
  "routingConfigSetName": "defaultRoutingConfigSet",
}
```

- If the above mentioned conditional parameters are not provided in the payload, then the default value is used for them.

Payload example for PUT request

```
{
  "routingOptionsConfigName": "defaultConfig",
  "routingConfigSetName": "amf-notification",
  "nfType": "ALL",
  "nfServiceType": "ALL",
  "messageType": ["notification-message"]
}
```

Data Model**Request Body (GET)**

The following table describes the field names of the RoutingOptionsConfiguration data type.

Table 2-29 RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
routingOptionsConfigName	String	M	-	-	Unique name to identify the routing option configurations.
routingConfigSetName	String	M	-	-	Name of the routing configuration used to retrieve routing options from another table (Routing Config Set); if a rule with this name is not present in the Routing Config Set table, then the request is rejected.

Table 2-29 (Cont.) RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
nftype	NFType: • TS29.510 section Table 6.1.6.3.3-1: Enumeration • custom NF type	M	All	5G_EIR, AMF, AUSF, BSF, CHF, LMF, NEF, NRF, NSSF, NWDAF, PCF, SEPP, SCP, SMF, SMSF, UDM, UDR	The NF type for which routing options are configured

Table 2-29 (Cont.) RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
nfservicename	Name of the 5G SBI service: 3GPP services defined as per TS29.510 section 6.1.6.3.11 - Enumeration: ServiceName and 5g-sbi-notification for all notification messages - Add custom service name	M	All	n5g-eir-eic, namf-comm, namf-evts, namf-loc, namf-mt, nausf-auth, nausf-sorprotection, nausf-upuprotection, nbsf-management, nchf-converged charging, nchf-spendinglimitcontrol, nchf-spendinglimitcontrol, nlmf-loc, nnef-pfdmanagement, nnef-eventexposure, nnef-afsessionwithqos, nnrf-disc, nnrf-nfm, nssf-nssaiavailability, nnssf-nssselection, nnwdaf-analyticsinfo, nnwdaf-eventsubscription, npcfa-policy-control, npcfa-bdtpolicycontrol, npcfa-eventexposure, npcfa-policyauthorization,	The NF service name for which routing options are configured.

Table 2-29 (Cont.) RoutingOptionsConfiguration

Field Name	Data Type	P	Default Values	Allowed Values	Description
				npcf-smpolicycontrol, npcf-ue-policy-control, ampolicy, bdtpolicycontrol, smpolicy, ue-policy, nscp-5g-sbi-proxy, nsmf-event-exposure, nsmf-pdusession, nsmsf-sms, nudm-ee, nudm-pp, nudm-sdm, nudm-ueau, nudm-uecm, nudr-dr, nudr-group-id-map, 5g-sbi-notification, nmediation-http, ocscp-sds	
messagetype	String	M	notification-message	notification message	Indicate whether routing options are for notification messages or not.

Payload example for GET response

```
{
  "routingOptionsConfigName": "defaultConfig",
  "routingConfigSetName": "amf-notification",
  "nftype": "ALL",
  "nfservicetype": "ALL",
  "messagetype": ["notification-message"]
}
```

Resource Definition**GET REST API:**

This resource fetches the routing options configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-options-config?

nftype=<nftype>&&nfservicename=<nfservicename>&&isnotification=<yes/no>

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-30 URI query parameters

Field Name	Data Type	P	Description
nftype	String	O	Parameter to fetch routing option data based on nftype.
nfservicename	String	O	Parameter to fetch routing options based on nfservicenames.
messageType	String	O	Query parameter to fetch routing options for notification messages or non-notification messages.

Note

If no query parameter is specified, the response will contain all the data.

The following table describes the data structures supported by the GET Response Body on this resource.

Table 2-31 Data structures

Data Type	P	Cardinality	Response Codes	Description
RoutingOptionsConfiguration	M	1	200 OK	The routing option configuration for the given parameters.
ProblemDetails	M	1	404	Problem details

Example

Successful response 1

```
curl -v -H "Content-Type: application/json" --request GET http://localhost:8081/ocscp/scpc-configuration/v1/routing-options-config?nftype=ALL&serviceName=ALL
```

HTTP/1.1 200 OK

```
[{"routingOptionsConfigName":"defaultConfig","nftype":"ALL","serviceName":"ALL
```

```
"", "messageTypeList": ["notification-  
message"], "routingConfigSetName": "defaultRoutingConfigSet"]}]
```

Successful response 2

```
curl -v -H "Content-Type: application/json" --request GET 'http://  
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config?nfType=UDM'
```

HTTP/1.1 200 OK

```
[{"routingOptionsConfigName": "newROConfig", "nfType": "UDM", "serviceName": "ALL",  
"messageTypeList": ["notification-  
message"], "routingConfigSetName": "defaultRoutingConfigSet"}]
```

Failure Case 1

```
curl -v -H "Content-Type: application/json" --request GET 'http://  
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config?  
nfType=ALL&serviceName=asa'
```

HTTP/1.1 400 Bad Request

```
{"title": "Bad Request", "status": "400", "detail": "Invalid nfService name  
provided no rule can be created for invalid nfService. Please refer to the  
User Guide.", "instance": "/ocscp/scpc-configuration/v1/routing-options-config?  
nfType=ALL&serviceName=asa", "cause": "INVALID_REQUEST_BODY"}
```

Failure Case 2

```
curl -v -H "Content-Type: application/json" --request GET 'http://  
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config?nfType=Aas'
```

HTTP/1.1 400 Bad Request

```
{"title": "Bad Request", "status": "400", "detail": "Invalid Nftype provided no  
rule can be created for invalid nfType. Please refer to the User  
Guide.", "instance": "/ocscp/scpc-configuration/v1/routing-options-config?  
nfType=Aas", "cause": "INVALID_REQUEST_BODY"}
```

GET REST API:

This resource fetches the routing option configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-options-
config/{routingOptionsConfigName}

Table 2-32 URI query parameters

Field Name	Data Type	P	Description
routingOptionsConfigName	String	O	The name of the routing option for which routingOptionsConfig needs to be retrieved.

The following table describes the data structures supported by the GET Response Body on this resource.

Table 2-33 Data structures

Data Type	P	Cardinality	Response Codes	Description
RoutingOptionsConfigur ation	M	1..N	200 OK	The routing option configuration with all other parameters.

Example of Congestion Control Configuration for GET

Success case

```
curl -v -H "Content-Type: application/json" --request GET http://
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/
defaultConfig
```

HTTP/1.1 200 OK

```
[{"routingOptionsConfigName":"defaultConfig","nfType":"ALL","serviceName":"ALL",
,"messageTypeList":["notification-
message"],"routingConfigSetName":"defaultRoutingConfigSet"}]
```

Failure case

```
curl -v -H "Content-Type: application/json" --request GET http://
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/
defaultConfig1
```

HTTP/1.1 404 Not Found

```
{"title":"Not Found","status":"404","detail":"RoutingOptionsConfig data not
found against given query parameters","instance":"/ocscp/scpc-
configuration/v1/routing-options-config/
defaultConfig1","cause":"DATA_NOT_FOUND"}
```

PUT REST API:

This resource creates or updates the routing option configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-options-
config/{routingOptionsConfigName}

Table 2-34 URI query parameters

Field Name	Data Type	P	Description
routingOptionsConfigName	String	O	The name used to identify the routing options configuration.

Table 2-35 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response codes	Description
RoutingOptionsConfigurationWrapper	M	1	201 Created	Response if a new record in the table is created.
RoutingOptionsConfigurationWrapper	M	1	200 OK	Response if an existing record in the table is updated.
ProblemDetails	M	1	400	Returns problem details.

Example

Successful response

```
curl -v -H "Content-Type: application/json" --request PUT http://localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/defaultConfig -d '{
  "routingOptionsConfigName": "defaultConfig",
  "nfType": "ALL",
  "serviceName": "ALL",
  "messageTypeList": [
    "notification-message"
  ],
  "routingConfigSetName": "defaultRoutingConfigSet"
}'
```

HTTP/1.1 200 OK

```
{"routingOptionsConfigName":"defaultConfig","nfType":"ALL","serviceName":"ALL",
,"messageTypeList":["notification-message"],"routingConfigSetName":"defaultRoutingConfigSet"}
```

Failure Case 1

```
curl -v -H "Content-Type: application/json" --request PUT http://localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/defaultConfig1 -d '{
  "routingOptionsConfigName": "defaultConfig1",
  "nfType": "ALL",
  "serviceName": "ALL",
  "messageTypeList": [
    "notification-message"
  ],
  "routingConfigSetName": "defaultRoutingConfigSet"
}'
```


HTTP/1.1 400 Bad Request

```
{"title":"Bad Request","status":"400","detail":"routingOptionsConfigName
inside RoutingOptionsConfig data does not match with routingOptionsConfigName
passed through API. Please refer to the User Guide.","instance":"/ocscp/scpc-
configuration/v1/routing-options-config/
defaultConfig1","cause":"INVALID_KEY_COMBINATION"}
```

Failure Case 2

```
curl -v -H "Content-Type: application/json" --request PUT http://
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/
defaultConfig1 -d '{
  "routingOptionsConfigName": "defaultConfig2",
  "nfType": "ALLaa",
  "serviceName": "ALL",
  "messageTypeList": [
    "notification-message"
  ],
  "routingConfigSetName": "defaultRoutingConfigSet"
}'
```

HTTP/1.1 400 Bad Request

```
{"title":"Bad Request","status":"400","detail":"Invalid Nftype provided no
rule can be created for invalid nfType. Please refer to the User
Guide.","instance":"/ocscp/scpc-configuration/v1/routing-options-config/
defaultConfig1","cause":"INVALID_REQUEST_BODY"}
```

Failure case 3

```
curl -v -H "Content-Type: application/json" --request PUT http://
localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/
defaultConfig -d '{
  "routingOptionsConfigName": "defaultConfig",
  "nfType": "UDM",
  "serviceName": "ALL",
  "messageTypeList": [
    "notification-message"
  ],
  "routingConfigSetName": "defaultRoutingConfigSet"
}'
```

HTTP/1.1 400 Bad Request

```
{"title":"Bad Request","status":"400","detail":"Cannot update NFType
ServiceName or MessageType of default Configuration present for
RoutingOptionsConfig. Please refer to the User Guide.","instance":"/ocscp/
scpc-configuration/v1/routing-options-config/
defaultConfig","cause":"INVALID_REQUEST_BODY"}
```

DELETE REST API:

This resource deletes the routing options configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-options-config/{routingOptionsConfigName}

Table 2-36 URI query parameters supported by the DELETE method on this resource

Field Name	Data Type	P	Description
routingOptionsConfigName	String	O	The name of the routing options configuration which needs to be deleted.

Table 2-37 Data structures supported by the Delete Response Body on this resource

Data Type	P	Cardinality	Response codes	Description
Default	M	1	200 OK	-
ProblemDetails	M	1	400/404	Problem details.

Example

Successful response

```
curl -v -H "Content-Type: application/json" --request DELETE http://localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/abc HTTP/1.1204No Content
```

Failure case 1

```
curl -v -H "Content-Type: application/json" --request DELETE http://localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/defaultConfig11
```

HTTP/1.1 404 Not Found

```
{"title":"Not Found","status":"404","detail":"RoutingOptionsConfig data not found against given routingOptionsConfig Name","instance":"/ocscp/scpc-configuration/v1/routing-options-config/defaultConfig11","cause":"DATA_NOT_FOUND"}
```

Failure case 2

```
curl -v -H "Content-Type: application/json" --request DELETE http://localhost:8081/ocscp/scpc-configuration/v1/routing-options-config/defaultConfig
```

HTTP/1.1 403 Forbidden

```
{"title":"Forbidden","status":"403","detail":"Default Configuration present for RoutingOptionsConfig cannot be deleted","instance":"/ocscp/scpc-configuration/v1/routing-options-config/defaultConfig","cause":"OPERATION_NOT_ALLOWED"}
```

2.6 Configuring System Options

These options are used to control system behavior per service. The user can configure SystemOptions by using the operations **GET** and **PUT**.

Note

- The default systemOptions are provided during the installation of Service Communication Proxy through Helm.
- The existing OutlierDetection parameters (URI: /ocscp/scpc-configuration/v1/systemoptions) cannot be modified. The same functionality is achieved using the OutlierDetection (URI: /ocscp/scpc-configuration/{version}/outlier-detection) API to the nextHopScpODRule rule assigned to odScpRuleName.

REST Message sample

Request_Type: **GET and PUT**

URI: http://<SCP configuration FQDN/External IP>:8081//ocscp/scpc-configuration/v1/systemoptions

```
{
  "cbEnabled": false,
  "odEnabled": true,
  "odScpRuleName": "nextHopScpODRule",
  "odSeppEnabled": false,
  "odSeppRuleName": "defaultRule",
  "cbScpEnabled": false,
  "cbScpRuleName": "defaultRule",
  "cbSeppEnabled": false,
  "cbSeppRuleName": "defaultRule",
  "forwardNfDiscoveryHeaders": true,
  "trafficPolicy": {
    "connectionPool": {
      "http": {
        "idleTimeout": "600s"
      },
      "https": {
        "idleTimeout": "600s"
      },
      "tcp": {
        "connectTimeout": "250ms",
        "tcpKeepalive": {
          "enable": true,
          "probes": 9,
          "time": "180s",
          "interval": "1s"
        }
      }
    },
    "outlierDetection": {
```

```

        "consecutiveErrors": 100,
        "interval": "86400s",
        "baseEjectionTime": "5s",
        "maxEjectionPercent": 100
    }
},
"ttl": "900s",
"dnsQueryTimeout": "5000ms"
}

```

The following table describes System Options parameters.

Table 2-38 Configuring Parameters for System Options

Parameter	Value	Description
cbEnabled	Boolean	Provides information whether Circuit- Breaking is enabled. The default value is false. For more information, see Circuit Breaking Configurations Note: This attribute change is not allowed due to other attributes controlling circuit breaking in InterPLMN routing and interSCP routing.
odEnabled	Boolean	Provides information whether the Outlier Detection feature is enabled. The default value is false. For more information, see Outlier Detection Configuration
odScpRuleName	String	Indicates the name of the rule holding the configuration of outlier detection for next Hop SCP. The Outlier Detection feature for next Hop SCP works based on configuration under this rule. For more information, see Outlier Detection Configuration
odSeppEnabled	Boolean	Enables or disables the Outlier Detection feature for the next Hop SEPP. For more information, see Outlier Detection Configuration
odSeppRuleName	String	Indicates the name of the rule holding the configuration of outlier detection for next Hop SEPP. The Outlier Detection feature for next Hop SEPP works based on configuration under this rule. For more information, see Outlier Detection Configuration
cbScpEnabled	Boolean	Enables or disables circuit breaking for next Hop SCP. The default value is false. For more information, see Circuit Breaking Configurations
cbScpRuleName	String	Name of the rule holding the configuration of Outlier detection for next Hop SCP. Based on configuration under this Rule, circuit breaking for next Hop SCP will work. The default value is "defaultRule" string. { "ruleName": "defaultRule", "data": { "v1": { "http2MaxRequests": 1000 } } } For more information, see Circuit Breaking Configurations

Table 2-38 (Cont.) Configuring Parameters for System Options

Parameter	Value	Description
cbSeppEnabled	Boolean	Enables or disables circuit breaking for next Hop SEPP. The default value is false. For more information, see Circuit Breaking Configurations
cbSeppRuleName	String	Name of the rule holding the configuration of circuit breaking for next Hop SEPP. Based on configuration under this Rule, circuit breaking for next Hop SEPP will work. The default value is "defaultRule". string. <code>{ "ruleName": "defaultRule", "data": { "v1": { "http2MaxRequests": 1000 } } }</code> For more information, see Circuit Breaking Configurations
forwardNfDiscoveryHeaders	Boolean	Enables or disables the forwarding of discovery headers to next hop SCP. The default value is true.
trafficPolicy.connectionPool.ht tp.idleTimeout	String	The idle timeout for upstream connection pool connections. The idle timeout is defined as the period in which there are no active requests. If not set, there is no idle timeout. When the idle timeout is reached the connection will be closed. Note that request based timeouts mean that HTTPS/2 PINGs will not keep the connection alive. The default value is 3600s.
trafficPolicy.connectionPool.ht tps.idleTimeout	String	The idle timeout for upstream connection pool connections is defined as the period in which there are no active requests. If not set, there is no idle timeout. When the idle timeout is reached, the connection will be closed. Note that request-based timeouts mean that HTTP/2 PINGs will not keep the connection alive. The default value is 3600s.
trafficPolicy.connectionPool.tc p.connectTimeout	String	TCP Connection timeout. Valid time units are ns, us (or μ s), ms, s. For example: 300ms.
trafficPolicy.connectionPool.tc p.tcpKeepalive	TcpKeepalive	Contains the TcpKeepalive information. If set, enable TCP Keepalives to upstream peer. All the parameters of tcpkeepAlive are needed if this information is being configured.
trafficPolicy.connectionPool.tc p.tcpKeepalive.enable	Boolean	Indicate to enable or disable tcp keepalive for upstream connections. The default value is true.
trafficPolicy.connectionPool.tc p.tcpKeepalive.probes	Integer	Maximum number of keepalive probes to send without response before deciding the connection is dead. For example: 9 The default value is 9, minimum value is 1, and maximum value is 16.
trafficPolicy.connectionPool.tc p.tcpKeepalive.time	String	The time duration a connection needs to be idle before keep-alive probes start being sent. Valid time unit is second. For example: 180s The default value is 180 seconds, minimum value is 1 second, and maximum value is 7200 seconds.

Table 2-38 (Cont.) Configuring Parameters for System Options

Parameter	Value	Description
trafficPolicy.connectionPool.tcpKeepalive.interval	String	The time duration between keep-alive probes. Valid time unit is seconds. For example: 1s The default value is 1 second, minimum value is 1 second and maximum value is 120 seconds.
outlierDetection.consecutiveErrors	Integer	Number of errors before a host is ejected from the connection pool. Defaults to 5. When the upstream host is accessed over HTTP, a 502, 503 or 504 return code qualifies as an error. When the upstream host is accessed over an opaque TCP connection, connect timeouts and connection error/failure events qualify as an error. Note: These parameters are not modifiable, and the new OutlierDetection API is used to fill in this information. For more information, see Outlier Detection Configuration
outlierDetection.interval	String	Time interval between ejection sweep analysis. Format: 1h/1m/1s/1ms. Must be >=1ms. Default is 10s. Note: These parameters are not modifiable, and the new OutlierDetection API is used to fill in this information. For more information, see Outlier Detection Configuration
outlierDetection.baseEjectionTime	String	Minimum ejection duration. A host will remain ejected for a period equal to the product of minimum ejection duration and the number of times the host has been ejected. This technique allows the system to automatically increase the ejection period for unhealthy upstream servers. format: 1h/1m/1s/1ms. Must be >=1ms. Default is 30s. Note: These parameters are not modifiable, and the new OutlierDetection API is used to fill in this information. For more information, see Outlier Detection Configuration
outlierDetection.maxEjectionPercent	Integer	Maximum % of hosts in the load balancing pool for the upstream service that can be ejected. Defaults to 10% Note: These parameters are not modifiable, and the new OutlierDetection API is used to fill in this information. For more information, see Outlier Detection Configuration
ttl	String	Indicates the duration in which the DNS record is valid. This is used by DNS SRV feature to refresh the DNS SRV record. The range is between 30 to 86400 seconds.
dnsQueryTimeout	String	The maximum amount of time in milliseconds to wait for a response during a DNS SRV query. The range is between 30 to 86400

2.7 Configuring NRF

This section provides information about configuration of NRF preferred by SCP for access token requests.

Resources

The following table describes the resource name to retrieve and update the NRF data based on the query parameters.

Table 2-39 Resource Name

Resource Name	Resource URI	HTTP Method	Description
nrf-configuration	/ocscp/scpc-configuration/v1/nrf-configuration	GET	Retrieves NRF configurations.
nrf-configuration	/ocscp/scpc-configuration/v1/nrf-configuration	PUT	Updates NRF configurations.

Data Model

Request Body

The following table describes the field names of the NrfConfigurationWrapper data model.

Table 2-40 NrfConfigurationWrapper

Field Name	Data Type	P	Default Value	Supported Values	Description
Service	String	M	"nnrf-oauth2"	"nnrf-oauth2", "nnrf-disc"	Indicates the service name of the preferred NRF configuration.
NrfConfigData	JSON	M	See Table 2-41		Configures preferred NRF. This parameter can be configured as nrfInstanceId or nrfSetId or both.

Table 2-41 NrfConfigData

Field Name	Data Type	P	Default Value	Description
nrfInstanceId	String	C	6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a	Indicates the NF Instance ID of the preferred NRF. Note: When only nrfInstanceId is provided, then SCP forwards the route to the matching NRF with nrfInstanceId.
nrfSetId	Array	C	setnrf1.nrfset.5gc.mnc012.mcc345	The NF Set ID of the preferred NRF. Array(nrfSetId) uses the value from the first index even if multiple values are added. Note: When only nrfSetId is provided, then SCP supports load balancing to the matching NRFs selected by nrfSetId.

①

Note
If both nfinstanceid and nfSetId are provided, SCP forwards the route to the matching NRF with nfinstanceid; if it fails, then SCP does an alternate route to the NRFs selected by nfSetId.

Resource Definition

GET REST API

This resource fetches the NrfConfiguration data based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/nrf-configuration

Table 2-42 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
Service	String	O	Indicates the configuration name. If the parameter is empty, all configurations are returned.

Table 2-43 array(NrfConfigurationWrapper)

Field Name	P	Cardinality	Response Code	Description
array(NrfConfigurationWrapper)	M	1	200 OK	The list of NrfConfigurations available.

Preferred NRF oauth2 GET SCP JSON example:

```
$ curl -X 'GET' 'http://10.75.212.36:30174/ocscp/scpc-configuration/v1/nrf-configuration?service=nnrf-oauth2' -H 'accept: application/json'

{
  "service": "nnrf-oauth2",
  "nrfConfigData": {
    "nrfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a",
    "nrfSetId": [
      "setnrfl1.nrfset.5gc.mnc012.mcc345"
    ]
  }
}
```


Preferred NRF disc GET SCP JSON example:

```
$ curl -X 'GET' 'http://10.75.226.46:32224/ocscp/scpc-configuration/v1/nrf-configuration?service=nnrf-disc' -H 'accept: application/json'
```

```
{
  "service": "nnrf-disc",
  "nrfConfigData": {
    "nrfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a",
    "nrfSetId": [
      "setnrfl1.nrfset.5gc.mnc012.mcc345"
    ]
  }
}
```

PUT REST API

This resource update the NrfConfiguration data using the request body.

Resource URI: /ocscp/scpc-configuration/v1/nrf-configuration

Table 2-44 Data Structures Supported by the PUT Response Body

Name	P	Cardinality	Response Code	Description
NrfConfiguration	M	1	200 OK	Indicates NrfConfiguration to be set.
ProblemDetails	M	1	400 BAD REQUEST	Returns when both the nfinstancid and nrfsetid are not present.

JSON Example of NRF Configuration for PUT

Successful response for NRF oauth2:

```
$ curl -X 'PUT' 'http://10.75.212.36:30898/ocscp/scpc-configuration/v1/nrf-configuration?service=nnrf-oauth2' -H 'accept: */*' -H 'Content-Type: application/json' -d '{"service": "nnrf-oauth2", "nrfConfigData": {"nrfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a", "nrfSetId": ["setnrfl1.nrfset.5gc.mnc012.mcc345"]}}'
```

```
{
  "service": "nnrf-oauth2",
  "nrfConfigData": {
    "nrfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a",
    "nrfSetId": [
      "setnrfl1.nrfset.5gc.mnc012.mcc345"
    ]
  }
}
```

Successful response for NRF disk:

```
$ curl -X 'PUT' 'http://10.75.226.46:32224/ocscp/scpc-configuration/v1/nrf-configuration?service=nnrf-disc' -H 'accept: */*' -H 'Content-Type: application/json' -d
```

```
{
  "service": "nnrf-disc",
  "nrfConfigData": {
    "nrfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a",
    "nrfSetId": [
      "setnrf11.nrfset.5gc.mnc012.mcc345"
    ]
  }
}
```

Failure response:

```
$ curl -X 'PUT' 'http://10.75.212.36:30898/ocscp/scpc-configuration/v1/nrf-configuration?service=nnrf-oauth2' -H 'accept: */*' -H 'Content-Type: application/json' -d '{"service": "nnrf-oauth2","nrfConfigData": { } }'
```

```
{
  "title": "Forbidden",
  "status": "403",
  "detail": "Minimum one value ninstanceid or ninstancesetid must present",
  "instance": "/ocscp/scpc-configuration/v1/nrf-configuration?service=nnrf-oauth2",
  "cause": "INVALID_REQUEST_BODY"
}
```

2.8 OAuth2.0 Configurations

This section provides information about NRF configurations and configuring access token granularity and requests for NF types or NF service instances.

2.8.1 Configuring OAuth2.0 Access Token Granularity

This section provides information about configurations required for access token granularity and access token requests for NFType, specific NF, or NF instance ID.

Resources

The following table describes the resource name to retrieve, add, and delete the access token granularity configurations data based on the query parameters.

Table 2-45 Resource Name

Resource Name	Resource URI	HTTP Method	Description
oauth2-authorization/ access-token-granularity	/ocscp/scpc-configuration/v1/ oauth2-authorization/ access-token-granularity	GET	Retrieves access token granularity configurations.
oauth2-authorization/ access-token-granularity	/ocscp/scpc-configuration/v1/ oauth2-authorization/ access-token-granularity	PUT	Adds an access token granularity configuration.
oauth2-authorization/ access-token-granularity	/ocscp/scpc-configuration/v1/ oauth2-authorization/ access-token-granularity	DELETE	Removes an access token granularity configuration.

Data Model**Request Body**

The following table describes the field names of the `accessTokenGranularityWrapper` data model.

Table 2-46 `accessTokenGranularityWrapper`

Field Name	Data Type	P	Default Value	Description
ruleName	String	M	defaultNonRoaming	Indicates the unique string that works as an ID.
data	AccessTokenGranularityData	M	See Table 2-47	Indicates the specific data for each OAuth2 configuration type.

Note

There are two default entries: one for non-roaming and another for roaming.

Table 2-47 `AccessTokenGranularityData`

Field Name	Data Type	P	Default Value	Range	Description
requesterPlmnIds	PLMN List	C	null	empty or plmn ids	Indicates the list of Local PLMNs IDs. Note: These can be present for NON_ROAMING traffic, but not mandatory to have it in this scenario.

Table 2-47 (Cont.) AccessTokenGranularityData

Field Name	Data Type	P	Default Value	Range	Description
targetPlmnIds	PLMN List	C	null	empty or plmn ids	Indicates the list of target PLMN IDs. Note: These can be present for NON_ROAMING traffic as well, but not mandatory to have it in this scenario.
trafficScenario	enum	M	NON-ROAMING	NON-ROAMING	Represents Local PLMN messages.
consumerNfTypes	Array	O	null	empty or Valid NF Type	Indicates the list of consumer NF types.
targetNfTypes	Array	M	*	* or Valid NF Types	Indicates the list of Target NF types.
targetServiceNames	Array	O	null	empty or valid service names	Indicates the list of Target service names.
supportedAccessTokenGranularity	enum	M	NF-TYPE	NF-TYPE or NF-INSTANCE	This configuration is used when SCP initiates access token process. Based on this value, SCP determines whether to use NF-Type of NF-Instance based query. There possible values are: - NF-TYPE: NF: Represents target NF type based access token. - NF-INSTANCE: Represents target NF instance ID based access token.

Table 2-47 (Cont.) AccessTokenGranularityData

Field Name	Data Type	P	Default Value	Range	Description
accessTokenReqInfo	accessTokenReqInfo Data	O	Structure of accessTokenReqInfo Data: <pre> "accessTokenReqInfo": { "localPlmn" : { "intraScp": { "mandatory" : ["grant_type", "nfInstanceId", "scope", "nfType", "targetNfType"], "preferred" : ["string1", "string2"] }, "interScp": { "mandatory" : ["grant_type", "nfInstanceId", "scope", "nfType", "targetNfType", "targetNfSetId"], "preferred" : ["string1", "string2"] } }, </pre>	composite type	Access token request info configuration is used when SCP initiates access token process. SCP composes query parameters based on these mandatory and preferred parameters. Also, it provides separate section for intra-SCP and inter-SCP. The operator is expected to configure AccessTokenReqInfo as per the allowed access token in the deployed network. - The Mandatory list defines the attributes that are required in an access token request so that NRF can issue the access token. - The preferred list defines the attributes that are expected to be used in access token requests based on their presence in 5G SBI requests from consumer NF; for example, if attributes are present, they are used in access token requests; otherwise, they are not.

Table 2-47 (Cont.) AccessTokenGranularityData

Field Name	Data Type	P	Default Value	Range	Description
			<pre> "remotePlmn" ": { "intraScp": { "mandatory" : ["grant_type", "nfInstanceId", "scope", "nfType", "targetNfType"], "preferred" : ["string1", "string2"] }, } Default: "accessTokenReqInfo": { "localPlmn" : { "intraScp": { "mandatory" : ["grant_type", "nfInstanceId", "scope", "nfType", "targetNfType"] }, "interScp": { </pre>		

Table 2-47 (Cont.) AccessTokenGranularityData

Field Name	Data Type	P	Default Value	Range	Description
			<pre>"mandatory" : ["grant_type","nfInstanceId", "scope","nfType","targetNfSetId", "targetNfSetId"],] } } }</pre>		

Response Body

The response body data model varies based on Rest operation status.

Table 2-48 Response Body

Data Type	P	Cardinality	Response Codes	Description
array(accessTokenGranularityWrapper)	M	1	200 OK	Indicates the list of oauth2 configurations (accessTokenGranularityWrapper) Matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when invalid combination or more than 3 query parameters are provided.

JSON Example of "accessTokenGranularityWrapper"

```
[
{
  "ruleName": "defaultNonRoaming",
  "data": {
    "trafficScenario": "NON-ROAMING",
    "targetNfTypes": [
      ""
    ],
    "supportedAccessTokenGranularity": "NF-TYPE",
    "accessTokenReqInfo": {
      "localPlmn": {
        "intraScp": {
          "mandatory": ["grant_type","nfInstanceId",
"scope","nfType","targetNfType"]
        },

```

```

        "interScp": {
            "mandatory": ["grant_type", "nfInstanceId",
"scope", "nfType", "targetNfSetId", "targetNfSetId"]
        }
    }
}
},
{
    "ruleName": "Config1",
    "data": {
        "requesterPlmnIds": [{"mcc": "325", "mnc": "13"}, { "mcc": "326", "mnc":
"14"}],
        "targetPlmnIds": [{"mcc": "324", "mnc": "12"}, { "mcc": "327", "mnc": "15"}],
        "trafficScenario": "NON-ROAMING",
        "consumerNfTypes": ["PCF", "UDM"],
        "targetNfTypes": ["PCF", "UDM"],
        "targetServiceNames": ["nudm-uecm", "nudm-sdm"],
        "supportedAccessTokenGranularity": "NF-TYPE",
        "accessTokenReqInfo": {
            "localPlmn": {
                "intraScp": {
                    "mandatory": ["grant_type", "nfInstanceId",
"scope", "nfType", "targetNfType"],
                    "preferred": ["requesterFqdn", "targetPlmn"]
                },
                "interScp": {
                    "mandatory": ["grant_type", "nfInstanceId", "scope", "nfType",
"targetNfType", "targetNfSetId"],
                    "preferred": ["requesterFqdn", "targetPlmn"]
                }
            }
        }
    }
},
{.....}
]

```

Resource Definition

GET REST API

This resource fetches the OAuth2 configuration (accessTokenGranularityWrapper) based on the query parameters.

If no query parameter is provided, all message priorities are returned.

Resource URI: /ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity

Table 2-49 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
ruleName	String	O	Indicates the configuration name. If the parameter is empty, all configurations are returned.

Table 2-50 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
array(accessTokenGranularityWrapper)	M	1	200 OK	Indicates the list of OAuth2 configurations (accessTokenGranularityWrapper) matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than three query parameters are provided.

Example

Successful response 1

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity" -H "accept: application/json"
```

Response Body:

```
[
  {
    "ruleName": "defaultNonRoaming",
    "data": {
      "trafficScenario": "NON-ROAMING",
      "targetNfTypes": [
        "*"
      ],
      "supportedAccessTokenGranularity": "NF-TYPE",
      "accessTokenReqInfo": {
        "localPlmn": {
          "intraScp": {
            "mandatory": ["grant_type", "nfInstanceId",
"scope", "nfType", "targetNfType"]
          },
          "interScp": {
            "mandatory": ["grant_type", "nfInstanceId", "scope", "nfType",
"targetNfType", "targetNfSetId"]
          }
        }
      }
    }
  },
  {
    "ruleName": "Config1",
    "data": {
      "requesterPlmnIds": [{"mcc": "325", "mnc": "13"}, { "mcc": "326", "mnc":
"14"}],
      "targetPlmnIds": [{"mcc": "324", "mnc": "12"}, { "mcc": "327", "mnc": "15"}],
      "trafficScenario": "NON-ROAMING",
      "consumerNfTypes": ["PCF", "UDM"],
      "targetNfTypes": ["PCF", "UDM"],
      "targetServiceNames": ["nudm-uecm", "nudm-sdm"]
    }
  }
]
```

```

        "supportedAccessTokenGranularity": "NF-TYPE",
        "accessTokenReqInfo": {
            "localPlmn": {
                "intraScp": {
                    "mandatory": ["grant_type", "nfInstanceId",
"scope", "nfType", "targetNfType"],
                    "preferred": ["string1", "string2"]
                },
                "interScp": {
                    "mandatory": ["grant_type", "nfInstanceId", "scope", "nfType",
"targetNfType", "targetNfSetId"],
                    "preferred": ["string1", "string2"]
                }
            }
        }
    },
    {.....}
]

```

Successful response 2

```

$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-
authorization/access-token-granularity?ruleName=defaultNonRoaming" -H
"accept: application/json"

```

```

[
  {
    "ruleName": "defaultNonRoaming",
    "data": {
      "trafficScenario": "NON-ROAMING",
      "targetNfTypes": [
        ""
      ],
      "supportedAccessTokenGranularity": "NF-TYPE",
      "accessTokenReqInfo": {
        "localPlmn": {
          "intraScp": {
            "mandatory": ["grant_type", "nfInstanceId",
"scope", "nfType", "targetNfType"]
          },
          "interScp": {
            "mandatory": ["grant_type", "nfInstanceId", "scope", "nfType",
"targetNfType", "targetNfSetId"]
          }
        }
      }
    }
  }
]

```

Failure response

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularityruleName=ojhasflakhsdvg" -H "accept: application/json"
```

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "access Token Granularity configuration data not found against
given query parameter(s), Please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/ruleName=ojhasflakhsdvg",
  "cause": "DATA_NOT_FOUND"
}
```

PUT REST API

This resource adds one Oauth 2 configuration (accessTokenGranularityWrapper) using the request body.

If no query parameter is provided, all message priorities are returned.

Resource URI: /ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity

Table 2-51 Data Structures Supported by the PUT Response Body

Name	P	Cardinality	Response Code	Description
array(accessTokenGranularityWrapper)	M	1	200 OK	Indicates the list of oauth2 configurations (accessTokenGranularityWrapper) matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails when an invalid combination or more than three query parameters are provided.

Example

Successful response\$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity" -H "accept: application/json" -H "Content-Type: application/json" -d '{"ruleName":"Config2","data":{"trafficScenario ":"NON-ROAMING"},"targetNfTypes":["PCF"]},"supportedAccessTokenGranularity":"NType"}'

```
{
  "ruleName": "Config2",
  "data": {
    "trafficScenario ": "NON-ROAMING",
    "targetNfTypes": ["PCF"],
    "supportedAccessTokenGranularity": "NType"
  }
}
```

200 OK

```
Failure response$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity" -H "accept: application/json" -H "Content-Type: application/json" -d '{"ruleName\":\"Config2\",\"data\":{\"targetNfTypes\":[\"PCF\"]},\"supportedAccessTokenGranularity\":\"NFType\"}'
```

```
{
  "title": "Bad Request",
  "status": "400",
  "detail": "trafficScenario Object is missing, Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity",
  "cause": "MANDATORY_IE_MISSING"
}
```

DELETE REST API

This resource removes one Oauth 2 configuration (accessTokenGranularityWrapper) based on query parameters.

Resource URI: /ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity

Table 2-52 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
ruleName	String	O	1	Defines the name of the rule. The name of the rule must be unique.

Table 2-53 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None	-	-	204 OK	In a success case, only the response code is returned.
ProblemDetails	M	1	404 NOT FOUND	Returns when no matching entry is found.

Example

Successful response

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity?ruleName=Config2" -H "accept: application/json" */*
```

204OK

Failure response

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/access-token-granularity?ruleName=Config222" -H "accept: */*"

{
  "title": "Not Found",
  "status": "404",
  "detail": "oauth2-authorization/access-token-granularity configuration data not found for the given 'ruleName': Config222",
  "instance": "/ocscp/scpc-configuration/v1/oauth2-authorization/Config222",
  "cause": "DATA_NOT_FOUND"
}
```

2.8.2 Configuring OAuth2.0 Local PLMN Required

This section provides information about configurations required for local PLMN OAuth2.0.

Resources

The following table describes the resource name to retrieve, add, and remove the Oauth2 required configurations data based on the query parameters.

Table 2-54 Resource Name

Resource Name	Resource URI	HTTP Method	Description
oauth2-authorization/local-plmn-oauth2-required-config	/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config	GET	Retrieves the Oauth2 required configurations.
oauth2-authorization/local-plmn-oauth2-required-config	/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config	PUT	Adds and updates the Oauth2 required configuration.
oauth2-authorization/local-plmn-oauth2-required-config	/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config	DELETE	Removes one Oauth2 required configuration.

Data Model

Request Body

The following table describes the field names of the Oauth2RequiredWrapper data model.

Table 2-55 Oauth2RequiredWrapper

Field Name	Data Type	P	Default Value	Description
ruleName	String	M	default	Indicates a unique string that works as an ID.

Table 2-55 (Cont.) OAuth2RequiredWrapper

Field Name	Data Type	P	Default Value	Description
data	LocalNfOAuth2RequiredData	M	See Table 2-56	Indicates the specific data for each OAuth2 configuration type.

Table 2-56 LocalNfOAuth2RequiredData

Field Name	Data Type	P	Default Value	Range	Description
nfType	String	M	*	* or Valid NF type	Indicates the producer NF types for this configuration.
localPlmnIds	PLMN List	O	-	empty or Valid service Names	Indicates the list of Local PLMNs IDs of Producers. Following this pattern: [{"mcc": "234", "mnc": "987"}, {"mcc": "123", "mnc": "987"}, {"mcc": "987"}, {...}....]
serviceNames	Array	O	-	empty or valid service names	Indicates the list valid services names of NF types.
nfInstanceIdList	Array	O	-	empty or instance ids	Indicates the list of producer NF instances IDs.
nfServiceInstanceIdsList	Array	O	-	empty or service instance ids	Indicates the list of producer NF service IDs.
oauth2Required	Boolean	M	false	true or false	OAuth2Required indicates that OAuth2.0 based authorization is required: - If true, it means an access token is required at the selected target NF service instance and for service requests. - If false, then it means an access token is not required at the selected target NF service instance for service requests.

Table 2-56 (Cont.) LocalNfOAuth2RequiredData

Field Name	Data Type	P	Default Value	Range	Description
defaultScope	OAuth2DefaultScopeData	O	{scopeSource: NF-TYPE}	"SERVICE-SPECIFIC"/"NF-TYPE"/"CUSTOM-SCOPE"	Provides different scopes selection options which can be used in the access token process. SERVICE-SPECIFIC: The scope is selected from incoming service request. NF-TYPE: The scope is selected based on the configured NF type (all the services under this NF type will be the scope list). CUSTOM-SCOPE: Allows to explicitly configure the required NF services for scope.

Table 2-57 OAuth2DefaultScopeData Model

Field Name	Data Type	P	Default Value	Description
scopeSource	enum	M	NF-TYPE	Indicates enum with three different values: ScopeSource Enum { "SERVICE-SPECIFIC", "NF-TYPE", "CUSTOM-SCOPE"; }
scopelist	Array	C	-	List of valid services, this is mandatory when scopeSource is CUSTOM-SCOPE and SERVICE-SPECIFIC and NF-TYPE are null.

Response Body

The response body data model varies based on REST operation status.

Table 2-58 Response Body

Data Type	P	Cardinality	Response Codes	Description
array(OAuth2RequiredWrapper)	M	1	200 OK	List of OAuth2 configurations (OAuth2RequiredWrapper) matching criteria.

Table 2-58 (Cont.) Response Body

Data Type	P	Cardinality	Response Codes	Description
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than three query parameters are provided.

Example,

```
[
  {
    "ruleName": "default",
    "data": {
      "nfType": "*"
      "oauth2Required": false,
      "defaultScope": {
        "scopeSource": "NF-TYPE"
      }
    }
  }, {
    "ruleName": "config1",
    "data": {
      "nfType": "AMF",
      "localPlmnIds": [{ "mcc": "325", "mnc": "13"}, { "mcc": "326", "mnc": "14"}],
      "serviceNames": ["nudm-ee"],
      "nfInstanceIdsList": ["1aaf1bbc-6e4a-4454-a507-111111111111",
"1aaf1bbc-6e4a-4454-a507-222222222222"],
      "nfServiceInstanceIdsList": ["1aaf1bbc-6e4a-4454-0000-111111111111",
"1aaf1bbc-6e4a-4454-0000-222222222222"],
      "oauth2Required": true,
      "defaultScope": {
        "scopeSource": "CUSTOM-SCOPE",
        "scopelist": ["nudm-uecm", "nudm-sdm"]
      }
    }
  }, {
    .....
    .....
  }
]
```

Resource Definition

GET REST API

This resource fetches the OAuth2 configuration (OAuth2RequiredWrapper) based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config

Table 2-59 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
ruleName	String	O	Indicates the configuration name. If the parameter is empty, all configurations are returned.

Table 2-60 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
array(Oauth2RequiredWrapper)	M	1	200 OK	Indicates the list of oauth2 configurations (Oauth2RequiredWrapper) matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than three query parameters are provided.

Example

Successful response 1\$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config" -H "accept: application/json"

```
[
  {
    "ruleName": "default",
    "data": {
      "nfType": "*"
      "oauth2Required": false,
      "defaultScope": {
        "scopeSource": "NF-TYPE"
      }
    }
  },
  {
    "ruleName": "config1",
    "data": {
      "nfType": "AMF",
      "localPlmnIds": [{"mcc": "325", "mnc": "13"}, {"mcc": "326", "mnc": "14"}],
      "serviceNames": ["nudm-ee"],
      "nfInstanceIdsList": ["1aaf1bbc-6e4a-4454-a507-111111111111",
"1aaf1bbc-6e4a-4454-a507-222222222222"],
      "nfServiceInstanceIdsList": ["1aaf1bbc-6e4a-4454-0000-111111111111",
"1aaf1bbc-6e4a-4454-0000-222222222222"],
      "oauth2Required": true,
      "defaultScope": {
        "scopeSource": "CUSTOM-SCOPE",
        "scopelist": ["nudm-uecm", "nudm-sdm"]
      }
    }
  },
  {
    .....
    .....
  }
]
```

```

    }
  ]

Failure response$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config?ruleName=ojhasflakhsdv" -H "accept: application/json"

{
  "title": "Not Found",
  "status": "404",
  "detail": "oauth2 configuration data not found against given query parameter(s), Please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/ruleName=ojhasflakhsdv",
  "cause": "DATA_NOT_FOUND"
}

```

PUT REST API

This resource adds one Oauth 2 configuration (Oauth2RequiredWrapper) using the Request Body.

Resource URI: /ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config

Table 2-61 Data Structures Supported by the PUT Response Body

Name	P	Cardinality	Response Code	Description
array(Oauth2RequiredWrapper)	M	1	200 OK	Indicates the list of oauth2 configurations (Oauth2RequiredWrapper) matching criteria
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than three query parameters are provided.

Example

```

Successful response$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config" -H "accept: application/json" -H "Content-Type: application/json" -d '{"ruleName\":\"Config2\",\"data\":{\"nfType\":\"PCF\"},\"oauth2Required\":true}'

{
  "ruleName": "Config2",
  "data": {
    "nfType": "PCF",
    "oauth2Required": true,
  }
}

200 OK

```

DELETE REST API

This resource removes one OAuth 2 configuration (OAuth2RequiredWrapper) based on query parameters.

Resource URI: /ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config

Table 2-62 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
ruleName	String	O	1	Indicates the rule name.

Table 2-63 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None	-	-	204 OK	Returns the successful response. Only response code is returned.
ProblemDetails	M	1	404 NOT FOUND	Returns when no matching entry is found.

Example

Successful response

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config?ruleName=Config2" -H "accept: application/json" */*
```

204 OK

Failure response\$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/oauth2-authorization/local-plmn-oauth2-required-config?ruleName=Config222" -H "accept: */*"

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "OAuth2 configuration data not found for the given 'ruleName': Config222",
  "instance": "/ocscp/scpc-configuration/v1/oauth2-authorization/Config222",
  "cause": "DATA_NOT_FOUND"
}
```

2.9 Configuring Error Profiles

This section provides information about configuring different Error Profiles, which can be used to build problem details sent in response body to the consumer.

Resources

The following table describes the resource name to retrieve, add, update, and remove error profile configuration based on the query parameters.

Table 2-64 Resource Name

Resource Name	Resource URI	HTTP Method	Description
error-response-profile	/ocscp/scpc-configuration/{version}/error-response-profile	GETALL	Retrieves all error profile configurations.
error-response-profile	/ocscp/scpc-configuration/{version}/error-response-profile/{name}	GET	Retrieves error profile configuration for given name.
error-response-profile	/ocscp/scpc-configuration/{version}/error-response-profile/{name}	PUT	Add or update error profile configuration for given name.
error-response-profile	/ocscp/scpc-configuration/{version}/error-response-profile/{name}	DELETE	Deletes error profile configuration for a given name; if the name is in use, it can't be deleted.

Data Model

Request Body

The following table describes the field names of the ErrorProfileData data type.

Table 2-65 ErrorProfileData

Field Name	Data Type	P	Description
name (256)	String	M	Name of the configuration record
errorProfile	JSON	M	Error Profile JSON object

Table 2-66 ErrorProfile

Parameter	Data Type	P	Default Value	Allowed Value	Description
status	Integer	M	500	300-511	HTTP Status Code
cause	String	M	UNSPECIFIED_FAILURE	For list of error causes, see Table 2-72	This parameter indicates the list of error causes that are specific to the occurrence of the problem.
customCause	String (256)	C	null	NA	User defined custom cause. This field will be used only if cause field value is set to "CUSTOM".

Table 2-66 (Cont.) ErrorProfile

Parameter	Data Type	P	Default Value	Allowed Value	Description
title	String (256)	O	Internal Server Error	NA	If this field is null, a standard HTTP status code description is added.
detail	enum	O	null	NA	If present, the same data is used; otherwise, the application can add it optionally.
retryAfter	Integer	C	0	NA	This parameter indicates the number of seconds after client should retry.
redirectURL	String (256)	C	null	NA	This parameter indicates the AbsoluteURL of the resource to which the message is redirected.

Request Body JSON Format

```
{
  "name": "defaultErrorProfile",
  "errorProfile": {
    "status": 500,
    "cause": "UNSPECIFIED_NF_FAILURE",
    "customCause": null,
    "title": "INTERNAL_SERVER_ERROR",
    "detail": null,
    "retryAfter": 0,
    "redirectURL": null
  }
}
```

Resource Definition**GET REST API:**

This resource fetches all the error profile based on the query parameters.

Resource URI: /ocscp/scpc-configuration/{version}/error-response-profile

The following table describes the data structure supported by the GET method on this resource.

Table 2-67 Data structures supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
errorProfile	M	1..N	200 OK	Indicates error profile configurations.

This resource fetches all the error profile based on name.

Resource URI: /ocscp/scpc-configuration/{version}/error-response-profile/{name}

The following table describes the path parameter supported by the GET method on this resource.

Table 2-68 Path Parameter

Name	Data Type	P	Description
name	String	M	Fetches configurations on name.

Example

Successful response - 1

```
$ curl -X 'GET' 'http://10.75.212.104:31109/ocscp/scpc-configuration/v1/error-response-profile' -H 'accept: application/json'
```

```
[
  {
    "name": "ccaHeaderNotPresentError",
    "errorProfile": {
      "status": 400,
      "cause": "MANDATORY_IE_MISSING",
      "title": "BAD_REQUEST",
      "detail": "Bad Request, Mandatory 3gpp-Sbi-Client-Credential header missing",
      "retryAfter": 0
    }
  },
  {
    "name": "ccaVerificationError",
    "errorProfile": {
      "status": 403,
      "cause": "CCA_VERIFICATION_FAILURE",
      "title": "FORBIDDEN",
      "detail": "Forbidden, CCA verification failed",
      "retryAfter": 0
    }
  },
  {
    "name": "defaultErrorProfile",
    "errorProfile": {
      "status": 500,
      "cause": "UNSPECIFIED_NF_FAILURE",
      "title": "INTERNAL_SERVER_ERROR",
      "detail": "Internal Server Error",
      "retryAfter": 0
    }
  },
  {
    "name": "healthCheckErrorProfile",
    "errorProfile": {
      "status": 503,
```

```

        "cause": "NF_CONGESTION_RISK",
        "title": "NF service is overloaded/congested",
        "detail": "NF service is overloaded/congested"
    }
}
]

```

Successful response - 2

```
$ curl -X 'GET'\http://10.75.212.104:31109/ocscp/scpc-configuration/v1/error-
response-profile/defaultErrorProfile\ -H 'accept:
application/json'
```

```

[
  [
    {
      "ruleName": "udm_test",
      "data": {
        "nfServiceName": "nudm_uecm",
        "httpMethods": [
          "GET",
          "POST"
        ],
        "messageType": "REQUEST",
        "enableAssignPriority": true,
        "assignPriority": 10,
        "enableOverridePriority": false,
        "overridePriority": -1
      }
    }
  ]
]

```

Failure Case

```
$ curl -X 'GET'\http://10.75.212.104:31109/ocscp/scpc-configuration/v1/error-
response-profile/defaultError\ -H 'accept: application/json'
```

```

{
  "title": "Not Found",
  "status": "404",
  "detail": "Error Profile data not found against given name. Please refer to
the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/error-response-profile/
defaultError",
  "cause": "DATA_NOT_FOUND"
}
]

```

PUT REST API:

This resource adds or updates the error profile configuration using the request body.

Resource URI: /ocscp/scpc-configuration/{version}/error-response-profile/{name}

Table 2-69 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response codes	Description
errorProfile	M	1	200 OK	Indicates Error Profile to be added.
ProblemDetails	M	1	400/404	Returns ProblemDetails.

Example

Successful response

```
$ curl -X 'PUT'\http://10.75.212.104:31109/ocscp/scpc-configuration/v1/error-response-profile/defaultErrorProfile\ -H 'accept: application/json' \ -H 'Content-Type: application/json' \ -d '{"name": "defaultErrorProfile", "errorProfile": {"status": 500, "cause": "UNSPECIFIED_NF_FAILURE", "title": "INTERNAL_SERVER_ERROR", "detail": "Internal Server Error", "retryAfter": 0}}'
```

```
{
  "name": "defaultErrorProfile",
  "errorProfile": {
    "status": 500,
    "cause": "UNSPECIFIED_NF_FAILURE",
    "title": "INTERNAL_SERVER_ERROR",
    "detail": "Internal Server Error",
    "retryAfter": 0
  }
}
```

Failure Case

```
$ curl -X 'PUT'\http://10.75.212.104:31109/ocscp/scpc-configuration/v1/error-response-profile/defaultErrorProfile\ -H 'accept: application/json' \ -H 'Content-Type: application/json' \ -d '{"name": "defaultErrorProfile", "errorProfile": {"status": 500, "cause": "abc", "title": "INTERNAL_SERVER_ERROR", "detail": "Internal Server Error", "retryAfter": 0}}'
```

```
{
  "title": "Bad Request",
```



```

    "status": "400",
    "detail": "The value given should be either 'custom' or present in
ApplicationError Enum List. Please refer to the User Guide.",
    "instance": "/ocscp/scpc-configuration/v1/error-response-profile/
defaultErrorProfile",
    "cause": "MANDATORY_IE_MISSING"
}

```

DELETE REST API:

This resource deletes the error profile configuration data based on name.

Resource URI: /ocscp/scpc-configuration/{version}/error-response-profile/{name}

Table 2-70 Path Parameter

Name	Data Type	P	Description
name	String	M	Delete configurations for name.

Table 2-71 Data structures supported by the Delete Response Body on this resource

Data Type	P	Cardinality	Response codes	Description
ProblemDetails	M	1	400/404	Problem Details.

Example

Successful response

```

$ curl -X 'DELETE' \ 'http://10.75.212.104:31109/ocscp/scpc-configuration/v1/
error-response-profile/defaultErrorProfile' \ -H 'accept: application/
json'
Server response
Code Details
204
Response headers
date: Fri, 12 May 2023 07:13:56 GMT

```

Failure case

```

$ curl -X 'DELETE' \ 'http://10.75.212.104:31109/ocscp/scpc-configuration/v1/
error-response-profile/defaultErrorProfile' \ -H 'accept: application/json'

```

```

{
  "title": "Not Found",
  "status": "404",
  "detail": "Error Profile data not found against given name. Please refer to
the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/error-response-profile/
defaultErrorProfile",

```

```
"cause": "DATA_NOT_FOUND"
}
```

Protocol or application Error

Table 2-72 Common Protocol and Application Errors

Protocol or application Error	HTTP status code	Description
INVALID_API	400 Bad Request	The HTTP request contains an unsupported API name or API version in the URI.
INVALID_MSG_FORMAT	400 Bad Request	The HTTP request has an invalid format.
INVALID_QUERY_PARAM	400 Bad Request	The HTTP request contains an unsupported query parameter in the URI. See NOTE 1.
MANDATORY_QUERY_PARAM_INCORRECT	400 Bad Request	A mandatory query parameter, or a conditional query parameter that is mandatory, for an HTTP method was received in the URI with a semantically incorrect value. See NOTE 1.
OPTIONAL_QUERY_PARAM_INCORRECT	400 Bad Request	An optional query parameter for an HTTP method was received in the URI with a semantically incorrect value that prevents successful processing of the service request. See NOTE 1.
MANDATORY_QUERY_PARAM_MISSING	400 Bad Request	A query parameter that is defined as mandatory, or as conditional but mandatory, for an HTTP method is not included in the URI of the request. See NOTE 1.
MANDATORY_IE_INCORRECT	400 Bad Request	A mandatory IE within the JSON body, within a variable part of an <code>apiSpecificResourceUriPart</code> or within an HTTP header, or a conditional IE but mandatory for an HTTP method was received with a semantically incorrect value. See NOTE 1.
OPTIONAL_IE_INCORRECT	400 Bad Request	An optional IE within the JSON body or within an HTTP header for an HTTP method was received with a semantically incorrect value that prevents successful processing of the service request. See NOTE 1.
MANDATORY_IE_MISSING	400 Bad Request	A mandatory IE within the JSON body or within the variable part of an <code>apiSpecificResourceUriPart</code> or within an HTTP header, or a conditional IE but mandatory, for an HTTP method is not included in the request. See NOTE 1.
UNSPECIFIED_MSG_FAILURE	400 Bad Request	The request is rejected due to an unspecified client error. See NOTE 2.

Table 2-72 (Cont.) Common Protocol and Application Errors

Protocol or application Error	HTTP status code	Description
RESOURCE_CONTEXT_NOT_FOUND	400 Bad Request	The notification request is rejected because the callback URI still exists in the receiver of the notification, but the specific resource context identified within the notification payload is not found in the NF service consumer.
CCA_VERIFICATION_FAILURE	403 Forbidden	The request is rejected due to a failure to verify the CCA at the receiving entity, for example, an NRF or NF service producer.
TOKEN_CCA_MISMATCH	403 Forbidden	The request is rejected due to a mismatch between the subject claim in the access token and the subject claim in the CCA.
MODIFICATION_NOT_ALLOWED	403 Forbidden	The request is rejected because the contained modification instructions attempt to modify IE, which is not allowed to be modified.
SUBSCRIPTION_NOT_FOUND	404 Not Found	The request for modification or deletion of the subscription is rejected because the subscription is not found in the NF.
RESOURCE_URI_STRUCTURE_NOT_FOUND	404 Not Found	The request is rejected because a fixed part after the first variable part of an <code>apiSpecificResourceUriPart</code> (as defined in clause 4.4.1 of 3GPP TS 29.501 [5]) is not found in the NF. This fixed part of the URI may represent a sub-resource collection, for example, contexts, subscriptions, policies, or a custom operation. See NOTE 5.
INCORRECT_LENGTH	411 Length Required	The request is rejected due to the incorrect value of the content-length header field.
NF_CONGESTION_RISK	429 Too Many Requests	The request is rejected due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation.
INSUFFICIENT_RESOURCES	500 Internal Server Error	The request is rejected due to insufficient resources.
UNSPECIFIED_NF_FAILURE	500 Internal Server Error	The request is rejected due to unspecified reason at the NF. See NOTE 3.
SYSTEM_FAILURE	500 Internal Server Error	The request is rejected due to generic error condition in the NF.
NF_FAILOVER	500 Internal Server Error	The request is rejected due to the unavailability of the NF, and the requester may trigger an immediate re-selection of an alternative NF based on this information. See NOTE 6

Table 2-72 (Cont.) Common Protocol and Application Errors

Protocol or application Error	HTTP status code	Description
NF_SERVICE_FAILOVER	500 Internal Server Error	The request is rejected due to the unavailability of the NF service, and the requester may trigger an immediate re-selection of an alternative NF service based on this information. See NOTE 6.
NF_CONGESTION	503 Service Unavailable	The NF experiences congestion and performs overload control, which does not allow the request to be processed. See NOTE 4.
TARGET_NF_NOT_REACHABLE	504 Gateway Timeout	The request is not served as the target NF is not reachable.
TIMED_OUT_REQUEST	504 Gateway Timeout	The request is rejected due to a request that has timed out at the HTTP client.

Note

NOTE 1: `invalidParams` attribute is included in the "ProblemDetails" data structure, indicating unsupported, missing, or incorrect IEs, query parameters, or 3gpp-Sbi-Discovery-* headers.

Note

NOTE 2: This application error indicates an error in the HTTP request, and there is no other application error value that can be used instead.

Note

NOTE 3: This application error indicates an error condition in the NF, and there is no other application error value that can be used instead.

Note

NOTE 4: If the reason for rejection is a temporary overload, the NF may include in the response a `Retry-After` header field to indicate how long the service is expected to be unavailable.

Note

NOTE 5: If the request is rejected because of an error in an URI before the first variable part of an "apiSpecificResourceUriPart", the "404 Not Found" HTTP status code may be sent without the "ProblemDetails" data structure indicating a protocol or application error.

Note

NOTE 6: The NF service consumer (as receiver of the cause code) should stop sending subsequent requests addressing the resource contexts in the producer's NF instance (for NF_FAILOVER) or NF service instance (for NF_SERVICE_FAILOVER) to avoid massive rejections. The NF service consumer may reselect an alternative NF service producer as specified in clause 6.5 of 3GPP TS 23.527 [38], for example, using the binding indication of resource context. It is implementation specific for the NF service consumer to determine when and whether the NF producer becomes available again, for example, when there is no other alternative available or at expiry of a local configured timer.

2.10 Configuring CanaryRelease Options

You can configure CanaryRelease options using REST APIs. The supported operations are: **LIST**, **GET**, and **PATCH**.

The following REST message samples provide the details about the operations and parameters for CanaryRelease Options. The default values of parameters related to CanaryRelease are mentioned in the following samples, however, you can modify these values. These parameters are applicable at the pod level.

REST Message Samples

Request_Type: GET

URI: /ocscp/scpc-configuration/v1/canaryrelease/

Port: 8081

Message

```
[{
  "canaryReleaseFlag": false,
  "serviceName": "nudm-uecm"
  "apiFullVersion": "1.R15.1.0",
  "canaryTraffic": 5
}
...
]
```

Example:

```
curl --header 'Content-type: application/json' --header 'accept: application/
json' --request GET http://<SCP configuration FQDN/External IP>:8081/ocscp/
scpc-configuration/v1/canaryrelease/
```

```
[{
  "canaryReleaseFlag": false,
  "serviceName": "nudm-uecm",
  "apiFullVersion": "2.R16.1.0",
  "canaryTraffic": 5
```

```
}
...
]
```

Request_Type: LIST
Message

```
curl --header 'Content-type: application/json' --header 'accept: application/
json' --request GET http://<SCP configuration FQDN/External IP>:8081/ocscp/
scpc-configuration/v1/canaryrelease/
```

```
[{
  "canaryReleaseFlag": false,
  "serviceName": "nudm-uecm",
  "apiFullVersion": "2.R16.1.0",
  "canaryTraffic": 5
}
...
]
```

Request_Type: PATCH
Field Name and Type: canaryReleaseFlag <Boolean>

Description: Enable or disable canary release support. Set the value of the canaryReleaseFlag field and mention the serviceName for which the configuration is required in the resource path of the following curl command.

Default Value: null

Message: canaryReleaseFlag UPDATE Command

```
curl --header "Content-Type: application/json" --request PATCH --data '{
  "canaryReleaseFlag": true
}' http://<SCP configuration FQDN/External IP>:8081/ocscp/scpc-
configuration/v1/canaryrelease/<serviceName>
```

Request_Type: PATCH
Field Name and Type: apiFullVersion <String>

Description: The API full version of the canary service. Set the value of the apiFullVersion field and mention the serviceName for which the configuration is required in the resource path of the following curl command.

Default Value: null

Message: apiFullVersion UPDATE Command

```
curl --header "Content-Type: application/json" --request PATCH --data '{
  "apiFullVersion": "2.R16.1.0"
}' http://<SCP configuration FQDN/External IP>:8081/ocscp/scpc-
configuration/v1/canaryrelease/<serviceName>
```

Request_Type: PATCH**Field Name and Type:** canaryTraffic <Integer>**Description:** The traffic that should be distributed to Canary release. Set the value of the canaryTraffic field and mention the serviceName for which the configuration is required in the resource path of the following curl command.**Default Value:** null**Message:** canaryTraffic UPDATE Command

```
curl --header "Content-Type: application/json" --request PATCH --data '{
  "canaryTraffic": 10
}' http://<SCP configuration FQDN/External IP>:8081/ocscp/scpc-
configuration/v1/canaryrelease/<serviceName>
```

2.11 Outlier Detection Configuration

This section describes the REST API configurations required for Outlier Detection. Outlier Detection is configured for each service in the routing option and for inter-SCP and SEPP in System Options. Outlier Detection configurations created using this REST API are used in Routing Options for NF Services and in System Options for inter-SCP and SEPP. This feature can be disabled at the global or system level and enabled at the NF service level in the routing option to work for those services.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the outlier-detection resource type.

Table 2-73 Resources

Resource Name	Resource URI	HTTP Method	Description
outlier-detection	/ocscp/scpc-configuration/{version}/outlier-detection	GET	Retrieves all outlier-detection configurations.
outlier-detection	/ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}	GET	Retrieves outlier-detection configuration for a given ruleName.
outlier-detection	/ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}	PUT	Create or update the outlier-detection configuration for a given ruleName.
outlier-detection	/ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}	PATCH	Updates outlier-detection configuration by ruleName.
outlier-detection	/ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}	DELETE	Removes outlier-detection configuration for a given ruleName. If the rule is in use, then it cannot remove the ruleName.

Data Model

Request Body

The following table describes outlierDetectionConfig data types.

Table 2-74 outlierDetectionConfig

Field Name	Data Type	P	Default Value	Range	Description
ruleName	String	M	NA	NA	Provides the unique rule present in the outlier detection table that must not be repeated.
consecutiveErrors	Integer	O	100	5 - 500	Number of consecutive errors after which an endpoint is considered unhealthy.
interval	String	O	86400 seconds	30 seconds - 86400 seconds	Interval after which stale records are removed from the outlier data cache. Stale records are identified as the records that are not referenced by any message in this interval. Note: The interval value must be significantly greater than baseEjectionTime.
baseEjectionTime	String	O	5 seconds	1 second - 500 seconds	Duration for which an endpoint is ejected
ErrorList	Array(String)	O	["Connection Error", "Time outs", 500, 501, 502, 503, 504, 505, 506, 507, 508, 510, 511]	["Connection Error", "Time outs", 301, 302, 303, 304, 307, 308, 400, 401, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 425, 426, 428, 429, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 510, 511]	List with errors to be considered for outlier detection.

Response Body

JSON Format

```
{
  "ruleName": "defaultRule",
  "outlierDetectionConfigData": {
```



```
        "consecutiveErrors": 100,
        "interval": "86400s",
        "baseEjectionTime": "5s",
        "ErrorList": [
            "500"
        ]
    }
}
```

Response Body
JSON Format

```
{
  "ruleName": "defaultRule",
  "outlierDetectionConfigData": {
    "consecutiveErrors": 100,
    "interval": "86400s",
    "baseEjectionTime": "5s",
    "ErrorList": [
      "500"
    ]
  }
}
```

Resource Definition

This section describes GET, PUT, PATCH, and DELETE resource types supported by this feature.

GET REST API

This section describes the resources to fetch all the outlier-detection configurations.

Resource URI: /ocscp/scpc-configuration/{version}/outlier-detection

Table 2-75 Data Structures Supported by the GET Response Body

Data Type	P	Cardinalit y	Response Codes	Description
outlierDetectionConfig	M	1,,N	200 OK	Indicates outlier-detection configurations.

Resource to fetch all the outlier-detection configurations based on ruleName.

Resource URI: /ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}

Table 2-76 Path Parameters

Name	Data Type	P	Description
ruleName	String	M	Fetches configurations on ruleName.

Table 2-77 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
outlierDetectionConfig	M	1	200 OK	Indicates outlier-detection configurations.
ProblemDetails	M	1	404	Provides problem details.

PUT REST API

This section describes outlier-detection configurations for a given data.

Resource URI: /ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}

Table 2-78 Data Structures Supported by the PUT Request Body

Data Type	P	Cardinality	Response Codes	Description
outlierDetectionConfig	M	1	200 OK	Indicates outlier-detection configurations.
ProblemDetails	M	1	400 or 404 BAD REQUEST	Provides problem details.

PATCH REST API

This section describes resource to update the outlier-detection configurations using the request body.

Resource URI: /ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}

Table 2-79 Data Structures Supported by the PATCH Request Body

Name	Data Type	P	Description
ruleName	String	M	Rule name for which Outlier Detection configuration is modified.
outlierDetectionConfig	JSON	0	patchDocument to be sent. For example, [{ "op": "replace", "path": "/outlierDetectionConfigData/interval", "value": "50s" }][{ "op": "replace", "path": "/outlierDetectionConfigData/ErrorMessage", "value": ["500", "501"] }]

DELETE REST API

This section describes resources to fetch all the outlier-detection configurations based on ruleName.

Resource URI: /ocscp/scpc-configuration/{version}/outlier-detection/{ruleName}

Table 2-80 Path Parameter

Name	Data Type	P	Description
ruleName	String	M	Fetch configurations on ruleName.

Table 2-81 Data Structures Supported by the DELETE Request Body

Data Type	P	Cardinality	Response codes	Description
ProblemDetails	M	1	400 or 404 BAD REQUEST	Provides problem details.

2.12 Configuring NF Service Groups

Service Communication Proxy (SCP) provides NF Service Group configuration and the operator provides the primary and secondary CHF instance information to create the routing rules based on the CHF NF topology information, which is provided by NRF through NF register, reregister, or change notifications.

Parameters for Configuring NF Service Groups

Table 2-82 Parameters for NF Service Groups

Resource Name	Resource URI	HTTP method or custom operation	Description
servicegroups	{apiRoot}/ocscp/scpc-configuration/v1/servicegroups/{serviceName} Ex: {apiRoot}/ocscp/scpc-configuration/v1/servicegroups/nchf-spendinglimitcontrol	GET	Returns the NF Service for a given serviceName.
servicegroups	{apiRoot}/ocscp/scpc-configuration/v1/servicegroups?nfType=value Ex: {apiRoot}/ocscp/scpc-configuration/v1/servicegroups?nfType=CHF	GET	Returns a list of NF Services for a given NF Type.
servicegroups	{apiRoot}/ocscp/scpc-configuration/v1/servicegroups	PUT	Updates the NF Service.
servicegroups	{apiRoot}/ocscp/scpc-configuration/v1/servicegroups?nfType=value&serviceName=value Ex: {apiRoot}/ocscp/scpc-configuration/v1/servicegroups?nfType=CHF&serviceName=nchf-spendinglimitcontrol	PATCH	Updates a single NF Service based on serviceName or Updates multiple NF Services based on NF Type.

Table 2-82 (Cont.) Parameters for NF Service Groups

Resource Name	Resource URI	HTTP method or custom operation	Description
servicegroups	{apiRoot}/ocscp/scpc-configuration/v1/servicegroups/{serviceName} Ex: {apiRoot}/ocscp/scpc-configuration/v1/servicegroups/nchf-spendinglimitcontrol	DELETE	Deletes the given NFService with serviceName.
servicegroups	{apiRoot}/ocscp/scpc-configuration/v1/servicegroups?nfType=value Ex: {apiRoot}/ocscp/scpc-configuration/v1/servicegroups?nfType=CHF	DELETE	Deletes all the services for a given NF Type.

Resource Definition

Table 2-83 Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
servicename	n/a	GET	NFService Group	M	1	200 OK	Upon success, a response body is returned containing the NFService Group for requested Service Name.
servicename	n/a	GET	String	M	1	404 NOT FOUND	The response body contains the message indicating that there were no services found for the requested Service Name.

Table 2-83 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
serviceName: Optional nfType: Optional Note: Either one of above parameters are mandatory. Both cannot be left empty.	NFServiceGroupModifiableFields object with any of the attributes. Note: Data Model for this request body is provided in "Data Models" section.	PATCH	String	M	1	200 OK	Upon success, the following message is returned: Updated NF Service with serviceName: nchf-spendinglimitcontrol
serviceName: Optional nfType: Optional	NFServiceGroupModifiableFields object with any of the attributes. Note: Data Model for this request body is provided in "Data Models" section.	PATCH	String	M	1	403 FORBIDDEN	primaryRegionLocalities can not be empty or its size cannot be zero.
serviceName: Optional nfType: Optional	NFServiceGroupModifiableFields object with any of the attributes. Note: Data Model for this request body is provided in "Data Models" section.	PATCH	String	M	1	400 BAD REQUEST	If both the request parameters are missing, then Bad Request error is returned with the following message: Please pass either serviceName or nfType.

Table 2-83 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
serviceName	n/a	DELETE	String	M	1	200 OK	Upon success, the following message is returned: Successfully deleted the Nf Service for ServiceName: nchf - spendinglimitcontrol
nfType	n/a	GET	List<NFServiceGroup>	M	1	200 OK	Upon success, a response body is returned containing a List of NFService Group's for requested nfType.
nfType	n/a	GET	String	M	1	404 BAD REQUEST	Required parameter 'nfType' is not present.
nfType	n/a	DELETE	String	M	1	200 OK	Upon success, the following message is returned: Successfully deleted all Services for NFType : CHF.

Table 2-83 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
n/a	"NFService Group" object with updated fields. Note: Sample data is provided in Example column and also the "Data Model" for this Request Body could be found in the "Data Models" section.	PUT	NFService Group	M	1	200 OK	Upon success, a response body is returned containing the updated NFService Group object.
n/a	"NFService Group" object with updated fields. Note: Sample data is provided in Example column and also the "Data Model" for this Request Body could be found in the "Data Models" section.	PUT	String	M	1	403 FORBIDDEN	Not allowed to modify NfType or serviceName of NFService Group.

Table 2-83 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
n/a	"NFService Group" object with updated fields. Note: Sample data is provided in Example column and also the "Data Model" for this Request Body could be found in the "Data Models" section.	PUT	String	M	1	400 BAD REQUEST	If any of the mandatory parameters are missing in the Request Body, then BAD REQUEST error would be returned. Note: Refer to Data Model for Mandatory parameters .
n/a	"NFService Group" object with updated fields. Note: Sample data is provided in Example column and also the "Data Model" for this Request Body could be found in the "Data Models" section.	PUT	String	M	1	400 BAD REQUEST	If "primaryRegionLocalities" attribute in Request Body is assigned with empty list, then a BAD REQUEST error would be returned as this value cannot be empty. Response message: Primary Region Localities for a NF Service cannot be Null or empty.

Data Models for NF Service Groups**NFServiceGroup**

Table 2-84 NFServiceGroup

Field Name	Type	P	Description(With default Values)
nfType	Enum	M	NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC, 5GEIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP Note: This parameter cannot be modified.
serviceName	String	M	Only CHF Services are supported: nchf-convergedcharging, nchf-spendinglimitcontrol. Note: This parameter cannot be modified.
primaryRegionLocalities	List<String>	M	This parameter can be modified, but empty values cannot be assigned to this parameter.
secondaryRegionLocalities	List<String>	O	This is an optional parameter and can be modified.

ReroutePolicy**Table 2-85 ReroutePolicy**

Field Name	Type	P	Description(With default Values)
rerouteOptions	Enum	M	Default values: RerouteWithinSite This enables SCP to perform alternate routing from one service to another.

NFServiceGroupModifiableFields**Table 2-86 NFServiceGroupModifiableFields**

Field Name	Type	P	Description(With default Values)
primaryRegionLocalities	List<String>	O	This parameter can be modified, but empty values cannot be assigned to this parameter.
secondaryRegionLocalities	List<String>	O	

Configuring NF Service Groups

User can configure routing options by using the operations GET, PUT, and PATCH.

The following table provides sample details of the operations to configure routing options.

Table 2-87 NF Service Groups Operations

Operations	Message
GET	<pre>curl -X GET "http://10.178.246.62:31108/ocscp/scpc-configuration/v1/servicegroups/nchf-spendinglimitcontrol" -H "accept: application/json"</pre>

Table 2-87 (Cont.) NF Service Groups Operations

Operations	Message
PUT	<pre>curl -X PUT "http://10.178.246.62:31108/ocscp/scpc-configuration/v1/servicegroups" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"nfType\": \"CHF\", \"serviceName\": \"nchf-spendinglimitcontrol\", \"primaryRegionLocalities\": [\"Loc7\", \"USEast\", \"Loc6\"], \"secondaryRegionLocalities\": [\"Loc8\", \"Loc9\"], \"reroutePolicy\": { \"rerouteOptions\": \"RerouteWithinRegion\" } } }</pre>
PATCH	<pre>curl -X PATCH "http://10.178.246.62:31108/ocscp/scpc-configuration/v1/servicegroups?serviceName=nchf-spendinglimitcontrol" -H "accept: application/json" -H "Content-Type: application/merge-patch+json" -d "{ \"primaryRegionLocalities\": [\"Loc7\"] } }</pre>

2.13 Configuring NF Topology Groups

This section describes the configuration on Service Communication Proxy (SCP), which allows SCP to:

- determine the 5G topology from NRF and use it for creating the routing rules.
- stop determining the 5G topology information from NRF and utilize the user configured or updated NF profiles.

5G Topology Source Information

SCP uses this configuration to determine the 5G topology source, and to create the routing rules accordingly.

TopologySourceInfo

Table 2-88 TopologySourceInfo

NF Type (M)	5G topology source (M)
- All 3gpp 5G defined NF types - As defined in TS29.510 section 6.1.6.3.3 String: NFType - Custom NF types	- NRF (default) - learning from NRF - LOCAL

Enumeration: TopologySource

Table 2-89 Enumeration: TopologySource

Enumeration Value	Description
"NRF"	SCP 5G Topology information source is NRF.
"LOCAL"	SCP 5G Topology information source is user configured and not from NRF. This status may result from an NF service failure and may trigger restoration procedures. For more information, see clause 6.2 of 3GPP 23.527 [27]. - Transition from NRF ==> LOCAL: Stop learning from NRF and use available, modified, or created information from SCP. - Transition from LOCAL ==> NRF: Start learning from NRF and create the routing rules accordingly. In this scenario statically configured NF rules may get deleted because their information is not available in NRF.

Table 2-90 Resources and Methods Overview

Resource Name	Resource URI	HTTP Method or Custom Operation	Request Body, Query Parameters	Response Status Code, Body	Description
topologysource	{apiroot}/ocscp/scpc-configuration/v1 / topologysourceinfo	PUT	Body TopologySource	200 OK	Create or update the topology source information for all the NF types.
topologysource	{apiroot}/ocscp/scpc-configuration/v1 / topologysourceinfo	GET	Query Parameters NFType		Read the topology source information for all the NF types.
NFtopologysource (individual NF types)	{apiroot}/ocscp/scpc-configuration/v1 / topologysource/{NFType}	PUT	Body TopologySource	200 OK	Create or update the topology source information for a specific NF type.

Table 2-90 (Cont.) Resources and Methods Overview

Resource Name	Resource URI	HTTP Method or Custom Operation	Request Body, Query Parameters	Response Status Code, Body	Description
NFtopologysource (individual NF types)	{apiroot}/ocscp/scpc-configuration/v1/topologysource/{NFType}	GET	Query Parameters NFType		Read the topology source information for a specific NF type.

5G NF Topology Information

This information is used for configuring 5G NF profiles for the NF whose source has been set to "Local". When the learning source is set to "Local", users can modify the 5G NF profile irrespective of whether they are learned from NRF, that is, source='NRF', or configured statically, that is, source='Local'.

Note

By setting the source to Local, the system does not delete already determined profiles.

Table 2-91 Parameters for NF Topology Groups

Resource Name	Resources and Methods Overview	HTTP Method or Custom Operation	Request Body, Query Parameters	Response Status Code, Body	Description
nf-instances (Store)	{apiRoot}/ocscp/scpc-configuration/v1/nf-instances/	GET	Query Parameters - NFType - ServiceName - NF instance Id - Max number of NF profiles For more information, see Query Parameters .	200, OK, SearchResult. For more information, see Table 2-93. 400 Bad Request, ProblemDetails 500 Internal server error, ProblemDetails	Read a collection of NF Instances.

Table 2-91 (Cont.) Parameters for NF Topology Groups

Resource Name	Resources and Methods Overview	HTTP Method or Custom Operation	Request Body, Query Parameters	Response Status Code, Body	Description
nf-instance s (Store)	{apiRoot}/ocscp/scpc-configuration/v1/nf-instances/	GET	Query Parameters - NFType (M) - array(ServiceName) (O)	200, OK, uriList, For more information, see Table 2-94. - The response body contains a "_links" object containing the URI of each NF in the SCP, or an empty object if there are no NFs to return in the query result, that is, because there are no learned or configured NFs in the SCP, or because there are no matching NFs of the type specified in the "nf-type" query parameter. 400 Bad Request, ProblemDetails 500 Internal server error,	Read a collection of NF Instance Id.

Table 2-91 (Cont.) Parameters for NF Topology Groups

Resource Name	Resources and Methods Overview	HTTP Method or Custom Operation	Request Body, Query Parameters	Response Status Code, Body	Description
				ProblemDetails	
nf-instance (Document)	{apiRoot}/ocscp/scpc-configuration/v1/nf-instances/{nfInstanceId}	GET	Query Parameters - n/a Body - n/a	200 OK, NFProfile	Read the profile of a given NF Instance .
nf-instance (Document)	{apiRoot}/ocscp/scpc-configuration/v1/nf-instances/{nfInstanceId}	PUT	Body NFProfile	200 OK, NFProfile 201 Created, NFProfile	Register or configure in SCP a new NF Instance , or replace the profile of an existing NF Instance , by providing an NF profile.
nf-instance (Document)	{apiRoot}/ocscp/scpc-configuration/v1/nf-instances/{nfInstanceId}	PATCH	Body PatchDocument It contains the list of changes to be made to the profile of the NF Instance, according to the JSON PATCH format specified in IETF RFC 6902.	200 OK, NFProfile 204, NO content	Modify the NF profile of an existing NF Instance .
nf-instance (Document)	{apiRoot}/ocscp/scpc-configuration/v1/nf-instances/{nfInstanceId}	DELETE	Query - n/a Body - n/a	204, NO content	Deregister or delete from SCP a given NF Instance .

Query Parameters

Table 2-92 Query Parameters

Name	Data Type	P	Cardinality	Description	Applicability
nf-type	NFType	M	1	This IE shall contain the NF type of the NF Service Producer being queried.	NF type of the NF Instances whose status is requested to be monitored.
service-names	array(ServiceName)	O	1..N	If included, this IE contains an array of service names for which SCP is queried to provide the list of NF profiles. SCP returns the NF profiles that have at least one NF service matching the NF service names in this list. If not included, the NRF returns all the NF service names registered in the NF profile.	Service name offered by the NF Instances whose status is requested to be monitored. This parameter is optional but if provided it returns with NF profile information.
nf-instance-id	NfInstanceID	O	0..1	Identity of the NF instance being queried.	NF Instance ID of the NF Instance whose status is requested to be monitored.
limit	integer	O	0..1	Maximum number of NFProfiles to be returned in the response.	Query-Params-Ext1.

SearchResult

Table 2-93 SearchResult

Attribute name	Data type	P	Cardinality	Description
nfInstances	array(NF Profile)	M	1..N	It contains an array of NF Instance profiles, matching the search criteria indicated by the query parameters of the query request. An empty array means there is no NF instance that can match the search criteria.

uriList

Table 2-94 uriList

Attribute name	Data type	P	Cardinality	Description
_links	map(LinksValueSchema)	O	1..N	For the description of the members, see clause 4.9.4 of 3GPP TS 29.501.

Configuring NFProfile

Following are the minimum information required by SCP for statically configuring the NFProfile.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-95 Configuring NFProfile

Attribute name	Data type	P	Cardinality	Description
nfInstanceId	String	M	1	Identity of the NF instance being queried.
nfType	NFType	M	1	This IE contains the NF type of the NF Service Producer being queried.
nfStatus	NFStatus	M	1	This contains the NF status of NF Service Producer.
nsiList	array(String)	O	0..N	Returned when SMF is provided as the NFType.
fqdn	String	O	0..1	FQDN of the NF.
interPlmnFqdn	String	O	0..1	If the NF needs to be discovered by other NFs in a different PLMN, then an FQDN that is used for inter-PLMN routing.
ipv4Addresses	array(String)	O	0..N	IPv4 addresses of the NF.
priority	Integer	O	0..1	Priority (relative to other NFs of the same type) in the range of 0-65535, to be used for NF selection; lower values indicate a higher priority.
locality	String	O	0..1	Operator defined information about the location of the NF instance. Note: This value is case-sensitive.
udmInfo	UDMInfo	O	0..1	Specific data for the UDM (ranges of SUPI, group ID...).
ausfInfo	AUSFInfo	O	0..1	Specific data for the AUSF (ranges of SUPI, group ID...).
amfInfo	AMFInfo	O	0..1	Specific data for the AMF (AMF Set ID, ...).
smfInfo	SMFInfo	O	0..1	Specific data for the SMF (DNN's, ...).
pcfInfo	PCFInfo	O	0..1	Specific data for PCF.
chfInfo	CHFInfo	O	0..1	Specific data for CHF.
nfServices	array(NF Service)	O	0..N	List of NF Service Instances. It includes the services produced by the NF that can be discovered by other NFs, if any.

Table 2-95 (Cont.) Configuring NFProfile

Attribute name	Data type	P	Cardinality	Description
nrfRegionOrSetId	String	O	0..1	If not provided, it is taken as "default". It must lie under supportedNRFRegionOrSetIdList of SCP profile, otherwise the Profile is rejected. If supportedNRFRegionOrSetIdList of SCP profile is not provided, it must be left empty. If supportedNRFRegionOrSetIdList of SCP profile is provided, then it must be set to any one of the configured nrfRegionOrSetId. It is the Region (in case of rel15) or SetId (in case of rel16) of NRF to which the profile belongs to. Note: nrfRegionOrSetId is an SCP introduced parameter and used only for NRF profiles or Statically configured profiles.
nfSetIdList	List	O	0..N	Set ID to which NF belongs to.
capacity	Integer	O	0..1	Static capacity information in the range of 0-65535, expressed as a weight relative to other services of the same type.
load	Integer	O	0..1	Dynamic load information, ranged from 0 to 100, indicates the current load percentage of the NF service.
servingScope	String	O	0..1	An SCP parameter that is used only for NRF profiles or statically configured profiles. If it is not provided, it is considered as "default". It must remain under servingScope of SCP, otherwise the profile is rejected. If servingScope of SCP is not provided, then it must be left blank. If servingScope of SCP is provided, it must be set to any one of the configured servingScope.
customInfo	String	O	0..1	Provides custom information for an NF. It is applicable only for SCP or CUSTOM_ORACLE_SCP NF types.

Configuring UDMInfo

Following are the minimum information required by SCP for statically configuring UDMInfo.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-96 Configuring UDMInfo

Attribute name	Data type	P	Cardinality	Description
supiRanges	array(SupiRange)	O	0..N	List of SUPI ranges whose profile data is available in the UDM instance.
gpsiRanges	array(IdentityRange)	O	0..N	List of GPSI ranges whose profile data is available in the UDM instance.

Configuring AUSFInfo

Following are the minimum information required by SCP for statically configuring AUSFInfo.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-97 Configuring AUSFInfo

Attribute name	Data type	P	Cardinality	Description
supiRanges	array(SupiRange)	O	1..N	List of SUPI ranges that can be served by the AUSF instance. If not provided, the AUSF can serve any SUPI.
routingIndicators	array(String)	O	0..N	List of Routing Indicator information that allows to route network signaling with SUCI (see 23.003 [12]) to the AUSF instance. If not provided, the AUSF can serve any Routing Indicator.
GroupId	String	O	0..1	Identifier of the AUSF group. If not provided, the AUSF instance does not pertain to any AUSF group.

Configuring AMFInfo

Following are the minimum information required by SCP for statically configuring AMFInfo.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-98 Configuring AMFInfo

Attribute name	Data type	P	Cardinality	Description
guamiList	array(Guami)	M	1..N	List of supported GUAMIs.

Configuring SMFInfo

Following are the minimum information required by SCP for statically configuring SMFInfo.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-99 Configuring SMFInfo

Attribute name	Data type	P	Cardinality	Description
sNssaiSmfInfoList	array(SnssaiSmfInfoItem)	M	1..N	List of parameters supported by the SMF per S-NSSAI.
pgwFqdn	String	O	0..1	The FQDN of the PGW if the SMF is a combined SMF/PGW-C.
accessType	array(AccessType)	O	0..N	If included, this IE shall contain the access type (3GPP_ACCESS and/or NON_3GPP_ACCESS) supported by the SMF. If not included, it is assumed the both access types are supported.

Configuring PCFInfo

Following are the minimum information required by SCP for statically configuring PCFInfo.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-100 Configuring PCFInfo

Attribute name	Data type	P	Cardinality	Description
supiRanges	array(SupiRange)	O	1..N	List of ranges of SUPIs that can be served by the PCF instance. If not provided, the PCF can serve any SUPI.

Configuring CHFInfo

Following are the minimum information required by SCP for statically configuring CHFInfo.

Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-101 Configuring CHFInfo

Attribute name	Data type	P	Cardinality	Description
supiRangeList	array(SupiRange)	O	1..N	List of SUPI ranges that can be served by the CHF instance. If not provided, the CHF can serve any SUPI.
gpsiRangeList	array(IdentityRange)	O	0..N	List of GPSI ranges that can be served by the CHF instance. If not provided, the CHF can serve any GPSI.

Configuring NFService

Following are the minimum information required by SCP for statically configuring NFService.

① Note

The parameters mentioned in the following table are according to the 3GPP TS 29.510 specification and SCP uses only these parameters.

Table 2-102 Configuring NFService

Attribute name	Data type	P	Cardinality	Description
serviceInstanceId	String	M	1	Unique ID of the service instance within a given NF Instance.
serviceName	Service Name	M	1	Name of the service instance, that is, "udm-sdm".
nfServiceStatus	NFSERVICESTATUS	M	1	Status of the NF Service Instance.
versions	array(NFServiceVersion)	M	1..N	The API versions supported by the NF Service and if available, the corresponding retirement date of the NF Service.
scheme	UriScheme	M	1	URI scheme, for example, "http", "https". Note: Only HTTP is supported.
fqdn	String	O	0..1	FQDN of the NF Service Instance.
ipEndpoints	array(IpEndpoint)	O	0..N	IP addresses and port information of the Network Function, including IPv4 and IPv6 address, where the service is listening for incoming service requests. Note: IPV4 is supported.
apiPrefix	String	O	0..1	Optional path segments is used to construct the {apiRoot} variable of the different API URIs, as described in 3GPP 29.501 [5], clause 4.4.1.
priority	Integer	O	0..1	Priority, relative to other services of the same type, in the range of 0-65535 must be used for the NF service selection; lower values indicate a higher priority.
capacity	Integer	O	0..1	Static capacity information in the range of 0-65535, expressed as a weight relative to other services of the same type.

Table 2-102 (Cont.) Configuring NFService

Attribute name	Data type	P	Cardinality	Description
load	Integer	O	0..1	Dynamic load information, ranged from 0 to 100, indicates the current load percentage of the NF service.

The CustomInfo parameter is used only for nfType as "SCP" or "CUSTOM_ORACLE_SCP".

Table 2-103 CustomInfo

Attribute Name	Data Type	Range	P	Cardinality	Description
Release 15 Deployment					
mateScpInfo	None	NA	O	1	Provides information about mate SCP. This parameter is only applicable for releaseVersion as "R15"
mateScpInfo.capacity	Integer	0-65535	O	1	Indicates the capacity of mate SCP.
mateScpInfo.priority	Integer	0-65535	O	1	Indicates the priority of mate SCP.
mateScpInfo.scpFqdn	String	NA	O	1	Indicates the FQDN of mate SCP.
mateScpInfo.scpInstanceld	String	NA	O	1	Indicates the NFInstanceld of mate SCP.
mateScpInfo.mateSCP Localities	List(String)	NA	O	0..N	Indicates the list of Localities served by mate SCP.
Release 16 Deployment					
mateScpInfoList	List	0-N	O	1	Indicates the list to provide information about mate SCPs.
mateScpInfoList.capacity	Integer	0-65535	O	1	Indicates the capacity of mate SCP.
mateScpInfoList.priority	Integer	0-65535	O	1	Indicates the priority of mate SCP.
mateScpInfoList.scpFqdn	String	NA	O	1	Indicates the FQDN of mate SCP.
mateScpInfoList.scpInstanceld	String	NA	O	1	Indicates the NFInstanceld of mate SCP.
mateScpInfoList.mateSCP Localities	List(String)	NA	O	0..N	Indicates the list of Localities served by mate SCP.

Note

Only for self SCP, you can modify CustomInfo using this REST API. You can add, modify, and remove mate SCP information for self SCP.

2.14 Fetching Release 15 Routing Rules

This section provides the following information about Release 15 Routing Rules configurations:

Request_Type: GET**URI:** /ocscp/scpc-configuration/v1/routing-rules**Port:** 8080**Description:** Retrieve a collection list of routing rules (virtual services) configured in SCP.**Table 2-104 Parameter for fetching routing rules**

Name	DataType	P	Cardinality	Description
nfFqdn	FQDN	O	1	FQDN of NF service.
nfType	NFType	O	1	This IE shall contain the NF type of the NF for which Routing Rules are being fetched.
nfInstanceId	NfInstanceId	O	1	Identity of the NF instance for which Routing Rules are being fetched.
nfServiceType	NFService	O	1	NFService, that is, nudm-uecm, for which Routing Rules are being fetched.
nflp	Ipv4Addr	O	1	IPv4 address for which Routing Rules are being fetched.
nfServiceInstancel d	String	C	1	NF Service Instance ID for which Routing Rules are being fetched. To be used along with nfInstanceId.

Note

- Only one or two Query parameters are supported.
- Valid combination of two query parameters are provided as follows:
 - nfFqdn + nfType
 - Nflp+ nfServiceType
 - nfInstanceId + nfServiceInstancel

Table 2-105 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
array (VirtualServices)	M	1	200 OK	List of routing Rules (Virtual Services) matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than two query parameters are provided.

Sample Data Structure:

```
[{
  "spec": {
    "hosts": ["string"],
    "http": [{
      "match": [{
        "app_name": "string",
        "authority": {
          "exact": "string",
          "ocscpc_exact_into": "string",
          "ocscpw_range_match": {
            "additionalProp1": 0,
            "additionalProp2": 0,
            "additionalProp3": 0
          },
        },
        "ocscpw_snssai": {
          "additionalProp1": "string",
          "additionalProp2": "string",
          "additionalProp3": "string"
        },
        "prefix": "string",
        "regex": "string"
      },
      "headers": {
        "additionalProp1": {
          "exact": "string",
          "ocscpc_exact_into": "string",
          "ocscpw_range_match": {
            "additionalProp1": 0,
            "additionalProp2": 0,
            "additionalProp3": 0
          },
        },
        "ocscpw_snssai": {
          "additionalProp1": "string",
          "additionalProp2": "string",
          "additionalProp3": "string"
        },
        "prefix": "string",
        "regex": "string"
      },
      "additionalProp2": {
        "exact": "string",
        "ocscpc_exact_into": "string",
        "ocscpw_range_match": {
          "additionalProp1": 0,
          "additionalProp2": 0,
          "additionalProp3": 0
        },
      },
      "ocscpw_snssai": {
        "additionalProp1": "string",
        "additionalProp2": "string",
        "additionalProp3": "string"
      },
      "prefix": "string",
      "regex": "string"
    }
  }
}]
```

```

    },
    "additionalProp3": {
      "exact": "string",
      "ocscpc_exact_into": "string",
      "ocscpw_range_match": {
        "additionalProp1": 0,
        "additionalProp2": 0,
        "additionalProp3": 0
      },
      "ocscpw_snssai": {
        "additionalProp1": "string",
        "additionalProp2": "string",
        "additionalProp3": "string"
      },
      "prefix": "string",
      "regex": "string"
    },
    "method": {
      "exact": "string",
      "ocscpc_exact_into": "string",
      "ocscpw_range_match": {
        "additionalProp1": 0,
        "additionalProp2": 0,
        "additionalProp3": 0
      },
      "ocscpw_snssai": {
        "additionalProp1": "string",
        "additionalProp2": "string",
        "additionalProp3": "string"
      },
      "prefix": "string",
      "regex": "string"
    },
    "scheme": {
      "exact": "string",
      "ocscpc_exact_into": "string",
      "ocscpw_range_match": {
        "additionalProp1": 0,
        "additionalProp2": 0,
        "additionalProp3": 0
      },
      "ocscpw_snssai": {
        "additionalProp1": "string",
        "additionalProp2": "string",
        "additionalProp3": "string"
      },
      "prefix": "string",
      "regex": "string"
    },
    "uri": {
      "exact": "string",
      "ocscpc_exact_into": "string",
      "ocscpw_range_match": {
        "additionalProp1": 0,
        "additionalProp2": 0,

```



```

        "additionalProp3": 0
      },
      "ocscpw_snssai": {
        "additionalProp1": "string",
        "additionalProp2": "string",
        "additionalProp3": "string"
      },
      "prefix": "string",
      "regex": "string"
    }
  ]],
  "ocscpc_app_info": {
    "api_version": "string",
    "ocscpc_app_name": "string",
    "ocscpc_group_id": "string",
    "ocscpc_trigger_points": "string"
  },
  "ocscpc_congestion": {
    "ocscpc_alt_rte_clear": 0,
    "ocscpc_alt_rte_onset": 0,
    "ocscpc_error_code": 0,
    "ocscpc_throttle_clear": 0,
    "ocscpc_throttle_onset": 0
  },
  "ocscpc_forward_route": {
    "ocscpc_host": "string",
    "ocscpc_host_header": "string",
    "ocscpc_load": 0,
    "ocscpc_nf_instance_id": "string",
    "ocscpc_service_instance_id": "string",
    "ocscpw_api_prefix": "string"
  },
  "ocscpc_type": "string",
  "ocscpw_reattempt_on": "string",
  "ocscpw_reroutes": {
    "ocscpw_reroute_attempts": 0
  },
  "ocscpw_rproxy": true,
  "retries": {
    "attempts": 0,
    "perTryTimeout": "string"
  },
  "route": [{
    "destination": {
      "endpoints": [{
        "address": "string",
        "ports": {
          "additionalProp1": 0,
          "additionalProp2": 0,
          "additionalProp3": 0
        }
      }
    ]
  },
  "host": "string",
  "location": "string",
  "port": {
    "number": 0
  }

```

```

    },
    "ports": [{
      "name": "string",
      "number": 0,
      "protocol": "string"
    }],
    "resolution": "string"
  },
  "ocscpc_load": 0,
  "ocscpw_api_prefix": "string",
  "ocscpw_nf_instance_id": "string",
  "ocscpw_priority": 0,
  "ocscpw_service_instance_id": "string",
  "weight": 0
}],
"timeout": "string"
}],
"ocscp_nf_instance_id": ["string"]
}
}]

```

Example: Successful response

```
$ curl -X GET "http://10.75.236.84:32360/ocscp/scpc-configuration/v1/routing-rules?nfType=NRF&nfFqdn=nrf1svc.scpsvc.svc.cluster.local" -H "accept: */*"

```

```

[{"spec": {
  "hosts": ["nrf1svc.scpsvc.svc.cluster.local:8080-nnrf-disc"],
  "http": [{
    "match": [{
      "uri": {
        "regex": "/nnrf-disc/v1/(.*)\\??(?:&?[^=&]*=[^=&]*)*"
      },
      "app_name": "END_NODE"
    }],
    "route": [{
      "destination": {
        "host": "nrf1svc.scpsvc.svc.cluster.local",
        "port": {
          "number": 8080
        },
        "location": "MESH_EXTERNAL",
        "ports": [{
          "number": 8080,
          "protocol": "HTTP2",
          "name": "http2"
        }],
        "resolution": "DNS"
      },
      "weight": 5000,
      "ocscpw_priority": 0,
      "ocscpw_nf_instance_id": "6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a",
      "ocscpw_service_instance_id": "fe137ab7-740a-46ee-aa5c-951806d77b02",
    }],
  }],
}
]

```

```

        "ocscpc_load": 0
    },
    "retries": {
        "attempts": 1,
        "perTryTimeout": "1s"
    },
    "ocscpw_reroutes": {
        "ocscpw_reroute_attempts": 2
    },
    "ocscpw_reattempt_on":
"5xx,404,408,retriable-4xx,410,429,307,308",
    "timeout": "6s",
    "ocscpc_type": "END_NODE",
    "ocscpc_congestion": {
        "ocscpc_alt_rte_onset": 80,
        "ocscpc_alt_rte_clear": 75,
        "ocscpc_throttle_onset": 90,
        "ocscpc_throttle_clear": 85,
        "ocscpc_error_code": 503
    },
    "ocscpc_forward_route": {
        "ocscpc_host": "nrf1svc.scpsvc.svc.cluster.local:8080",
        "ocscpc_host_header": ":authority",
        "ocscpc_load": 0,
        "ocscpc_nf_instance_id": "6faf1bbc-6e4a-4454-a507-
a14ef8e1bc5a",
        "ocscpc_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b02"
    }, {
        "match": [{
            "uri": {
                "prefix": "/nrf-disc/v1"
            },
            "app_name": "END_NODE"
        }],
        "route": [{
            "destination": {
                "host": "nrf1svc.scpsvc.svc.cluster.local",
                "port": {
                    "number": 8080
                },
                "location": "MESH_EXTERNAL",
                "ports": [{
                    "number": 8080,
                    "protocol": "HTTP2",
                    "name": "http2"
                }],
                "resolution": "DNS"
            },
            "weight": 5000,
            "ocscpw_priority": 0,
            "ocscpw_nf_instance_id": "6faf1bbc-6e4a-4454-a507-
a14ef8e1bc5a",
            "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b02",

```

```

        "ocscpc_load": 0
    }],
    "retries": {
        "attempts": 1,
        "perTryTimeout": "1s"
    },
    "ocscpw_reroutes": {
        "ocscpw_reroute_attempts": 0
    },
    "ocscpw_reattempt_on":
"5xx,404,408,retriable-4xx,410,429,307,308",
    "timeout": "6s",
    "ocscpc_type": "END_NODE",
    "ocscpc_congestion": {
        "ocscpc_alt_rte_onset": 80,
        "ocscpc_alt_rte_clear": 75,
        "ocscpc_throttle_onset": 90,
        "ocscpc_throttle_clear": 85,
        "ocscpc_error_code": 503
    }
    },
    "ocscp_nf_instance_id": ["6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a"]
}, {
    "spec": {
        "hosts": ["ocscp-scp-worker.scpsvc.svc.cluster.local:8000-nnrf-disc"],
        "http": [{
            "match": [{
                "uri": {
                    "regex": "(/*)?/nnrf-disc/v1/(.*)\\??(?:&?
[^=&]*=[^=&]*)*"
                },
                "app_name": "END_NODE"
            }],
            "route": [{
                "destination": {
                    "host": "nnrf1svc.scpsvc.svc.cluster.local",
                    "port": {
                        "number": 8080
                    },
                    "location": "MESH_EXTERNAL",
                    "ports": [{
                        "number": 8080,
                        "protocol": "HTTP2",
                        "name": "http2"
                    }],
                    "resolution": "DNS"
                },
                "weight": 5000,
                "ocscpw_priority": 0,
                "ocscpw_nf_instance_id": "6faf1bbc-6e4a-4454-a507-
a14ef8e1bc5a",
                "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b02",
                "ocscpc_load": 0
            }],

```

```
"retries": {  
    "attempts": 1,  
    "perTryTimeout": "1s"  
},  
"ocscpw_reroutes": {  
    "ocscpw_reroute_attempts": 2  
},  
"ocscpw_reattempt_on":  
"5xx,404,408,retriable-4xx,410,429,307,308",  
"timeout": "6s",  
"ocscpc_type": "END_NODE",  
"ocscpc_congestion": {  
    "ocscpc_alt_rte_onset": 80,  
    "ocscpc_alt_rte_clear": 75,  
    "ocscpc_throttle_onset": 90,  
    "ocscpc_throttle_clear": 85,  
    "ocscpc_error_code": 503  
}  
}]  
}
```

Failure Case

- If the number of Query Parameters is greater than three, following is the error response:

```
$ curl -X GET "http://localhost:8081//ocscp/scpc-configuration/v1/routing-rules?nfType=NRF&nfServiceType=nnrf-nfm&nfInstanceId=abcd" -H "accept: */*"
Error response for above curl Request:
Response Code: 400
Response Status: Error:BAD_REQUEST
Response Body : { "title": "Bad Request", "status": "400", "detail": "Maximum 2 Query Parameters are allowed", "instance": "/ocscp/scpc-configuration/v1/routing-rules?nfType=NRF&nfServiceType=nnrf-nfm&nfInstanceId=6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a", "cause": "INVALID_MSG_FORMAT" }
Response Headers :
  connection: keep-alive  content-type: application/problem+json  date: Wed30 Dec 2020 07:16:52 GMT  transfer-encoding: chunked
```

- If any invalid combination of Query Parameters is requested, following is the error response:

```
$ curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/routing-rules?nfType=NRF&nfInstanceId=6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a" -H "accept: */*"
Error response for above curl Request:
Response Code: 400
Response Status: Error:BAD_REQUEST
Response Body: { "title": "Bad Request", "status": "400", "detail": "Requested combination of Query Parameters is not allowed", "instance": "/ocscp/scpc-configuration/v1/routing-rules?nfType=NRF&nfInstanceId=6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a", "cause": "INVALID MSG FORMAT" }
```

Response Headers :
 connection: keep-alive content-type: application/problem+json date:
 Wed30 Dec 2020 07:16:52 GMT transfer-encoding: chunked

2.15 Configuring Ingress Rate Limiting

This section provides the following information about Ingress Rate Limiting configuration:

- List of resources required for retrieving, configuring, and deleting the Ingress Rate Limiting data.
- Ingress Rate Limiter data name and data type.
- Functionalities of GET, PUT, and DELETE APIs.

Resources

The following table describes the resources for retrieving, configuring, and deleting the Ingress Rate Limiting data.

Table 2-106 Ingress Rate Limiting Resource Names

Resource Name	Resource URI	HTTP Method	Query Parameters	Description
ingressRateLimiter	/ocscp/scpc-configuration/v1/ratelimit/ingress	GET	NfType or FQDN or NfInstanceId	Retrieves Ingress Rate Limiting data configured to the corresponding supplied query parameters.
ingressRateLimiter	/ocscp/scpc-configuration/v1/ratelimit/ingress	PUT	NA	Configures Ingress Rate Limiting data using the supplied request body in the JSON format.
ingressRateLimiter	/ocscp/scpc-configuration/v1/ratelimit/ingress	DELETE	FQDN or NfInstanceId	Deletes Ingress Rate Limiting data corresponding to supplied query parameters.

Data Model

Request Body

The following table describes Ingress Rate Limiter data name and data type.

Table 2-107 IngressRateLimiterData

Name	DataType	P	Cardinality	Description
nfType	NfType	C	1	Indicates the supported NfType as described in the 3GPP TS 29.510 section 6.1.6.3.3: UDM, AMF, SMF, AUSF, NEF, NRF, PCF, SMSF, NSSF, UDR, LMF, GMLC, F5GEIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP, SCP.
fqdn	String	C	1	Indicates the FQDN of consumer NF.
NfInstanceId	String	C	1	NfInstanceId of consumer NF
enabled	Boolean	O	1	Indicates whether the rate limiting is enabled for nfType/fqdn. Default value is false.
data	Data	M	1	Indicates the rate limit configuration data.

Data

The following table describes the types of data.

Table 2-108 Data Name and Type

Name	DataType	P	Cardinality	Description
config	Config	M	1	Indicates the rate limit data.
errorResponse	ErrorResponse	M	1	Indicates the error handling related data.

Config**Table 2-109 Config Data Type**

Name	DataType	P	Cardinality	Range	Description
durationInSec	integer	M	1	1-300	Indicates the time unit in seconds to calculate the rate.
rate	integer	M	1	1- 50000	Indicates the messages or time unit to be accepted.
burstPercentage	integer	O	1	0 - 100	Indicates the Burst percentage used to calculate the number of burst messages allowed per 100ms. The default value is 0. Note: Burst Control is not supported. Therefore, any value set for this parameter does not take effect.

Table 2-110 ErrorResponse

Name	DataType	P	Cardinality	Range	Description
errorResponse	String	O	1	0-200 characters	Indicates the Custom Error String used in cause field of the ProblemDetails structure as defined in the 3GPP TS 29.571 section 5.2.4.1. Default value shall be a constant string "INGRESS-RATE-LIMITER:TOO MANY REQUESTS" auto configured by SCP.
errorCode	Int	M	1	3xx,4xx,5xx	Indicates the Http Status code.

JSON Format

```
{
  "data": {
    "config": {
      "durationInSec": 0,
      "rate": 0,
      "burstPercentage" : 0
    }
  }
}
```

```

    },
    "errorResponse": {
      "errorCode": 0,
      "errorResponse": "string"
    }
  },
  "enabled": true,
  "fqdn": "string",
  "nfinstanceid": "string",
  "nfType": "string"
}

```

Response Body

The response body data model varies based on the Rest operation status. For more information, refer to the subsequent sections.

Table 2-111 Response Body Data Type

Data Type	Description
IngressRateLimiterData	Same as the request body as described in Table 2-107 .
ProblemDetails	Returns when an invalid combination or more than two query parameters are provided.
None	Indicates an empty body.

Resource Definition

GET REST API

This resource fetches the Ingress Rate Limiting Configuration based on the query parameters. If no query parameter is provided, all the Ingress Rate Limiting Configuration data is returned.

Resource URI: /ocscp/scpc-configuration/v1/ratelimit/ingress

The following table describes URI query parameters supported by the GET method on this resource.

Table 2-112 URI Query Parameters

Name	Data Type	P	Cardinalit y	Description
Fqdn	String	O	1	Indicates the FQDN of consumer NF.
NfInstanceId	String	O	1	NfInstanceId of consumer NF
NFType	NFType	O	1	Indicates the NFType supported as described in the 3GPP TS 29.510 section 6.1.6.3.11: UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC, F5GEIRSEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP, SCP.

Note

Only 1 Query parameters is supported at a time.

The following table describes data structures supported by the GET Response Body on this resource.

Table 2-113 Data Structures

Data Type	P	Cardinality	Response Code	Description
array(IngressRateLimitData)	M	1	200 OK	Indicates the list of Ingress Rate Limiting Configuration data.
IngressRateLimiterData	M	1	200 OK	Indicates the Ingress Rate Limiting Configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Indicates that the requested combination of Query Parameters is not allowed.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example:

Successful response

```
curl -X GET "http://10.75.225.82:31578/ocscp/scpc-configuration/v1/ratelimit/ingress?nfType=PCF" -H "accept: */*"
{
  "nfType": "PCF",
  "data": {
    "config": {
      "rate": 1000,
      "durationInSec": 1,
      "burstPercentage": 0
    },
    "errorResponse": {
      "errorResponse": "TOO MANY REQUESTS",
      "errorCode": 429
    }
  },
  "enabled": true
}
```

Failure response, If the Ingress rate limiting data is not configured.

```
curl -X GET "http://10.75.225.82:31578/ocscp/scpc-configuration/v1/ratelimit/ingress?fqdn=amf" -H "accept: */*"
{
  "title": "Not Found",
  "status": "404",
  "detail": "Ingress Rate Limiting Configuration data not found against given query parameter.",
  "instance": "/ocscp/scpc-configuration/v1/ratelimit/ingress?fqdn=amf",
  "cause": "DATA_NOT_FOUND"
}
```

PUT API

This resource adds Ingress Rate Limiting Configuration using the Request Body.

Resource URI: /ocscp/scpc-configuration/v1/ratelimit/ingress

Note

One of the following fields must be present in the request body:

- Fqdn
- NFType

The following table describes Data structures supported by the PUT Response Body on this resource.

Table 2-114 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
IngressRateLimiterData	M	1	200 OK	Indicates the Ingress Rate Limiting Configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Indicates that both NFType and Fqdn is provided in the request. Returns when an invalid combination or more than two query parameters are provided.

Example:

Successful response

```
curl -X PUT "http://10.75.225.82:30361/ocscp/scpc-configuration/v1/ratelimit/ingress" -H "accept: */*" -H "Content-Type: application/json" -d "{\"data\": {\"config\": {\"durationInSec\": 1, \"rate\": 80}, \"errorResponse\": {\"errorCode\": 429, \"errorResponse\": \"INGRESS-RATE-LIMITER:TOO MANY REQUESTS\"}}, \"enabled\": true, \"nfType\": \"UDM\"}"
```

```
{
  "nfType": "UDM",
  "data": {
    "config": {
      "rate": 80,
      "durationInSec": 1,
      "burstPercentage": 0
    },
    "errorResponse": {
      "errorResponse": "INGRESS-RATE-LIMITER:TOO MANY REQUESTS",
      "errorCode": 429
    }
  },
  "enabled": true
}
```

200 OK

Failure response: If both FQDN and NFType are given in the request body.

```
curl -X PUT "http://10.75.225.82:31578/ocscp/scpc-configuration/v1/ratelimit/ingress" -H "accept: */*" -H "Content-Type: application/json" -d "{\"data\": {\"config\": {\"durationInSec\": 1, \"rate\": 200}, \"errorResponse\": {\"errorCode\": 429, \"errorResponse\": \"TOO MANY REQUESTS\"}}, \"enabled\": true, \"fqdn\": \"udm.oracle.com\", \"nfType\": \"UDM\"}"
```

```
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Both NFType and Fqdn is provided in the request body, Only one of the 2 fields can be provided.",
  "instance": "/ocscp/scpc-configuration/ratelimit/ingress",
  "cause": "INVALID_KEY_COMBINATION"
}
```

Failure response: if rate divided by durationInSec is less than 10, then the configuration is considered as invalid.

```
curl -X 'PUT' \
  'http://10.75.215.197:32438/ocscp/scpc-configuration/v1/ratelimit/ingress' \
  -H 'accept: */*' \
  -H 'Content-Type: application/json' \
  -d '{
    "data": {
      "config": {
        "burstPercentage": 0,
        "durationInSec": 1,
        "rate": 1
      },
      "errorResponse": {
        "errorResponse": "INGRESS-RATE-LIMITER:TOO MANY REQUESTS",
        "errorCode": 429
      }
    },
    "enabled": true,
    "fqdn": "amf1svc.oracle.com"
  },
  {
    "title": "Bad Request",
    "status": "400",
    "detail": "rate divided by durationInSec should be more than or equal to 10, Please refer to the User Guide.",
    "instance": "/ocscp/scpc-configuration/v1/ratelimit/ingress",
    "cause": "MANDATORY_IE_INCORRECT"
  }
}
```

DELETE API:

This resource deletes the Ingress Rate Limiting Configuration data based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/ratelimit/ingress

The following table describes URI query parameters supported by the DELETE method on this resource.

Table 2-115 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
Fqdn	String	O	1	Indicates the FQDN of consumer NF.
NfInstanceId	String	O	1	NfInstanceId of Consumer NF

Note

Rate limit configuration corresponding to NFType is used as the default configuration and only update operation is supported on it.

The following table describes Data structures supported by the DELETE Response Body on this resource.

Table 2-116 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			200 OK	Indicates that the response is successful.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found. Returns when an invalid combination or more than two query parameters are provided.

Example

Successful response

```
curl -X DELETE
  "http://10.75.225.82:31578/ocscp/scpc-configuration/v1/ingressratelimiter?
fqdn=udm.oracle.com" -H
  "accept: */*" 200 OK
```

Failure Response: When no matching entry is found.

```
curl -X DELETE
  "http://10.75.225.82:31578/ocscp/scpc-configuration/v1/ingressratelimiter?
fqdn=amf" -H "accept:
*/*" { "title": "Not Found", "status": "404", "detail": "Ingress Rate
Limiting
Configuration data not found against given fqdn.", "instance":
"/ocscp/scpc-configuration/v1/ratelimit/ingress?fqdn=amf", "cause":
"DATA_NOT_FOUND"
}
```

2.16 Configuring Egress Rate Limiting and Global Egress Rate Limiting

This section provides the information about Egress Rate Limiting and Global Egress Rate Limiting configurations:

- List of resources required for retrieving, configuring, and deleting the rate limiting data.
- Rate limiter data name and data type.
- Functionalities of GET, PUT, and DELETE REST APIs.

Resources

The following table describes the resources for retrieving, configuring, and deleting the egress rate limiting data.

Table 2-117 Egress Rate Limiting Resource Names

Resource Name	Resource URI	HTTP Method	Query Parameters	Description
egressRateLimiter	/ocscp/scpc-configuration/v1/ratelimit/egress	GET	Combination of NFType/FQDN/serviceName	Retrieves egress rate limiting data configured to the corresponding supplied query parameters.
egressRateLimiter	/ocscp/scpc-configuration/v1/rateimit/egress	PUT	NA	Configures egress rate limiting data using the supplied request body in the JSON format.
egressRateLimiter	/ocscp/scpc-configuration/v1/ratelimit/egress	DELETE	Combination of NFType/FQDN/serviceName	Removes egress rate limiting data corresponding to supplied query parameters.

Data Model

Request Body

The following table describes egress rate limiter data name and data type.

Table 2-118 EgressRateLimiterData

Name	DataType	P	Cardinality	Description
nfType	NFType	C	1	Indicates the supported NFType as described in the 3GPP TS 29.510 section 6.1.6.3.3: NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC, F5GEIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP, SCP.
serviceName	ServiceName	C	1	Indicates the ServiceName as per the supported NFType.
fqdn	String	C	1	Indicates the FQDN of producer NF.
enabled	Boolean	O	1	Indicates whether the rate limiting is enabled for this entry: Default value is false.
data	Data	M	1	Indicates the rate limit configuration data.

Data

The following table describes the types of data.

Table 2-119 Data Name and Type

Name	DataType	P	Cardinality	Description
config	Config	M	1	Indicates the rate limit data.
errorResponse	ErrorResponse	C	1	Indicates the error handling related data.

Config

Table 2-120 Config Data Type

Name	DataType	P	Cardinality	Range	Description
durationInSec	integer	M	1	1-300	Indicates the time unit in seconds to calculate the rate.
rate	integer	M	1	1- 75000	Indicates the messages / time unit to be accepted when aggregatedRate is set to 0 or the Global Egress Rate Limit feature is disabled.
aggregatedRate	integer	O	1	0- 75000	Indicates the messages / time unit to be accepted when the Global Egress Rate Limit feature is enabled. If it is set to 0, this field is ignored and this configuration is not considered for Global Egress Rate Limit. It is considered for local rate limit.
burstPercentage	integer	O	1	0 - 100	Indicates the Burst percentage used to calculate the number of burst messages allowed per 100ms. Note: Burst Control is not supported. Therefore, any value set for this parameter does not take effect.
action	String	O	1	"sendResponse" / "AlternateRoute" Default value is "sendResponse"	Defines the action if the rate limit quota is exhausted. "sendResponse": send configured error response back immediately "AlternateRoute": attempt alternate routing

Table 2-121 ErrorResponse

Name	Data Type	P	Cardinality	Range	Description
errorResponse	String	O	1	0-200	Indicates the Custom Error String used in cause field of the ProblemDetails structure as defined in the 3GPP TS 29.571 section 5.2.4.1. Default value shall be a constant string "EGRESS-RATE-LIMITER:TOO MANY REQUESTS" auto configured by SCP.
errorCode	Int	M	1	3xx,4xx,5xx	Indicates the Http Status code.

JSON Format

```
{
  "data": {
    "config": {
      "action": "string",
      "aggregatedRate": 0,
      "burstPercentage": 0,
      "durationInSec": 0,
      "rate": 0
    },
    "errorResponse": {
      "errorCode": 0,
      "errorResponse": "string"
    }
  },
  "enabled": true,
  "fqdn": "string",
  "nfType": "string",
  "serviceName": "string"
}
```

Response Body

The response body data model varies based on the REST operation status.

Table 2-122 Response Body Data Type

Data Type	Description
EgressRateLimiterData	Same as the request body as described in Table 2-118 .
ProblemDetails	Indicates the ProblemDetails structure as defined in the 3GPP TS 29.571 section 5.2.4.1.
None	Indicates an empty body.

Resource Definition**GET REST API**

This resource fetches the egress rate limiting configuration based on the query parameters. If no query parameter is provided, all the egress rate limiting configuration data is returned.

Resource URI: /ocscp/scpc-configuration/v1/ratelimit/egress

The following table describes URI query parameters supported by the GET method on this resource.

Table 2-123 URI Query Parameters

Name	Data Type	P	Cardinality	Description
NFType	NFType	O	1	Indicates the supported NFType as described in the 3GPP TS 29.510 section 6.1.6.3.3: UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC, F5GEIRSEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP, SCP.
serviceName	ServiceName	O	1	Indicates the ServiceName as per the supported NFType.
Fqdn	String	O	1	Indicates the FQDN of producer NF.

Note

The valid combination of query parameters are as follows:

- Fqdn + serviceName
- Fqdn + NFType
- Fqdn
- serviceName
- NFType

The following table describes data structures supported by the GET Response Body on this resource.

Table 2-124 Data Structures Supported by the GET Response Body on this resource

Data Type	P	Cardinality	Response Code	Description
array (EgressRateLimiterData)	M	1	200 OK	Indicates the list of egress rate limiting configuration data.
EgressRateLimiterData	M	1	200 OK	Indicates the egress rate limiting configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Indicates that the requested combination of query parameters is not allowed.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example:

Successful response - 1, Combination of Fqdn, serviceName

```
$ curl -X GET "http://10.75.224.67:31612/ocscp/scpc-configuration/v1/
ratelimit/egress?serviceName=nudm-uecm&fqdn=udm1svc.scpsvc.svc.cluster.local"
-H "accept: */*"

{
  "fqdn": "udm1svc.scpsvc.svc.cluster.local",
  "serviceName": "nudm-uecm",
  "data": {
    "config": {
      "rate": 1000,
      "durationInSec": 1,
      "action": "AlternateRoute",
      "burstPercentage": 0,
      "aggregatedRate": 5000
    },
    "errorResponse": {
      "errorResponse": "TOO MANY REQUEST",
      "errorCode": 429
    }
  },
  "enabled": true
}
```

Successful response - 2, Only serviceName

```
$ curl -X GET "http://10.75.224.67:31612/ocscp/scpc-configuration/v1/
ratelimit/egress?serviceName=nudm-uecm" -H "accept: */*"

{
  "serviceName": "nudm-uecm",
  "data": {
    "config": {
      "rate": 1000,
      "durationInSec": 1,
      "action": "AlternateRoute",
      "burstPercentage": 0,
      "aggregatedRate": 5000
    },
    "errorResponse": {
      "errorResponse": "TOO MANY REQUEST",
      "errorCode": 429
    }
  },
  "enabled": true
}
```

Failure case, Incorrect combination of parameters such as NFType and serviceName

```
$ curl -X GET "http://10.75.226.108:30331/ocscp/scpc-configuration/v1/
ratelimit/egress?nfType=UDM&serviceName=nudm-uecm" -H "accept: */*"
Response Body :
{
  "title": "Bad Request",
```

```

    "status": "400",
    "detail": "Requested combination of Query Parameters is not allowed, please
refer to the User Guide",
    "instance": "/ocscp/scpc-configuration/v1/ratelimit/egress?
nfType=UDM&serviceName=nudm-uecm",
    "cause": "INVALID_QUERY_PARAM"
}

```

PUT REST API

This resource adds and updates egress rate limiting configuration using the Request Body.

Resource URI: /ocscp/scpc-configuration/v1/ratelimit/egress

The following table describes data structures supported by the PUT Response Body on this resource.

Table 2-125 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinalit y	Response Codes	Description
EgressRateLimiterData	M	1	200 OK	Indicates the egress rate limiting configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Indicates that both NFType and Fqdn is provided in the request. The ProblemDetails structure is defined in the 3GPP TS 29.571 Section 5.2.4.1.

Note

The valid combination of fields in the request body is as follows:

- Fqdn, serviceName
- Fqdn, NFType
- Fqdn
- serviceName
- NFType

Example:

Successful response - 1, Combination of Fqdn and ServiceName.

Configuring with a global rate of 5000 with aggregatedRate field.

```

$ curl -X PUT "http://10.75.226.108:32042/ocscp/scpc-configuration/v1/
ratelimit/egress" -H "accept: */*" -H "Content-Type: application/json" -d
{"data":{"config":
{"action":"AlternateRoute","durationInSec":1,"rate":100},"errorRespon
se":{"errorCode":429,"errorMessage":"EGRESS_RATE_LIMITER:T00 MANY
REQUEST"}},{"enable":true,"fqdn":"udm1.vzw.com","serviceName":"nudm-
uecm"}}
{

```

```

    "fqdn": "udm1.vzw.com",
    "serviceName": "nudm-uecm",
    "enabled": true,
    "data": {
      "config": {
        "rate": 100,
        "durationInSec": 1,
        "burstPercentage" : 0,
        "action": "AlternateRoute"
      },
      "globalConfig": {
        "rate": 120,
        "durationInSec": 1,
        "burstPercentage" : 0,
        "action": "AlternateRoute"
      },
      "errorResponse": {
        "errorResponse": "EGRESS_RATE_LIMITER:TOO MANY REQUEST",
        "errorCode": 429
      }
    }
  }
}

```

200 OK

Successful response - 2, Combination of Fqdn and ServiceName.

```

curl -X 'PUT' \
  'http://<SCP configuration FQDN>:30446/ocscp/scpc-configuration/v1/ratelimit/egress' \
  -H 'accept: */*' \
  -H 'Content-Type: application/json' \
  -d '{
    "fqdn": "nef1.vzw.com",
    "serviceName": "nnef-eventexposure",
    "enabled": true,
    "data": {
      "config": {
        "rate": 100,
        "durationInSec": 1,
        "burstPercentage" : 0,
        "action": "AlternateRoute"
      },
      "globalConfig": {
        "rate": 120,
        "durationInSec": 1,
        "burstPercentage" : 0,
        "action": "AlternateRoute"
      },
      "errorResponse": {
        "errorResponse": "EGRESS_RATE_LIMITER:TOO MANY REQUEST",
        "errorCode": 429
      }
    }
  }'

```

Failure case 1: Incorrect combination of fields such as NFType and serviceName in request body

```
$ curl -X PUT "http://10.75.226.108:30331/ocscp/scpc-configuration/v1/ratelimit/egress" -H "accept: */*" -H "Content-Type: application/json" -d '{"data":{"config":{"action":"AlternateRoute","durationInSec":1,"rate":300},"errorResponse":{"errorCode":0,"errorResponse":"","enable":true},"nfType":"UDM","serviceName":"nudm-uecm"}}'
```

Response Body:

```
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Incorrect combination of Keys in request Body, please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/ratelimit/egress",
  "cause": "INVALID_KEY_COMBINATION"
}
```

Failure response: if rate divided by durationInSec is less than 10, then the configuration is considered as invalid.

```
curl -X 'PUT' \
'http://10.75.215.197:32438/ocscp/scpc-configuration/v1/ratelimit/egress' \
-H 'accept: */*' \
-H 'Content-Type: application/json' \
-d '{
  "data": {
    "config": {
      "action": "sendResponse",
      "burstPercentage": 0,
      "durationInSec": 1,
      "rate": 1,
      "aggregatedRate": 0
    },
    "errorResponse": {
      "errorResponse": "EGRESS-RATE-LIMITER:T00 MANY REQUESTS",
      "errorCode": 429
    }
  },
  "enabled": true,
  "fqdn": "udm1svc.scpsvc.svc.cluster.local"
}'
{
  "title": "Bad Request",
  "status": "400",
  "detail": "rate divided by durationInSec should be more than or equal to 10, Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/ratelimit/egress",
  "cause": "MANDATORY_IE_INCORRECT"
}
```

DELETE REST API

This resource deletes the egress rate limiting configuration data based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/ratelimit/egress

The following table describes URI query parameters supported by the DELETE method on this resource.

Table 2-126 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
NFType	NFType	O	1	Indicates supported NFType as described in the 3GPP TS 29.510 section 6.1.6.3.3: UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC, F5GEIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP, SCP.
serviceName	ServiceName	O	1	Indicates the ServiceName as per supported NFType.
Fqdn	String	O	1	Indicates the FQDN of producer NF.

Note

The valid combination of query parameters are provided as follows:

- Fqdn, serviceName
- Fqdn, NFType
- Fqdn
- serviceName

The following table describes data structures supported by the DELETE Response Body on this resource.

Table 2-127 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			200 OK	Indicates that the response is successful.
ProblemDetails	M	1	400 BAD REQUEST	Indicates that the requested combination of query parameters is not allowed.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Successful response - 1, Combination of Fqdn and serviceName

```
$ curl -X DELETE "http://10.75.226.108:30331/ocscp/scpc-configuration/v1/ratelimit/egress?fqdn=udm1.vzw.com&serviceName=nudm-uecm" -H "accept: */*" 200OK
```

Successful response - 2, Only Fqdn Delete

```
$ curl -X DELETE "http://10.75.226.108:30331/ocscp/scpc-configuration/v1/egressratelimiter?fqn=udm1.vzw.com"-H "accept: */*" 200OK
```

Failure case 1, Incorrect query parameter like NFType

```
$ curl -X DELETE "http://10.75.226.108:30331/ocscp/scpc-configuration/v1/ratelimit/egress?nfType=UDM"-H "accept: */*" Response Body:{ "title": "Bad Request", "status": "400", "detail": "Requested Delete combination of Query Parameters is not allowed, please refer to the User Guide", "instance": "/ocscp/scpcconfiguration/v1/ratelimit/egress?nfType=UDM", "cause": "INVALID_QUERY_PARAM"}
```

Failure case 2, When no matching entry is found

```
$ curl -X DELETE "http://10.75.226.108:30331/ocscp/scpcconfiguration/v1/ratelimit/egress?serviceName=nudm-sdm"-H "accept: */*" Response Body:{ "title": "Not Found", "status": "404", "detail": "Egress Rate Limiting configuration data not found against given query parameter(s), Please refer to the User Guide", "instance": "/ocscp/scpc-configuration/v1/ratelimit/egress?serviceName=nudm-sdm", "cause": "DATA_NOT_FOUND"}
```

2.17 Configuring Dynamic Logging

Service Communication Proxy (SCP) provisions an option to change log levels of SCP microservices dynamically through SCP configuration service.

Retrieving all Service Level Logs

Table 2-128 Retrieving all Service Level Logs

Resource URI	HTTP Method	Content Type	Response Codes
Configuration attributes for all service level logs			
<code>http://<ip>:<port>/ocscp/scpc-configuration/v1/all/logging</code>	GET	application/json	200: Successfully returns Log Levels of all SCP microservices 404: No SCP Log levels found in system
Configuration attributes at service level logs			
<code>http://<ip>:<port>/ocscp/scpc-configuration/v1/<microservice-name>/logging</code>	GET	application/json	200: Successfully returns Log Levels of all SCP microservices 404: No SCP Log levels record found for microservice

Table 2-128 (Cont.) Retrieving all Service Level Logs

Resource URI	HTTP Method	Content Type	Response Codes
<code>http://<ip>:<port>/ocscp/scpc-configuration/v1/<microservice-name>/logging</code>	PUT	application/json	200: Successfully returns Log Levels of all SCP microservices 400: Request Body is empty for service 404: No SCP Log levels record found for microservice

Note

The following microservices are supported: scp-worker, scpc-notification, scpc-configuration, scpc-audit, and scpc-subscription.

Response Body of GET Method for all Service Level Logs:

```
[
  {
    "scpc-audit": {
      "appLogLevel": "WARN",
      "packageLogLevel": [
        {
          "packageName": "library",
          "logLevelForPackage": "OFF"
        }
      ],
      "logRateControl": {
        "rate": 1,
        "logLevel": "OFF"
      }
    },
    "scpc-notification": {
      "appLogLevel": "WARN",
      "packageLogLevel": [
        {
          "packageName": "library",
          "logLevelForPackage": "OFF"
        }
      ],
      "logRateControl": {
        "rate": 1,
        "logLevel": "OFF"
      }
    },
    "scpc-subscription": {
      "appLogLevel": "WARN",
      "packageLogLevel": [
        {
          "packageName": "library",
          "logLevelForPackage": "OFF"
        }
      ]
    }
  ],
]
```

```

        "logRateControl": {
            "rate": 1,
            "logLevel": "OFF"
        }
    },
    "scpc-configuration": {
        "appLogLevel": "INFO",
        "packageLogLevel": [
            {
                "packageName": "library",
                "logLevelForPackage": "OFF"
            }
        ],
        "logRateControl": {
            "rate": 1,
            "logLevel": "OFF"
        }
    },
    "scp-worker": {
        "appLogLevel": "WARN",
        "packageLogLevel": [
            {
                "packageName": "library",
                "logLevelForPackage": "OFF"
            }
        ],
        "logRateControl": {
            "rate": 1,
            "logLevel": "OFF"
        }
    },
    "scp-cache": {
        "appLogLevel": "WARN",
        "packageLogLevel": [
            {
                "packageName": "library",
                "logLevelForPackage": "OFF"
            }
        ],
        "logRateControl": {
            "rate": 1,
            "logLevel": "OFF"
        }
    }
}
]

```

Response Body of GET Method at Service Level Logs:

```

{
  "appLogLevel": "INFO",
  "packageLogLevel": [
    {
      "logLevelForPackage": "library",
      "packageName": "OFF"
    }
  ]
}

```



```

    }
  ],
  "logRateControl": {
    "rate": 1,
    "logLevel": "OFF"
  }
}

```

Response Body of PUT Method at Service Level Logs:

```

{
  "appLogLevel": "INFO",
  "packageLogLevel": [
    {
      "logLevelForPackage": "library",
      "packageName": "OFF"
    }
  ],
  "logRateControl": {
    "rate": 1,
    "logLevel": "OFF"
  }
}

```

Table 2-129 Logging

Attribute Name	Data Type	Constraints	Default Values	Description
appLogLevel	string	INFO,DEBUG,WARN,ERROR	WARN	Specifies the log level of the application Note: WARN - data plane (scp-worker); INFO - control planes (scpc-audit, scpc-subscription, scpc-notification, and scpc-configuration)
packageLogLevel	array (PackageLogLevel)		See PackageLogLevel table	Specifies a list of individual packages and their respective log levels
logRateControl	See LogRateControl table	See LogRateControl table	See LogRateControl table	Specifies the log levels of the application to support rate control.

Table 2-130 PackageLogLevel

Attribute Name	Data Type	Constraints	Default Values	Description
packageName	string	root	root	Specifies the name of the package
logLevelForPackage	string	INFO,DEBUG,WARN,ERROR,FATAL,OFF,TRACE	WARN	Specifies the log level for the given package

Table 2-131 LogRateControl

Attribute Name	Data Type	Constraints	Default Values	Description
rate	Integer	1-1000	1	Specifies the average number of logs per second that should be allowed.
logLevel	string	ERROR,WARN,INFO,DEBUG,TRACE,OFF	OFF	Specifies the log level to control log rate.

Log levels during deployment

The default log levels of SCP Services can be set during deployment time as below:

```
# ***** LOG LEVELS OF ALL SERVICES ***** #
serviceLogLevels:
  scpcAudit: &auditLogLevelRef INFO
  scpcConfiguration: &configLogLevelRef INFO
  scpcSubscription: &subsLogLevelRef INFO
  scpcNotification: &notifLogLevelRef INFO
  scpWorker: &workerLogLevelRef WARN
# ***** END ***** #
```

Note

The variables start with **&** are reference variables that must not be modified.

Changing log levels from internal config pod

The log levels can be changed from inside config pod.

Step: curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/all/logging" -H "accept: application/json" or to get log level of particular service. curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/<microservice-name>/logging" -H "accept: application/json" Step3: To change log level of a service. Updating all services(PUT ALL) at once not supported. curl -X PUT "http://localhost:8081/ocscp/scpc-configuration/v1/<microservice-name>/logging" -H "accept: application/json" -H "Content-Type: application/json" -d '{"appLogLevel":"warn","packageLogLevel":{"packageName":"library","logLevelForPackage":"OFF"}}'

1. Execute the following command into config pod:

```
kubectl exec -it <config_pod_name> -n <namespace> bash
```

2. Check log levels of all services as follows:

```
curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/all/logging" -H "accept: application/json"
```

3. Get log level of particular service as follows:

```
curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/
<microservice-name>/logging" -H "accept: application/json"
```

4. To change log level of a service. Updating log level for all the services at once (PUT ALL) is not supported:

```
curl -X PUT "http://localhost:8081/ocscp/scpc-configuration/v1/
<microservice-name>/logging" -H "accept: application/json" -H "Content-
Type: application/json" -d "{\"appLogLevel\":\"warn\",\"packageLogLevel\":
[{\\"packageName\":\"library\", \"logLevelForPackage\":\"OFF\"}]}"
```

For performing logging configurations using the CNC Console, see *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

2.18 Fetching Release 16 Routing Rules

This section provides details about fetching routing information that is supported in Release 16 deployment. The following information is fetched for routing:

- List of resources required for retrieving routing information
- URI Query parameters supported by the GET method
- Data structures supported by the GET response body

For information about Release 16, see 3GPP TS 23.501 version 16.6.0 Release 16.

Resources

The following table describes the resource name to retrieve a collection of routing information.

Table 2-132 Resource Name

Resource Name	Resource URI	HTTP Method	Description
routing-rules-r16	/ocscp/scpc-configuration/v1/routing-rules-r16	GET	Retrieves a collection or list of routing information (NfInstanceServices) configured in SCP. Use this API when Model C support is enabled in SCP. For information about enabling this feature, see <i>Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide</i> .

Resource Definition

This resource fetches the routing information (NfInstanceServices) based on the query parameters.

If no query parameter is provided, all the routing information is returned.

Resource URI: /ocscp/scpc-configuration/v1/routing-rules-r16

Table 2-133 URI Query Parameters Supported by the GET Method

Name	Data Type	P	Cardinality	Description
nfSetId	String	O	1	Indicates the nfSetId of the NF.
nfFqdn	FQDN	O	1	Indicates the FQDN of NF service.
nfType	NFType	O	1	Indicates the NF type of the NF for which routing information is fetched.
nfInstanceId	NfInstanceId	O	1	Identifies the NF instance for which routing information is fetched.
nfServiceType	NFService	O	1	Indicates NFService, for example, nudm-uecm, for which routing information is fetched.
nflp	Ipv4Addr	O	1	Indicates the IPv4 address for which routing information is fetched.
nfServiceInstanceId	String	C	1	Indicates the NF Service Instance ID for which routing information is fetched. Use it with nfInstanceId.

Note

- Supports only 0 to 3 query parameters.
- The valid combinations of 1 query parameter are as follows:
 - nfSetId
 - nflp
 - nfFqdn
 - nfType
 - nfInstanceId
 - nfServiceType
- The valid combinations of 2 query parameters are as follows:
 - nfSetId + nfFqdn
 - nfSetId + nflp
 - nfSetId + nfInstanceId
 - nfSetId + nfType
 - nfSetId + nfServiceType
 - nfFqdn + nfServiceType
 - Nflp+ nfServiceType
 - nfInstanceId + nfServiceInstanceId
- The valid combinations of 3 query parameters are as follows:
 - nfSetId + nfFqdn + nfServiceType
 - nfSetId + nflp + nfServiceType
 - nfSetId + nfInstanceId + nfServiceInstanceId
- If there are more than 3 query parameters, these combinations are considered as invalid.

The following tables describe query parameters for Local and InterSCP.

Table 2-134 One Query Parameter for Local and InterSCP

Parameter	Local	InterSCP (Foreign)	Description
nfInstnaceId	Allowed	Allowed	Identifies the NF instance for which routing information is fetched.
nfSetId	Allowed	NA	Indicates the nfSetId of the NF.
nfType	Allowed	NA	Indicates the NF type of the NF for which routing information is fetched.
nfServiceType	Allowed	NA	Indicates NFService, for example, nudmuecm, for which routing information is fetched.
locality	NA	Allowed	Identifies the InterSCP unknown instance for which routing information is fetched.
nfFqdn	Allowed	Allowed	Indicates the FQDN of NF service.

Table 2-134 (Cont.) One Query Parameter for Local and InterSCP

Parameter	Local	InterSCP (Foreign)	Description
nfIp	Allowed	Allowed	Indicates the IPv4 address for which routing information is fetched.

Two Query Parameter for Local and InterSCP

Table 2-135 Two Query Parameter for Local and InterSCP

Parameter	Local	InterSCP (Foreign)	Description
nfSetId + nfFqdn	Allowed	NA	nfSetId of the NF and FQDN of NF service.
nfSetId + nfIp	Allowed	NA	nfSetId of the NF and IPv4 address for which routing information is fetched.
nfSetId + nfInstncId	Allowed	NA	nfSetId of the NF and identity of the NF instance for which routing information is fetched.
nfSetId + nfType	Allowed	NA	nfSetId of the NF and the NF type for which routing information is fetched.
nfSetId + nfServiceType	Allowed	NA	nfSetId of the NF and NFService, for example, nudm-uecm, for which routing information is fetched.
nfFqdn + nfServiceType	Allowed	NA	FQDN of the NF service and the NF service type, for example, nudm-uecm, for which routing information is fetched.
nfIp+ nfServiceType	Allowed	NA	IPv4 address of the NF and the NF service type, for example, nudm-uecm, for which routing information is fetched.
nfInstncId + nfServiceInstncId	Allowed	NA	Identity of the NF instance and the NF Service Instance ID for which routing information is fetched. Note: To be used with nfInstncId.
nfFqdn + locality	NA	Allowed	FQDN of NF service and identity of the InterSCP of unknown records for which routing information is fetched.
nfIp+ locality	NA	Allowed	IPv4 address of the NF and identity of the InterSCP of unknown records for which routing information is fetched.
nfInstncId + locality	NA	Allowed	Identity of the NF instance and identity of the InterSCP of unknown records for which routing information is fetched.

Three Query Parameter for Local and InterSCP

Table 2-136 Three Query Parameter for Local and InterSCP

Parameter	Local	InterSCP (Foreign)	Description
nfSetId + nfFqdn + nfServiceType	Allowed	NA	Fetches SCP routing rules information for Release 16 using nfSetId, nfFqdn, and nfServiceType.
nfSetId + nfIp + nfServiceType	Allowed	NA	Fetches SCP routing rules information for Release 16 using nfSetId, nfIp, and nfServiceType.

Table 2-136 (Cont.) Three Query Parameter for Local and InterSCP

Parameter	Local	InterSCP (Foreign)	Description
nfSetId + nfInstanceId + nfServiceInstanceId	Allowed	NA	Fetches SCP routing rules information for Release 16 using nfSetId, nfInstanceId, and nfServiceInstanceId.

Data Structures Supported by the GET Response Body on this Resource

The following tables describes the supported data type by the GET response body.

Table 2-137 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
array(NfInstanceServices)	M	1	200 OK	Indicates the list of routing rules (NfInstance Services) matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than three query parameters are provided.

NfInstanceServices

```
{
  local: [
    {
      "kind": "NFInstanceServiceMapping",
      "spec": {
        "hosts": [
          "string"
        ],
        "nfType": "string",
        "nfSetsList": {
          nfSetIdList: ["string"]
        },
        "nfInstanceId": "3faf2bbc-6e4a-2828-a507-a14ef8e1bc7b",
        "nfServiceToRouteMapping": {
          "nfServiceToRoutesListMap": {
            "default": {
              "hosts": [
                "string"
              ],
              "destinations": [
                {
                  "destWeight": {
                    "weight": 0,

```

```

        "destination":{
            "host":"string",
            "port":{
                "number":0
            },
            "http2MaxRequests":0
        },
        "isRemoteScp":false,
        "ocscpc_load":0,
        "ocscpw_priority":0,
        "ocscpw_nf_instance_id":"string",
        "ocscpw_service_instance_id":"string"
    },
    "serviceSetIds":null
}
]
},
"nnrf-disc":{
    "hosts":[
        "string"
    ],
    "destinations":[
        {
            "destWeight":{
                "weight":0,
                "destination":{
                    "host":"string",
                    "port":{
                        "number":0
                    },
                    "http2MaxRequests":0
                },
                "isRemoteScp":false,
                "ocscpc_load":0,
                "ocscpw_priority":0,
                "ocscpw_nf_instance_id":"string",
                "ocscpw_service_instance_id":"string"
            },
            "serviceSetIds":null
        }
    ]
}
}
},
"metadata":{
    "name":"string",
    "namespace":"string"
},
"apiVersion":"string"
],
foreign:
[
    {
        "kind": "InterSCPRoutingInfo",

```



```

    "spec": {
      "hosts": ["udm1svc.default.svc.cluster.local:8080",
        "udm1svc.default.svc.cluster.local:8080-nudm-uecm",
        "192.168.2.143:8080-nudm-uecm", "192.168.2.143:8080"],
      "locality": "Loc1",
      "nfSetIdList": [],
      "nfInstanceIdList": ["9faf1bbc-6e4a-4454-a507-a14ef8e1bc5b"],
      "primaryDestinationList": [{
        "weight": 100,
        "destination": {
          "host": "ocscp-localscp-worker.scpsvc.svc.cluster.local",
          "port": {
            "number": 8000
          },
        },
        "http2MaxRequests": 100000
      }],
      "isRemoteScp": true,
      "ocscpc_load": 0,
      "ocscpw_priority": 0,
      "ocscpw_nf_instance_id": "3faf1bbc-6e4a-4454-a507-a14ef8e1bc5e",
      "ocscpw_service_instance_id": "f86b54b7-aef9-4c78-
b346-3bfb7f380811"
    },
    "secondaryDestinationList": {}
  },
  "metadata": {
    "name": "interScpRoutingInfo",
    "namespace": "scpsvc"
  },
  "apiVersion": "v1"
}
]
}

```

Example:**Successful Response1**

```

$ curl -X GET "http://10.75.236.84:32360/ocscp/scpc-configuration/v1/routing-
rules-r16?nfType=NRF" -H "accept: */*"
{
  "local": [
    {
      "spec": {
        "nfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a",
        "nfServiceToRouteMapping": {
          "nfServiceToRoutesListMap": {
            "default": {
              "hosts": [
                null
              ],
            },
            "destinations": [
              {
                "destinationInfo": {
                  "destination": {

```

```

        "port": {
          "number": 80
        }
      },
      "weight": 0,
      "ocscpw_priority": 0,
      "ocscpw_nf_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5a",
      "ocscpw_service_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5a",
      "ocscpc_load": 0
    }
  ]
},
"nnrf-nfm": {
  "hosts": [
    "nrf1svc.scpsvc.svc.cluster.local:8080-nnrf-nfm"
  ],
  "destinations": [
    {
      "destinationInfo": {
        "destination": {
          "host": "nrf1svc.scpsvc.svc.cluster.local",
          "port": {
            "number": 8080
          },
          "location": "MESH_EXTERNAL",
          "ports": [
            {
              "number": 8080,
              "protocol": "HTTP2",
              "name": "http2"
            }
          ]
        },
        "resolution": "DNS"
      },
      "weight": 5000,
      "ocscpw_priority": 0,
      "ocscpw_nf_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5a",
      "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b01",
      "ocscpc_load": 0
    }
  ]
},
"nnrf-disc": {
  "hosts": [
    "nrf1svc.scpsvc.svc.cluster.local:8080-nnrf-disc"
  ],
  "destinations": [
    {
      "destinationInfo": {
        "destination": {

```

```

        "host": "nrf1svc.scpsvc.svc.cluster.local",
        "port": {
            "number": 8080
        },
        "location": "MESH_EXTERNAL",
        "ports": [
            {
                "number": 8080,
                "protocol": "HTTP2",
                "name": "http2"
            }
        ],
        "resolution": "DNS"
    },
    "weight": 5000,
    "ocscpw_priority": 0,
    "ocscpw_nf_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5a",
    "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b02",
    "ocscpc_load": 0
    }
    }
    ]
    }
    },
    "hosts": [
        null
    ],
    "nfSetsList": {
        "nfSetIdList": [
            "Reg1"
        ]
    },
    "nfType": "NRF"
}
},
{
    "spec": {
        "nfInstanceId": "6faf1bbc-6e4a-2828-a507-a14ef8e1bc5b",
        "nfServiceToRouteMapping": {
            "nfServiceToRoutesListMap": {
                "default": {
                    "hosts": [
                        null
                    ],
                    "destinations": [
                        {
                            "destinationInfo": {
                                "destination": {
                                    "port": {
                                        "number": 80
                                    }
                                }
                            },
                            "weight": 0,

```

```

        "ocscpw_priority": 1,
        "ocscpw_nf_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5b",
        "ocscpw_service_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5b",
        "ocscpc_load": 0
    }
}
],
},
"nnrf-nfm": {
    "hosts": [
        "nrf2svc.scpsvc.svc.cluster.local:8080-nnrf-nfm"
    ],
    "destinations": [
        {
            "destinationInfo": {
                "destination": {
                    "host": "nrf2svc.scpsvc.svc.cluster.local",
                    "port": {
                        "number": 8080
                    },
                    "location": "MESH_EXTERNAL",
                    "ports": [
                        {
                            "number": 8080,
                            "protocol": "HTTP2",
                            "name": "http2"
                        }
                    ]
                },
                "resolution": "DNS"
            },
            "weight": 5000,
            "ocscpw_priority": 1,
            "ocscpw_nf_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5b",
            "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b01",
            "ocscpc_load": 0
        }
    ]
},
"nnrf-disc": {
    "hosts": [
        "nrf2svc.scpsvc.svc.cluster.local:8080-nnrf-disc"
    ],
    "destinations": [
        {
            "destinationInfo": {
                "destination": {
                    "host": "nrf2svc.scpsvc.svc.cluster.local",
                    "port": {
                        "number": 8080
                    },
                    "location": "MESH_EXTERNAL",

```

```

        "ports": [
            {
                "number": 8080,
                "protocol": "HTTP2",
                "name": "http2"
            }
        ],
        "resolution": "DNS"
    },
    "weight": 5000,
    "ocscpw_priority": 1,
    "ocscpw_nf_instance_id": "6faf1bbc-6e4a-2828-a507-
a14ef8e1bc5b",
    "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b02",
    "ocscpc_load": 0
    }
    }
    ]
    }
    },
    "hosts": [
        null
    ],
    "nfSetsList": {
        "nfSetIdList": [
            "Reg1"
        ]
    },
    "nfType": "NRF"
}
},
"foreign": []
}

```

Successful Response2:

```

$ curl -X GET "http://10.75.226.108:30701/ocscp/scpc-configuration/v1/routing-
rules-r16?nfType=AUSF&nfSetId=NONE" -H "accept: */*"
{
  "local": [
    {
      "spec": {
        "nfInstanceId": "8faf1bbc-6e4a-2828-a507-a14ef8e1bc5b",
        "nfServiceToRouteMapping": {
          "nfServiceToRoutesListMap": {
            "default": {
              "hosts": [
                "10.75.226.108:ip",
                "ausfsvc_fqdn"
              ]
            },
            "nausf-auth": {

```

```

    "hosts": [
      "nrf2svc.scpsvc.svc.cluster.local:8080-nausf-auth"
    ],
    "destinations": [
      {
        "destinationInfo": {
          "destination": {
            "host": "nrf2svc.scpsvc.svc.cluster.local",
            "port": {
              "number": 8080
            },
            "location": "MESH_EXTERNAL",
            "ports": [
              {
                "number": 8080,
                "protocol": "HTTP2",
                "name": "http2"
              }
            ]
          },
          "resolution": "DNS"
        },
        "weight": 5000,
        "ocscpw_priority": 1,
        "ocscpw_nf_instance_id": "8faf1bbc-6e4a-2828-a507-
a14ef8e1bc5b",
        "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b01",
        "ocscpc_load": 0
      }
    ]
  },
  "nausf-sorprotection": {
    "hosts": [
      "nrf2svc.scpsvc.svc.cluster.local:8080-nausf-sorprotection"
    ],
    "destinations": [
      {
        "destinationInfo": {
          "destination": {
            "host": "nrf2svc.scpsvc.svc.cluster.local",
            "port": {
              "number": 8080
            },
            "location": "MESH_EXTERNAL",
            "ports": [
              {
                "number": 8080,
                "protocol": "HTTP2",
                "name": "http2"
              }
            ]
          },
          "resolution": "DNS"
        },
        "weight": 5000,
        "ocscpw_priority": 1,

```

```

        "ocscpw_nf_instance_id": "8faf1bbc-6e4a-2828-a507-
a14ef8e1bc5b",
        "ocscpw_service_instance_id": "fe137ab7-740a-46ee-
aa5c-951806d77b02",
        "ocscpc_load": 0
    }
}
]
}
},
"nfSetsList": {},
"nfType": "AUSF"
}
}
],
"foreign": []
}

```

Failure cases

If the number of query parameters is greater than 3.

```

$ curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/routing-
rules-r16?nfType=NRF&nfServiceType=nnrf-
disc&nfIp=10.75.226.108&nfInstanceId=6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a" -H
"accept: */*"
Error response for above curl Request:
Response Code: 400
Response Status: BAD_REQUEST
Response Body : { "title": "Bad Request", "status": "400", "detail": "Maximum
3 Query Parameters are allowed, please refer to the User Guide",
"instance": "/ocscp/scpc-configuration/v1/routing-rules-r16?
nfType=NRF&nfServiceType=nnrf-
disc&nfIp=10.75.226.108&nfInstanceId=6faf1bbc-6e4a-4454-a507-a14ef8e1bc5a",
"cause": "INVALID_MSG_FORMAT" }
Response Headers :
  connection: keep-alive  content-type: application/problem+json  date: Wed30
Dec 2020 07:16:52 GMT  transfer-encoding: chunked

```

If any invalid combination of query parameters is requested.

```

$ curl -X GET "http://localhost:8081/ocscp/scpc-configuration/v1/routing-
rules-r16?nfType=NRF&nfServiceType=nnrf-nfm" -H "accept: */*"
Error response for above curl Request:
Response Code: 400
Response Status: BAD_REQUEST
Response Body: { "title": "Bad Request", "status": "400", "detail":
"Requested combination of Query Parameters is not allowed, please refer to
the User Guide",
"instance": "/ocscp/scpc-configuration/v1/routing-rules-r16?
nfType=NRF&nfServiceType=nnrf-nfm", "cause": "INVALID_MSG_FORMAT" }

```

Response Headers :

connection: keep-alive content-type: application/problem+json date: Wed30
Dec 2020 07:16:52 GMT transfer-encoding: chunked

2.19 Fetching Upgrade and Rollback Events

This section provides information about fetching upgrade and rollback event information.

Resources

The following table describes the resource name to retrieve the list of upgrade and rollback events.

Table 2-138 Upgrade and Rollback Resource Name

Resource Name	Resource URI	HTTP Method	Description
upgraderollbackevents	/ocscp/scpc-configuration/v1/upgraderollbackevents	GET	Retrieves a collection or list of upgrade and rollback events.

Resource Definition

This resource fetches upgrade or rollback events based on the query parameters.

If no query parameter is provided, all the events are returned.

Resource URI: /ocscp/scpc-configuration/v1/upgraderollbackevents

Table 2-139 URI Query Parameters Supported by the GET Method

Name	Data Type	P	Cardinality	Description	Allowed Values
serviceName	String	O	1	Name of the service	- scpc-audit - scpc-configuration - scpc-notification - scpc-subscription - scp-worker Example: scpc-audit
event	String	O	1	Event to be filtered	- Pre_Upgrade_Started - Pre_Upgrade_Completed - Pre_Upgrade_Failed - Post_Upgrade_Started - Post_Upgrade_Completed - Post_Upgrade_Failed - Pre_Rollback_Started - Pre_Rollback_Completed - Pre_Rollback_Failed - Post_Rollback_Started - Post_Rollback_Completed - Post_Rollback_Failed Example: Pre_Upgrade_Started

Table 2-139 (Cont.) URI Query Parameters Supported by the GET Method

Name	Data Type	P	Cardinality	Description	Allowed Values
sourceRelease	String	O	1	Source release version for performing upgrade and rollback. The convention to identify a release is as follows: 1.12.0 is identified as 101200 1.14.0 is identified as 101400	Any string followed the convention. Example: 101400
targetRelease	String	O	1	Target release version for performing upgrade and rollback. The convention to identify a release is as follows: 1.15.0 is identified as 101500 22.1.0 is identified as 221000	Any string followed the convention. Example: 221000

Table 2-140 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
array(UpgradeRollbackEvent)	M	1	200 OK	List of events matching criteria.

Example Response

```
$ curl -X GET "curl -X GET "http://10.75.224.18:32054/ocscp/scpc-configuration/v1/upgraderollbackevents" -H "accept: */*" -H "accept: */*"
[
  {
    "serviceName": "scpc-configuration",
    "event": "Pre_Upgrade_Started",
    "sourceRelease": "011200",
    "targetRelease": "011300",
    "creationTimestamp": "2021-05-26T00:36:40.000+00:00"
  },
  {
    "serviceName": "scpc-configuration",
```

```

    "event": "Pre_Upgrade_Completed",
    "sourceRelease": "011200",
    "targetRelease": "011300",
    "creationTimestamp": "2021-05-26T00:40:55.000+00:00"
  },
  {
    "serviceName": "scpc-configuration",
    "event": "Post_Upgrade_Started",
    "sourceRelease": "011200",
    "targetRelease": "011300",
    "creationTimestamp": "2021-05-26T00:50:23.000+00:00"
  },
  {
    "serviceName": "scpc-configuration",
    "event": "Post_Upgrade_Completed",
    "sourceRelease": "011200",
    "targetRelease": "011300",
    "creationTimestamp": "2021-05-26T01:02:02.000+00:00"
  },
  {
    "serviceName": "scpc-configuration",
    "event": "Upgrade_Completed",
    "sourceRelease": "011200",
    "targetRelease": "011300",
    "creationTimestamp": "2021-05-26T01:17:15.000+00:00"
  },
  {
    "serviceName": "scp-worker",
    "event": "Pre_Upgrade_Started",
    "sourceRelease": "011200",
    "targetRelease": "011300",
    "creationTimestamp": "2021-05-26T01:31:13.000+00:00"
  },
  {
    "serviceName": "scpc-subscription",
    "event": "Pre_Upgrade_Started",
    "sourceRelease": "011300",
    "targetRelease": "011400",
    "creationTimestamp": "2021-05-26T04:01:25.000+00:00"
  },
  {
    "serviceName": "scpc-subscription",
    "event": "Pre_Upgrade_Started",
    "sourceRelease": "011300",
    "targetRelease": "011400",
    "creationTimestamp": "2021-05-26T04:15:43.000+00:00"
  },
  {
    "serviceName": "scpc-subscription",
    "event": "Pre_Upgrade_Started",
    "sourceRelease": "011300",
    "targetRelease": "011400",
    "creationTimestamp": "2021-05-26T04:28:42.000+00:00"
  }
]

```

2.20 Updating HELM Configurable Parameters with REST APIs

This section provides REST API parameters required to update the Helm configurable options after SCP deployment.

Configuring Operations for PUT ALL Method

Request_Type: PUT ALL

URI: /ocscp/scpc-configuration/v1/tracing

Message:

```
[{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}]
```

Table 2-141 REST API: PUT ALL Method

Parameter	Description	DataType	Value Range	Mandatory
msgTracingEnabled	Enable/Disable jaeger trace	Boolean	True/False	Yes
msgJsonBodyEnabled	Enable/Disable body decoding in jaeger traces	Boolean	True/False	Yes
serviceName	Name of the service to which tracing is applied	String (scp-worker)	scp-worker	Yes

Success Response

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing*

Request Body:

```
[{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}]
```

Response:

```
[{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}]
```

Error Response

- Scenario 1: When the serviceName is anything else other than scp-worker
Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing*

Request Body:

```
[{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-workerbjasd"
}]
```

Response Header:

Status Code: 400 Bad

Request connection: keep-alive

content-type: application+problem/json

date: Mon, 15 Feb 2021 05:57:49 GMT

transfer-encoding: chunked

Response Body: { "title": "Invalid Service Name", "status": "400",
"cause": "Invalid Service Name" }

- Scenario 2: When the mandatory parameters are missing.

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing*

Request Body:

```
[{
  "bacd": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-workerbjasd"
}]
```

Response Body: { "status": "400", "error": "Bad Request" }

- Scenario 3: When the mandatory parameters' keys are incorrect.

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing*

Request Body:

```
[{
  "bacd": true,
  "msgJsonBodyEnabled": false,
  "serviceNameasd": "scp-worker"
}]
```

Response Body:

```
{ "status": "400", "error": "Bad Request" }
```

Configuring Operations for PUT Single Method

Request_Type: PUT

URI: */ocscp/scpc-configuration/v1/tracing/{serviceName}*

Table 2-142 Path Variable

Parameter	Description	Data Type	Value Range
serviceName	Name of the service to which tracing is applied.	String	scp-worker

Message:

```
{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}
```

Table 2-143 REST API: PUT Single Method

Parameter	Description	Data Type	Value Range	Mandatory
msgTracingEnabled	Enable/Disable jaeger trace	Boolean	True/False	Yes
msgJsonBodyEnabled	Enable/Disable json body trace	Boolean	True/False	Yes
serviceName	Name of the service to which tracing parameters are applied.	String	scp-worker	Yes

Success Response

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/scp-worker*

Request Body:

```
{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}
```

Response:

```
{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}
```

Error Response

- Scenario 1: When the serviceName is anything else other than scp-worker and the service name does not match with the servicename in URI.

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/scp-worker*

Request Body:

```
{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-workerbjasd"
}
```

Response Header:

Status Code: 400 Bad Request

Request connection: keep-alive

content-type: application+problem/json

date: Mon, 15 Feb 2021 05:57:49 GMT

transfer-encoding: chunked

Response body:

```
{ "title": "Invalid Service Name", "status": "400",
  "cause": "Invalid Service Name" }
```

- Scenario 2: When the mandatory parameters are missing.

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/scp-worker*

Request Body:

```
{
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}
or
{
  "msgTracingEnabled": true,
  "serviceName": "scp-worker"
}
or
{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
}
```

Response Body:

```
{ "status": "400", "cause": "<attribute-name> cannot be empty"
}
```

- Scenario 3: When the mandatory parameters' keys are incorrect.

Request URI: *http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/scp-worker*

Request Body:

```
{
  "bacd": true,
```

```
"msgJsonBodyEnabled": false,
"serviceName": "scp-worker"
}
Response body:

{ "status": "400", "error": "Bad Request" }
```

Configuring Operations for GET Method

Request_Type: GET

URI: */ocscp/scpc-configuration/v1/tracing/{serviceName}* and */ocscp/scpc-configuration/v1/tracing*

Message:

```
[{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}]
```

Table 2-144 REST API: GET Method

Parameter	Description	Data Type	Value Range
serviceName	Service Name to which tracing will be applied	String	scp-worker

Success Response

Request URI: */ocscp/scpc-configuration/v1/tracing/scp-worker*

Response body:

```
[{
  "msgTracingEnabled": true,
  "msgJsonBodyEnabled": false,
  "serviceName": "scp-worker"
}]
```

Error Response

Scenario 1: When the serviceName is anything else other than scp-worker

Request URI: */ocscp/scpc-configuration/v1/tracing/scp-worker-xyz*

Response body:

```
{ "title": "Invalid Service Name", "status": "400", "cause": "Invalid Service Name" }
```

Supported HTTP Status Code

- 200 - In case of success
- 400 - In case of Bad Request or invalid serviceName

- 404 - In case when serviceName is not found

Curl Commands

- GET:

```
curl -X GET -i 'http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/'
```

- PUT ALL:

```
curl -X PUT -H 'Content-Type: application/json' -i 'http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/' --data ' [{"msgTracingEnabled":true,"msgJsonBodyEnabled":false,"serviceName":"scp-worker"}]'
```

- PUT Single:

```
curl -X PUT -H 'Content-Type: application/json' -i 'http://<hostname>:<port>/ocscp/scpc-configuration/v1/tracing/scp-worker' --data '{"msgTracingEnabled":true,"msgJsonBodyEnabled":false,"serviceName":"scp-worker"}'
```

For information about HELM parameters, see the *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

2.21 Configuring Alternate NF Group

This section provides the following Alternate NF Group REST API configurations:

- Resource URIs for the alternatenfgroup resource type.
- Types of data model.
- URI query parameters supported by GET, PUT, and DELETE methods.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the alternatenfgroup resource type.

Table 2-145 alternatenfgroup Resource Type

Resource Name	Resource URI	HTTP Method	Mandatory (M) or Optional (O)	Query Parameters	Description
alternatenfgroup	/ocscp/scpc-configuration/v1/alternatenfgroup/configuration	GET	O	• serviceP • apiP	Retrieves the alternate NF group configuration data that are configured for corresponding query parameters. Displays both statically configured and alternate NF group data determined from NF profiles.

Table 2-145 (Cont.) alternatenfgroup Resource Type

Resource Name	Resource URI	HTTP Method	Mandatory (M) or Optional (O)	Query Parameters	Description
alternatenfgroup	/ocscp/scpc-configuration/v1/alternatenfgroup/configuration	PUT	O	NA	Configures the alternate NF group configuration data using the request body in the JSON format.
alternatenfgroup	/ocscp/scpc-configuration/v1/alternatenfgroup/configuration	DELETE	M	serviceProtoName	Removes the alternate NF group configuration data for corresponding query parameters.
alternatenfgroup	/ocscp/scpc-configuration/v1/alternatenfgroup/refreshdnssrvdata	PUT	O	NA	Refreshes the alternate NF group data when required.

Data Model

The following tables describe different data models required for configuring Alternate NF Group.

Table 2-146 AlternateNFGroupData

Name	Data Type	P	Cardinality	Range or Supported Value	Description
dnsSRVConfiguration	AlternateNFGroup Configuration	M	1	NA	The data type of the DNS SRV configuration.
array(dnsSrvRecords)	DNSSRVRecord	M	1	NA	This is the alternate NF group configuration data.

Table 2-147 AlternateNFGroupConfiguration

Name	Data Type	P	Cardinality	Range or Supported Value	Description
serviceProtoName	String	M	1	Extract and validate as per SCP FQDN regex	The service proto name of the producer NF. The DNS SRV format: _service._proto.name. ttl IN SRV priority weight port target. serviceProtoName represents _service._proto.name

Table 2-147 (Cont.) AlternateNFGroupConfiguration

Name	Data Type	P	Cardinality	Range or Supported Value	Description
apiPrefix	String	O	1	NA	This is used while constructing destination URI. If empty or null, then the string is provided.

Table 2-148 DNSSRVRecord

Name	Data Type	P	Cardinality	Range or Supported Value	Description
target	String	M	1	Validate as per SCP FQDN regex	Indicates the target NF type.
port	String	M	1	0-65535	Indicates the port number of the ipEndPoint attribute.
ttl	Long	O	1	30-86400 seconds	Determines the availability of data in the network and when the data can be removed. If the TTL value received is not within this range, then the default TTL value, which is 900s, is used as configured in the System Config table.
type	String	O	1	SRV	Identifies the record type.
dclass	String	O	1	IN	Defines DNS class values.
priority	Long	M	1	0-65535	Prioritizes the NF selection.
weight	Long	M	1	0-65535	Specifies a relative order or position for entries with the same priority. For more information, see RFC 2782.

Table 2-149 AlternateNFGroupRefreshData

Name	Data Type	P	Cardinality	Range or Supported Value	Description
refreshAll	String	O	1	true or false	Indicates whether all the alternate NF group data should be refreshed or not.

Table 2-149 (Cont.) AlternateNFGroupRefreshData

Name	Data Type	P	Cardinality	Range or Supported Value	Description
spnlist	Array	O	1	NA	Provides the list of service proto names to be refreshed.

Table 2-150 ProblemDetails

Name	Data Type	P	Cardinality	Description
type	String	O	1	Identifies the problem type.
title	String	M	1	Summarizes the problem type.
status	String	M	1	Indicates the HTTP status code for the occurrence of the problem type.
detail	String	M	1	Provides a description specific to the occurrence of the problem type.
instance	String	M	1	Identifies the specific occurrence of this problem type.
cause	String	M	1	Defines the application error cause specific to the occurrence of this problem type.

Request Body

The following table describes the AlternateNFGroupConfiguration data type.

Table 2-151 AlternateNFGroupConfiguration Data Type

Data Type	Description
AlternateNFGroupConfiguration	Indicates the data type of the DNS SRV configuration. For more information, see Table 2-147 .

Response Body

The response body data model varies based on the REST operation status. For more information, see the information provided in the subsequent tables.

Table 2-152 Response Body Data Type

Data Type	Description
DNSSRVData	This is the alternate NF group configuration data.
None	Empty body

Resource Definition

This section describes GET, PUT, and DELETE resource types supported by Alternate NF Group.

GET API

This resource fetches the alternate NF group configuration based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/alternatenfgroup/configuration

Request Body

There is no request body in GET Request API.

Table 2-153 URI Query Parameters Supported by the GET Method

Name	Data Type	P	Cardinality	Description
serviceProtoName	String	O	1	The service proto name of the producer NF.
apiPrefix	String	O	0..1	Optional path segments used to construct the {apiRoot} variable of the different API URIs as described in 3GPP 29.501.

Note

If none of the aforementioned query parameters are provided, all the user provisioned serviceProtoName data are returned.

Table 2-154 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
array(DNSSRVData)	M	1	200 OK	This is the alternate NF group configurations data.
ProblemDetails	M	1	400 BAD REQUEST	This data structure is sent if the query parameters validation fails.
ProblemDetails	M	1	404 NOT FOUND	This data structure is sent when no matching entry is found. For information about the ProblemDetails structure, see 3GPP TS 29.571.

Note

The GET request only retrieves the records provisioned by users.

The following examples are of successful and failed responses.

Success response:

```
curl -X GET "http://10.75.212.178:31147/ocscp/scpc-configuration/v1/alternatenfgroup/configuration?"
```

```
serviceProtoName=_http._tcp.nf2stub.scpsvc.svc" -H "accept: */*"
```

Response Body:

```
[{
  "dnsSRVConfiguration": {
    "serviceProtoName": "_http._tcp.nf2stub.scpsvc.svc",
    "apiPrefix": "USEast"
  },
  "dnsSrvRecords": [{
    "target": "nf2stub.scpsvc.svc",
    "port": 8080,
    "ttl": 86400,
    "type": "SRV",
    "dclass": "IN",
    "priority": 1,
    "weight": 60
  },
  {
    "target": "nf21stub.scpsvc.svc",
    "port": 8080,
    "ttl": 86400,
    "type": "SRV",
    "dclass": "IN",
    "priority": 20,
    "weight": 20
  },
  {
    "target": "nf22stub.scpsvc.svc",
    "port": 8080,
    "ttl": 86400,
    "type": "SRV",
    "dclass": "IN",
    "priority": 10,
    "weight": 20
  }
  ]
}]
```

Failure response: If the alternate NF group data is not configured.

```
curl -X GET "http://10.75.212.178:31147/ocscp/scpc-configuration/v1/
alternatenfgroup/configuration?
serviceProtoName=_http._tcp.nf23432stub.scpsvc.svc" -H "accept: */*"
```

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "Alternate NF Group Configuration not found against given query
parameters",
  "instance": "/ocscp/scpc-configuration/v1/alternatenfgroup/configuration?
serviceProtoName=_http._tcp.nf23432stub.scpsvc.svc",
  "cause": "DATA_NOT_FOUND"
}
```

PUT API

This resource adds the alternate NF group configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/alternatenfgroup/configuration

Table 2-155 Data Structures Supported by the PUT Request Body

Data Type	Description
AlternateNFGroupConfiguration	Indicates the data type of the DNS SRV configuration. For more information, see Table 2-147 .

Table 2-156 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
AlternateNFGroupConfiguration	M	1	200 OK	This response is used when an existing record is updated.
AlternateNFGroupConfiguration	M	1	201 CREATED	This response is used when a new entry is created.
ProblemDetails	M	1	400 BAD REQUEST	This response is used when the request body validation fails. For example, when serviceProtoName is missing in the request body. For information about the ProblemDetails structure, see 3GPP TS 29.571.

Note

The PUT request for Alternate NF Group is allowed only when the entry for that spn is already present in DNS SERVER otherwise, it gives a 404 Not Found error for such spn.

The following examples are of successful and failed responses.

Success response:

```
curl -X PUT "http://10.75.225.82:30361/ocscp/scpc-configuration/v1/alternatenfgroup/configuration" -H "accept: */*" -H "Content-Type: application/json" -d "{
  \"apiPrefix\": \"USEast\",
  \"serviceProtoName\": \"_http._tcp.nf2stub.scpsvc.svc\"
}"
```

Response:

```
{
  \"serviceProtoName\": \"_http._tcp.nf2stub.scpsvc.svc\",
  \"apiPrefix\": \"USEast\"
}
200 OK
```

Failure response: Invalid request body

```
curl -X PUT "http://10.75.225.82:31578/ocscp/scpc-configuration/v1/
alternatenfgroup/configuration" -H "accept: */*" -H "Content-Type:
application/json" -d "{
  "apiPrefix": "USEast",
  "serviceProtoName": "_http.npcf.rcklca63.we.pcf.5gc.oper.com"
}"
```

Response:

```
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Invalid request body received, please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/alternatenfgroup/configuration",
  "cause": "INVALID_REQUEST_BODY"
}
```

DELETE API

This resource removes the alternate NF group configuration based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/alternatenfgroup/configuration

Table 2-157 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Codes	Description
None			200 OK	This response is used when the query is successful.
Problem Details	M	1	404 NOT FOUND	This response is used when no matching entry is found. For information about the ProblemDetails structure, see 3GPP TS 29.571.
Problem Details	M	1	400 BAD REQUEST	This response is used when serviceProtoName is missing in the request. For information about the ProblemDetails structure, see 3GPP TS 29.571.

Note

The DELETE request body removes only the records provisioned by users.

The following examples are of successful and failed responses.

Success response:

```
curl -X DELETE "http://10.75.212.178:31147/ocscp/scpc-configuration/v1/
alternatenfgroup/configuration?
serviceProtoName=_http._tcp.nf2stub.scpsvc.svc" -H "accept: */*"
```

200 OK

Failure response: When no matching entry is found.

```
curl -X DELETE "http://10.75.212.178:31147/ocscp/scpc-configuration/v1/alternatenfgroup/configuration?serviceProtoName=_http._tcp.nf21232stub.scpsvc.svc" -H "accept: */*"

{
  "title": "Not Found",
  "status": "404",
  "detail": "Alternate NF Group Configuration not found against given query parameters",
  "instance": "/ocscp/scpc-configuration/v1/alternatenfgroup/configuration?serviceProtoName=_http._tcp.nf21232stub.scpsvc.svc",
  "cause": "DATA_NOT_FOUND"
}
```

REFRESH DNS Data API

This resource refreshes the alternate NF group configuration based on the request body parameters.

Resource URI: /ocscp/scpc-configuration/{version}/alternatenfgroup/refreshdnssrvdata

Table 2-158 Data Structures Supported by the PUT Request Body

Data Type	Description
AlternateNFGroupRefreshData	Indicates whether all the alternate NF group data should be refreshed or not. For more information, see Table 2-149 .

The following examples are of successful and failed responses.

Success response:

```
curl -X PUT "http://10.75.212.178:31147/ocscp/scpc-configuration/v1/alternatenfgroup/refreshdnssrvdata" -H "accept: */*" -H "Content-Type: application/json" -d "{
  \"refreshAll\": \"true\",
  \"spnlist\": [
  ]
}"

Response:
{
  \"refreshAll\": \"true\",
  \"spnlist\": []
}
200 OK
```


Failure response: Invalid request body

```
curl -X PUT "http://10.75.212.178:32137/ocscp/scpc-configuration/v1/alternatenfgroup/refreshdnssrvdata" -H "accept: */*" -H "Content-Type: application/json" -d '{"spnlist":[]}'

{
  "title": "Bad Request",
  "status": "400",
  "detail": "Invalid request body received, please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/alternatenfgroup/refreshdnssrvdata",
  "cause": "INVALID_REQUEST_BODY"
}
```

2.22 Configuring Server Header

This section describes the Server Header REST API configuration.

Resources

The following table describes the resource name to retrieve and update server header configurations in SCP.

Table 2-159 Resource Name

Resource Name	Resource URI	HTTP Method	Description
serverheader	/ocscp/scpc-configuration/{version}/serverheader	GET	Retrieves server header configurations in SCP.
serverheader	/ocscp/scpc-configuration/{version}/serverheader	PUT	Updates server header configurations in SCP.

Data Model

The following table describes different types of server header parameters.

Table 2-160 Types of Server Header Parameters

Field Name	Data Type	P	Default Value	Description
enableEnhanceServerHeaderBehavior	Boolean	M	false	Enables or disables the enhanced server header behavior. Possible values are: true, false, 1, or 0. The enhanced server header format: List of <NF-Type>-<NF-Instance Id> in reverse order of tried producers. Producer generated error: <NF-Type2>-<NF-Instance Id2> <NF-Type1>-<NF-Instance Id1> SCP generated error: SCP-<scp fqdn> <NF-Type2>-<NF-Instance Id2> <NF-Type1>-<NF-Instance Id1>
sideCarProxyServerHeader	List<String>	M	Empty List	Indicates the list of strings(eg: envoy,istio-envoy etc..)/string patterns(eg: e.*y, etc) to identify from server header value if error response is generated by side car proxy. If response received by SCP carries any of the configured strings or patterns in sideCarProxyServerHeader and response code matches with any of the configured sideCarProxyStatusCode, it will be treated as sidecar/service mesh generated error. Applicable to both enableEnhanceServerHeaderBehavior and enableEnhanceServerHeaderBehaviorV2. Note: This parameter allows the string regex patterns.

Table 2-160 (Cont.) Types of Server Header Parameters

Field Name	Data Type	P	Default Value	Description
addServerHeaderInProducerResponse	Boolean	M	false	Enables or disables the addition of a server header in producer NF-generated error responses by SCP during the default behavior (which means both <code>enableEnhanceServerHeaderBehavior</code> and <code>enableEnhanceServerHeaderBehaviorV2</code> are false). If set to TRUE - SCP will add a server header with the producer's information if a server header is not present in the error response received from the upstream peer. If set to FALSE - SCP will not add a server header with the producer's information if the server header is not present in the error response received from the upstream peer. The received response is passed as it is to the consumer. Possible values are: true, false, 1, or 0.
sideCarProxyStatusCode	List<Integer>	M	503	Indicates the list of server header status codes(503 etc.)/class of status code(5xx,4xx) to identify if error response is generated by side car proxy. If response received by SCP carries any of the configured strings or patterns in <code>sideCarProxyServerHeader</code> and response code matches with any of the configured <code>sideCarProxyStatusCode</code>, it will be treated as sidecar/service mesh generated error. Supported range or patterns are: 5xx and 4xx Values range: 400-599 Applicable to both <code>enableEnhanceServerHeaderBehavior</code> and <code>enableEnhanceServerHeaderBehaviorV2</code>.

Table 2-160 (Cont.) Types of Server Header Parameters

Field Name	Data Type	P	Default Value	Description
enableEnhanceServerHeaderBehaviorV2	Boolean	M	false	Enables or disables the new custom behavior. The behavior enabled is mutually exclusive with enableEnhanceServerHeaderBehavior.

Resource Definition**GET REST API**

URL: `curl -X GET "http://10.75.236.15:30862/ocscp/scpc-configuration/v1/serverheader" -H "accept: application/json"`

Request URI: `/ocscp/scpc-configuration/{version}/serverheader`

Example of a curl request:

```
curl -X GET "http://10.75.236.15:30862/ocscp/scpc-configuration/v1/serverheader"
-H "accept: application/json"
```

Response Data Structure:

Response of `"curl -X GET "http://10.75.236.15:30862/ocscp/scpc-configuration/v1/serverheader" -H "accept: application/json"`

```
{
  "enableEnhanceServerHeaderBehavior": false,
  "sideCarProxyServerHeader": [],
  "addServerHeaderInProducerResponse": false,
  "enableEnhanceServerHeaderBehaviorV2": false,
  "sideCarProxyServerHeaderStatusCode": ["503"]
}
```

PUT REST API

Request URI: `/ocscp/scpc-configuration/{version}/serverheader`

Example of a curl command:

```
curl -X PUT "http://10.75.236.15:30862/ocscp/scpc-configuration/v1/
serverheader" -H "accept: application/json" -H "Content-Type: application/
json" -d "
```

```
{"enableEnhanceServerHeaderBehavior":false,"sideCarProxyServerHeader":
```

```
["envoy"],"addServerHeaderInProducerResponse":false,"enableEnhanceServerH
eaderBehaviorV2":false,"sideCarProxyServerHeaderStatusCode":
["503","4xx"]}"
```

2.23 Configuring SBI Message Priority

This section provides Service Based Interface (SBI) Message Priority REST API configurations to support SCP behavior for SBI Messages priority headers received in message requests and responses.

Resources

The following table describes the resource name to retrieve, add, update, and remove SBI message priority information based on the query parameters.

Table 2-161 Resource Name

Resource Name	Resource URI	HTTP Method	Description
sbi-message-priority	/ocscp/scpc-configuration/v1/sbi-message-priority	GET	Retrieves the SBI Message Priority configured in SCP.
sbi-message-priority	/ocscp/scpc-configuration/v1/sbi-message-priority	PUT	Adds and updates the SBI Message Priority configured in SCP.
sbi-message-priority	/ocscp/scpc-configuration/v1/sbi-message-priority	PATCH	Updates or modifies the SBI Message Priority configured in SCP.
sbi-message-priority	/ocscp/scpc-configuration/v1/sbi-message-priority	DELETE	Removes the configured SBI Message Priority from SCP.

Data Model

Request Body

The following table describes the field names of the SbiMsgPriorityWrapper data type.

Table 2-162 SbiMsgPriorityWrapper

Field Name	Data Type	P	Default Value	Description
ruleName	String	M	default	Indicates the unique name for ruleName.
nfServiceName	String	M	*	Indicates all 3GPP defined NF Services as per 3GPP TS29.510.
httpMethods	String	M	*	Indicates the list of String HTTP methods, such as GET, POST, PUT, PATCH, DELETE, and OPTIONS.
messageType	String	M	*	Indicates the incoming request type. Possible values are: REQUEST or RESPONSE.
enableAssignPriority	boolean	O	false	Indicates whether the SMP header is available or not in the ingress message.
assignPriority	String	O	16	Indicates the "3gpp-Sbi-Message-Priority" header value. The value range is between 0 and 31.

Table 2-162 (Cont.) SbiMsgPriorityWrapper

Field Name	Data Type	P	Default Value	Description
enableOverridePriority	boolean	O	false	Indicates whether the SMP header is available or not in the ingress message.
overridePriority	String	O	16	Indicates the "3gpp-Sbi-Message-Priority" header value.

* indicates that the default value is applicable for all the possible message priority rules.

Response Body

The following table describes response body data models that varies based on the REST operation status.

Table 2-163 Response Body Data Type

Data Type	P	Cardinality	Response Codes	Description
array(SbiMsgPriorityWrapper)	M	1	200 OK	Indicates the list of Message Priorities (SbiMsgPriorityWrapper) that matches the criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than three query parameters are provided.

JSON Format

```
[
  {
    "ruleName": "default",
    "data": {
      "nfServiceName": "*",
      "httpMethods": [
        "*"
      ],
      "messageType": "*",
      "enableAssignPriority": false,
      "assignPriority": 16,
      "enableOverridePriority": false,
      "overridePriority": 16
    }
  }, {
    ....
    ...
  }
]
```

Resource Definition

GET REST API

This resource fetches the message priority (SBIMessagePriorityBean) based on the query parameters.

If no query parameter is provided, all the message priority are returned.

Resource URI: /ocscp/scpc-configuration/v1/sbi-message-priority

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-164 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
ruleName	String	O	Indicates the name of ruleName.
nfServiceName	String	O	Indicates all 3GPP defined NF Services as per 3GPP TS29.510 (callback and custom).
httpMethod	String	O	Indicates HTTP methods, such as GET, POST, PUT, PATCH, DELETE, and OPTIONS.
messageType	String	O	Indicates the message request or response. Possible values are: REQUEST or RESPONSE.

Note

The valid combination of query parameters is as follows:

- ruleName
- nfServiceName
- httpMethod
- messageType
- nfServiceName + httpMethod + messageType
- nfServiceName + httpMethod
- nfServiceName + messageType
- httpMethod + messageType

Table 2-165 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
array(SbiMsgPriorityWrapper)	M	1	200 OK	Indicates the list of Message Priority (SbiMsgPriorityWrapper) that matches the criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than 3 query parameters are provided.

Example

Successful response - 1

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority" -H "accept: application/json"
[
  {
    "ruleName": "default",
    "data": {
      "nfServiceName": "*",
      "httpMethods": [
        "*"
      ],
      "messageType": "*",
      "enableAssignPriority": false,
      "assignPriority": 16,
      "enableOverridePriority": false,
      "overridePriority": 16
    }
  },
  {
    "ruleName": "udm_test",
    "data": {
      "nfServiceName": "nudm_uecm",
      "httpMethods": [
        "GET",
        "POST"
      ],
      "messageType": "REQUEST",
      "enableAssignPriority": true,
      "assignPriority": 10,
      "enableOverridePriority": false,
      "overridePriority": -1
    }
  }
]
```

Successful response - 2

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority?nfServiceName=nudm_uecm" -H "accept: application/json"
[
  [
    {
      "ruleName": "udm_test",
      "data": {
        "nfServiceName": "nudm_uecm",
        "httpMethods": [
          "GET",
          "POST"
        ],
        "messageType": "REQUEST",
        "enableAssignPriority": true,
        "assignPriority": 10,
        "enableOverridePriority": false,
```



```

        "overridePriority": -1
    }
}
]

```

Successful response - 3

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority?nfServiceName=nudm_uecm&messageType=REQUEST" -H "accept:
application/json"
```

```

[
  {
    "ruleName": "udm_test",
    "data": {
      "nfServiceName": "nudm_uecm",
      "httpMethods": [
        "GET",
        "POST"
      ],
      "messageType": "REQUEST",
      "enableAssignPriority": true,
      "assignPriority": 10,
      "enableOverridePriority": false,
      "overridePriority": -1
    }
  }
]

```

Successful response - 4

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority?ruleName=default" -H "accept: application/json"
```

```

{
  "ruleName": "default",
  "data": {
    "nfServiceName": "*",
    "httpMethods": [
      "*"
    ],
    "messageType": "*",
    "enableAssignPriority": false,
    "assignPriority": 16,
    "enableOverridePriority": false,
    "overridePriority": 16
  }
}

```

PUT REST API

This resource adds or updates the SBI message priority configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/sbi-message-priority

Table 2-166 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
SbiMsgPriorityWrapper	M	1	200 OK	Indicates the SBI message priority configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.

Example

Successful response - 1

```
$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority" -H "accept: application/json" -H "Content-Type: application/
json" -d '{"ruleName\":\"nudm_test\",\"data\":
{\"nfServiceName\":\"nudm_uecm\",\"httpMethods\":
[\"PUT\",\"PATCH\"],\"messageType\":\"REQUEST\",\"enableAssignPriority\":true,
\"assignPriority\":10,\"enableOverridePriority\":true,\"overridePriority\":10}
}'
```

```
{
  "ruleName": "nudm_test",
  "data": {
    "nfServiceName": "nudm_uecm",
    "httpMethods": [
      "PUT",
      "PATCH"
    ],
    "messageType": "REQUEST",
    "enableAssignPriority": true,
    "assignPriority": 10,
    "enableOverridePriority": true,
    "overridePriority": 10
  }
}
```

200 OK

Successful response - 2

```
curl -X 'PUT' \
'http://<SCP configuration FQDN>:<port>/ocscp/scpc-configuration/v1/sbi-
message-priority' \
-H 'accept: */*' \
-H 'Content-Type: application/json' \
-d '{
  "ruleName": "nef_qos_test",
  "data": {
    "nfServiceName": "3gpp-as-session-with-qos",
    "httpMethods": [
      "GET",
      "POST"
    ]
  }
}'
```

```

    ],
    "messageType": "REQUEST",
    "enableAssignPriority": true,
    "assignPriority": 10,
    "enableOverridePriority": false,
    "overridePriority": 1
  }
}'

```

Failure case 1: Due to missing data object in the request body.

```
$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority" -H "accept: application/json" -H "Content-Type: application/
json" -d '{"ruleName\":"nudm_test\"}'
```

Response Body:

```

{
  "title": "Bad Request",
  "status": "400",
  "detail": "data Object is missing, Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/sbi-message-priority",
  "cause": "MANDATORY_IE_MISSING"
}

```

Failure case 2: Due to missing fields in request body.

```
$ curl -X PUT "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-
message-priority" -H "accept: application/json" -H "Content-Type: application/
json" -d '{"data\":
{"assignPriority\":10,"dNns\":"", "enableAssignPriority\":true,"enableOve
rridePriority\":true,"httpMethods\":
["PUT","PATCH"],"messageType\":"REQUEST","overridePriority\":10,"sNSS
AIs\":"", "ruleName\":"nudm_test\"}'
```

Response Body:

```

{
  "title": "Bad Request",
  "status": "400",
  "detail": "nfServiceName is missing, Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/sbi-message-priority",
  "cause": "MANDATORY_IE_MISSING"
}

```

PATCH REST API

This resource adds or updates the message priority configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/sbi-message-priority

Table 2-167 URI Query Parameters Supported by the PATCH method

Name	Data Type	P	Cardinality	Description
ruleName	String	M	1	Indicates the name of ruleName.
patchDocument	String	M	1	Indicates the patchDocument to be added to the request body. Example: [{"op":"replace","path":"/data/nfServiceName","value":"nudm_sdm"}, {"op":"replace","path":"/data/messageType","value":"REQUEST"}, {"op":"replace","path":"/data/httpMethods","value":["GET"]}]

Successful response

```
$ curl -X PATCH "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-  
message-priority?ruleName=udm_test1" -H "accept: application/json" -H "Content-  
Type: application/merge-patch+json" -d "[{"op":"replace","path":"/data/  
nfServiceName","value":"nudm_sdm"}, {"op":"replace","path":"/data/  
messageType","value":"REQUEST"}, {"op":"replace","path":"/data/  
httpMethods","value":["GET"]}]"
```

Table 2-168 PATCH Response Body

Data Type	P	Cardinality	Response Code	Description
SbiMsgPriorityWrapper	M	1	200 OK	Indicates the SBI message priority configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.

Response body

```
{  
  "ruleName": "udm_test1",  
  "data": {  
    "nfServiceName": "nudm_sdm",  
    "httpMethods": [  
      "GET"  
    ],  
    "messageType": "REQUEST",  
    "enableAssignPriority": true,  
    "assignPriority": 25,  
  }  
}
```

```

    "enableOverridePriority": false,
    "overridePriority": 16
  }
}

```

DELETE REST API

This resource removes the message priority configuration data based on query parameters.

Resource URI: /ocscp/scpc-configuration/v1/sbi-message-priority

Table 2-169 URI Query Parameters Supported by the DELETE method

Name	Data Type	P	Cardinality	Description
ruleName	String	O	1	Indicates the name of ruleName.

Note

ruleName is a valid combination of query parameters.

Table 2-170 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			204 OK	Returns only the response code in successful scenarios.
ProblemDetails	M	1	404 NOT FOUND	Returns when no matching entry is found.

Example

Successful response - 1

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-message-priority?ruleName=udm_test" -H "accept: application/json" */*
```

204 OK

Failure case 1: When no matching entry is found.

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sbi-message-priority?ruleName=udm_test" -H "accept: */*"
```

Response Body:

```

{
  "title": "Not Found",
  "status": "404",
  "detail": "Sbi Message Priority configuration data not found for the given
'ruleName': udm_test",
  "instance": "/ocscp/scpc-configuration/v1/sbi-message-priority/udm_test",

```

```
"cause": "DATA_NOT_FOUND"
}
```

2.24 Pod Overload Control Configurations

This section provides information about overload policy configurations to control and discard request messages sent to scp-worker.

2.24.1 Configuring Pod Overload Control Policy

This section provides information about configurations required for CPU and pending transactions onset threshold, abatement threshold, and abatement time for SCP-Worker.

Resources

The following table describes the resource name to retrieve, add, update, and remove the SCP-Worker Pod Overload Control Policy data based on the query parameters.

Table 2-171 Resource Name

Resource Name	Resource URI	HTTP Method	Description
pod-overload-control-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-control-policy	GET	Retrieves all the scp-worker Pod Overload Control Policy data configured in SCP.
pod-overload-control-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-control-policy	GET	Retrieves the scp-worker Pod Overload Control Policy data configured based on the threshold level in SCP when the threshold level is provided as query parameters, which is optional. If it is absent, then it retrieves all Overload Control Policy data configured in SCP.
pod-overload-control-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-control-policy	PUT	Adds or updates the scp-worker Pod Overload Control Policy data to SCP. Note: - You can add new customized threshold levels. - While configuring threshold levels, ensure that onset and abatement thresholds do not overlap with other threshold levels. - While configuring the WARN level, you should configure the lowest possible onset and abatement thresholds. - Ensure that the abatement threshold is lesser than the onset threshold.
pod-overload-control-policy	/ocscp/scpc-configuration/v1/pod-overload-control-policy	DELETE	Removes the configured scp-worker Pod Overload Control Policy data at the threshold level. Note: SCP does not allow the removal of default threshold levels: MINOR, MAJOR, WARN, and CRITICAL.

Data Model

Request Body

The following table describes the field names of the OverloadCtrlPolicyWrapper data type.

Table 2-172 OverloadCtrlPolicyWrapper

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the name of a threshold level, for example, MINOR, MAJOR, WARN, and CRITICAL.
data	WorkerPodOICtrlPolicy Data	M	Contains the cpuOverloadConfig data.

Table 2-173 WorkerPodOICtrlPolicyData

Field Name	Data Type	P	Description
cpuOverloadConfig	Object	M	Contains CPU overload control details.
pendingTransactionOverload Config	Object	C	Configures the parameters such as onSetThreshold, abatementThreshold, and abatementTimeInMilliseconds for all the threshold levels. Note: The pendingTransactionOverloadConfig parameter is optional, but if a user wants to keep this configuration, then all three parameters of this configuration should be provided.

Table 2-174 CpuOverloadConfig

Field Name	Data Type	P	Range	Description
onSetThreshold	Integer	M	2-100	Indicates the Pod CPU overload onset threshold value for a congestion level. Note: This value is the percentage of CPU utilization.
abatementThreshold	Integer	M	1-99	Indicates the congestion level abatement threshold value. Note: This value is the percentage of CPU utilization.
abatementTimeInMilliseconds	Integer	M	50 ms to 5000 ms	Indicates the congestion level abatement threshold time.

Table 2-175 pendingTransactionOverloadConfig

Field Name	Data Type	P	Range	Description
onSetThreshold	Integer	M	2-100	Indicates the Pod pending transaction overload onset threshold value for a congestion level. Note: This value is the percentage of the maximum allowed pending transactions supported by SCP.

Table 2-175 (Cont.) pendingTransactionOverloadConfig

Field Name	Data Type	P	Range	Description
abatementThreshold	Integer	M	1-99	Indicates the congestion level abatement threshold value. Note: This value is the percentage of the maximum allowed pending transactions supported by SCP.
abatementTimeInMilliseconds	Integer	M	50ms to 5000ms	Indicates the congestion level abatement threshold time.

Table 2-176 CpuOverloadConfig Threshold Level

Threshold Level	onSetThreshold	abatementThreshold	Abatement Time in millisecond
WARN	75	70	200
MINOR	82	76	200
MAJOR	87	83	200
CRITICAL	92	88	200

Note

These alarms are raised when the CPU utilization reaches the mentioned threshold level.

Table 2-177 pendingTransactionOverloadConfig Threshold Level

Threshold Level	onSetThreshold	abatementThreshold	Abatement Time in millisecond
WARN	75	70	200
MINOR	82	76	200
MAJOR	87	83	200
CRITICAL	92	88	200

Note

These alarms are raised when the pending transaction reaches the mentioned threshold level.

Resource Definition**GET REST API**

This resource fetches the scp-worker Pod Overload Control Policy data based on the query parameters.

If no query parameter is provided, all the Overload Control Policy data is returned.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-control-policy

Table 2-178 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the name of a threshold level, for example, MINOR, MAJOR, WARN, and CRITICAL. This is the threshold level for which the query is being triggered. This returns the overload Control policy configuration for the queried threshold level.

Table 2-179 Data Structures Supported by the GET ALL Response Body

Data Type	P	Cardinality	Response Code	Description
List<OverloadCtrlPolicyWrapper>	M	1	200 OK	Indicates the list of OverloadCtrlPolicyWrapper data.

Table 2-180 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
OverloadCtrlPolicyWrapper		1	200 OK	Indicates the OverloadCtrlPolicyWrapper configuration data. On successful response, returns the overload Control configuration data.
ProblemDetails	M	1	404 NOT FOUND	Returns error with problem details in case of any issue and if the query is unable to fetch the results. This data type can have 403 response code that indicates operation is not allowed.

Example

Successful response

```
{
  "thresholdLevel": "CRITICAL",
  "data": {
    "cpuOverloadConfig": {
      "onSetThreshold": 95,
      "abatementThreshold": 92,
      "abatementTimeInMilliseconds": 90
    },
    "pendingTransactionOverloadConfig": {
      "onSetThreshold": 95,
      "abatementThreshold": 92,
      "abatementTimeInMilliseconds": 50
    }
  }
}
```

```
    }  
  }  
}
```

PUT REST API

This resource adds or updates the scp-worker Pod Overload Control Policy configuration data using the request body.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-control-policy

Table 2-181 Data Structures Supported by the PUT Response Body

Name	P	Cardinality	Response Code	Description
OverloadCtrlPolicyWrapper	M	1	200 OK	Indicates the OverloadCtrlPolicyWrapper configuration data. On successful response, returns the overload Control configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571. This data type can have 403 response code that indicates operation is not allowed. Returns BAD request in case request is incorrect. In response, sends problemDetails as defined in 29.571.

Example

Successful response

```
curl -X PUT "http://10.75.227.181:30258/ocscp/scpc-configuration/V1/scp-worker/pod-overload-control-policy" -H "accept: */*" -H "Content-Type: application/json" -d "{\"data\":{\"cpuOverloadConfig\":{\"abatementThreshold\":96,\"abatementTimeInMilliseconds\":600,\"onSetThreshold\":97}},\"thresholdLevel\":\"Level1\"}"
```

```
Response Code: 201 CREATED
Response Body:
{
  "thresholdLevel": "Level1",
  "data": {
    "cpuOverloadConfig": {
      "onSetThreshold": 97,
      "abatementThreshold": 96,
      "abatementTimeInMilliseconds": 90
    },
    "pendingTransactionOverloadConfig": {
      "onSetThreshold": 97,
      "abatementThreshold": 96,
```

```
"abatementTimeInMilliseconds": 50
}
}
```

DELETE REST API

This resource removes the scp-worker Pod Overload Control Policy configuration data based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-control-policy

Table 2-182 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
thresholdLevel	String	M	1	Indicates the name of a custom threshold level. This is the threshold level for which the query is being triggered. This returns the overload Control policy configuration for the queried threshold level.

Note

- thresholdLevel is a valid combination of query parameters.
- Only custom threshold levels can be removed. The default levels, MINOR, MAJOR, WARN, and CRITICAL cannot be removed.

Table 2-183 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			204 OK	Returns the successful response in case deletion of record is successful.
ProblemDetails	M	1	404 NOT FOUND	Returns when no matching entry is found. This data type can have 403 response code that indicates operation is not allowed.

Example

Successful response

```
curl -X DELETE "http://10.75.227.181:30258/ocscp/scpc-configuration/V1/scp-worker/pod-overload-control-policy?thresholdLevel=LEVEL1" -H "accept: application/json"
```

Response code : 204 No Content

2.24.2 Configuring Pod Overload Action Policy

This section describes SCP-Worker Pod Overload Action Policy configurations based on the threshold level.

Resources

The following table describes the resource name to retrieve, add, update, and remove the SCP-Worker Pod Overload Action Policy data based on the query parameters.

Table 2-184 Resource Name

Resource Name	Resource URI	HTTP Method	Description
pod-overload-action-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy	GET	Retrieves all the scp-worker Pod Overload Action Policy data configured in SCP.
pod-overload-action-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy	GET	Retrieves the scp-worker Pod Overload Action Policy data configured based on the threshold level in SCP.
pod-overload-action-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy	PUT	Adds scp-worker Pod Overload Action Policy data to SCP. By default, this policy supports MINOR, MAJOR, and CRITICAL levels. Note: - You can add new customized threshold levels. - Do not configure the Warn threshold level.
pod-overload-action-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy	DELETE	Removes the configured scp-worker Pod Overload Action Policy data by the threshold level. Note: You cannot remove MINOR, MAJOR, and CRITICAL threshold levels.

Data Model

Request Body

The following table describes the field names of the OverloadActionWrapper data type.

Table 2-185 OverloadActionWrapper

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the name of a threshold level, for example, MINOR, MAJOR, and CRITICAL.
data	WorkerPodOlActionPolicyData	M	Contains the cpuOverloadConfig data.

Table 2-186 WorkerPodOIActionPolicyData

Field Name	Data Type	P	Range	Description
overloadAction	Enum	M	NO_ACTION and DISCARD	Indicates the overloadAction objects, for example: NO_ACTION and DISCARD. NO_ACTION indicates that no action is taken for the configured thresholdLevel. DISCARD indicates that the messages can be discarded based on the "3gpp-Sbi-Message-Priority" header or percentage. The default value is DISCARD.
errorResponsePercentage	Integer	M	100	Indicates the percentage of messages with error responses when overloadAction is DISCARD.
ErrorProfileConfiguration	Object	M	NA	Indicates error profiles to be used for responding with error responses if overloadAction is configured.
DiscardPolicyType	Enum	M	DISCARD_PERCENTAGE and SBI_MESSAGE_PRIORITY	Indicates the DiscardPolicyType objects. For example: DISCARD_PERCENTAGE and SBI_MESSAGE_PRIORITY. DISCARD_PERCENTAGE enables the discard message by percentage. SBI_MESSAGE_PRIORITY enables the discard message by priority.

Table 2-187 ErrorProfileConfiguration

Field Name	Data Type	P	Default Value	Description
errorCode	Integer	M	429	Indicates an HTTP status error code.
errorCause	String	M	NF_CONGESTION_RISK	Indicates the cause of the pod overload.
errorTitle	String	M	SCP is in pod overload congestion	Indicates the name of the error.
errorDescription	String	M	SCP <podName> pod is in <congestion level> pod overload congestion	Describes the cause of the error.
retryAfter	String	O	NA	Indicates the interval to start the next retry attempt.

Table 2-187 (Cont.) ErrorProfileConfiguration

Field Name	Data Type	P	Default Value	Description
redirectUrl	String	O	NA	Indicates the alternate URL to redirect request messages.

Resource Definition**GET REST API**

This resource fetches the scp-worker Pod Overload Action Policy data based on the query parameters.

If no query parameter is provided, all the Overload Action Policy data is returned.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy

Table 2-188 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the name of a threshold level, for example, MINOR, MAJOR, and CRITICAL. This is the threshold level for which the query is being triggered. This returns the overload action policy configuration for the queried threshold level.

Note

thresholdLevel is a valid combination of query parameters.

Table 2-189 Data Structures Supported by the GET ALL Response Body

Data Type	P	Cardinality	Response Code	Description
List<OverloadActionPolicyWrapper>		1	200 OK	Indicates the list of OverloadActionPolicyWrapper data.

Table 2-190 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
OverloadActionPolicyWrapper		1	200 OK	Indicates the OverloadActionPolicyWrapper configuration data. On successful response, returns the overload Action configuration data.

Example

Successful response

```
curl -X GET "http://10.75.227.181:30258/ocscp/scpc-configuration/v1/scp-
worker/pod-overload-action-policy?thresholdLevel=CRITICAL" -H "accept:
application/json"
```

Response code : 200 OK

Response data:

```
{
  "thresholdLevel": "CRITICAL",
  "data": {
    "overloadAction": "DISCARD",
    "errorResponsePercentage": 100,
    "errorProfileConfiguration": {
      "errorCode": 429,
      "errorCause": "",
      "errorTitle": "",
      "errorDescription": "",
    },
    "discardPolicyType": "DISCARD_PERCENTAGE"
  }
}
```

PUT REST API

This resource adds or updates the scp-worker Pod Overload Action Policy configuration data using the request body.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy

Table 2-191 Data Structures Supported by the PUT Response Body

Field Name	P	Response Codes	Description
OverloadActionWrapper	M	200 OK	Indicates the OverloadAction configuration data. On successful response, returns the overload Action configuration data.
ProblemDetails	M	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571. This data type can have 403 response code that indicates operation is not allowed. Returns BAD request in case request is incorrect. In response, sends probLemDetails as defined in 3GPP TS 29.571.

Example**Successful response**

```
curl -X PUT "http://10.75.227.181:30258/ocscp/scpc-configuration/V1/scp-
worker/pod-overload-action-policy" -H "accept: */*" -H "Content-Type:
application/json" -d "{\"data\":
{\"discardPolicyType\": \"DISCARD_PERCENTAGE\", \"errorProfileConfiguration\":
```

```
{\"errorCause\": \"\", \"errorCode\": 429, \"errorDescription\": \"string\", \"errorTitle\": \"string\", \"redirectUrl\": \"string\", \"retryAfter\": \"string\"}, \"errorResponsePercentage\": 67, \"overloadAction\": \"NO_ACTION\"}, \"thresholdLevel\": \"Level1\"}"
```

```
Response Code: 201 CREATED
Response Data:
{
  "thresholdLevel": "Level1",
  "data": {
    "overloadAction": "NO_ACTION",
    "errorResponsePercentage": 100,
    "errorProfileConfiguration": {
      "errorCode": 429,
      "errorCause": "",
      "errorTitle": "string",
      "errorDescription": "string",
      "retryAfter": "string",
      "redirectUrl": "string"
    },
    "discardPolicyType": "DISCARD_PERCENTAGE"
  }
}
```

DELETE REST API

This resource removes the scp-worker Pod Overload Action Policy configuration data based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy

Table 2-192 URI Query Parameters Supported by the DELETE Method

Field Name	Data Type	P	Cardinality	Description
thresholdLevel	String	M	1	Indicates the name of a threshold level, for example, MINOR, MAJOR, and CRITICAL. This is the threshold level for which the query is being triggered. This returns the overload Action policy configuration for the queried threshold level.

Note

thresholdLevel is a valid combination of query parameters.

Table 2-193 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			204 NO CONTENT	Returns the successful response in case deletion of record is successful.
ProblemDetails	M	1	404 NOT FOUND	Returns when no matching entry is found. This data type can have 403 response code that indicates operation is not allowed.

Example

Successful response

```
curl -X DELETE "http://10.75.227.181:30258/ocscp/scpc-configuration/v1/scp-worker/pod-overload-action-policy?thresholdLevel=LEVEL1" -H "accept: application/json"
```

Response Code: 204 No Content

2.24.3 Configuring Pod Overload Discard Policy

This section describes SCP-Worker Pod Overload Discard Policy configurations based on the threshold level.

Resources

The following table describes the resource name to retrieve, add, update, and remove the SCP-Worker Pod Overload Discard Policy data based on the query parameters.

Table 2-194 Resource Name

Resource Name	Resource URI	HTTP Method	Description
pod-overload-discard-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy	GET	Retrieves all the scp-worker Pod Overload Discard Policy data configured in SCP.
pod-overload-discard-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy	GET	Retrieves the scp-worker Pod Discard Policy data configured based on the threshold level in SCP.
pod-overload-discard-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy	PUT	Adds the scp-worker Pod Discard Policy data to SCP. By default, this policy supports MINOR, MAJOR, and CRITICAL levels. Note: - You can add new customized threshold levels. - Do not configure the Warn threshold level.

Table 2-194 (Cont.) Resource Name

Resource Name	Resource URI	HTTP Method	Description
pod-overload-discard-policy	/ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy	DELETE	Removes the configured scp-worker Pod Discard Policy data by the threshold level. Note: You cannot remove MINOR, MAJOR, and CRITICAL threshold levels.

Data Model**Request Body**

The following table describes the field names of the DiscardPolicyWrapper data type.

Table 2-195 DiscardPolicyWrapper

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the name of a threshold level, for example, MINOR, MAJOR, WARN, and CRITICAL.
data	WorkerPodOIDiscardPolicyData	M	Contains the cpuOverloadConfig data.

Table 2-196 DiscardPolicyConfig Threshold Level

Threshold Level	discardPercentage	sbiMsgPriorityDiscardForm
MINOR	20	16
MAJOR	50	8
CRITICAL	70	4

Table 2-197 WorkerPodOIDiscardPolicyData

Field Name	Data Type	P	Range	Description
discardPercentage	Integer	M	1-100	Indicates the percentage of messages to be discarded if the CPU overload threshold level exceeds the configured limit.
sbiMsgPriorityDiscardForm	Integer	M	0-31	Discards the requests having SBI message priority greater than or equal to the configured limit.

Resource Definition**GET REST API**

This resource fetches the scp-worker Pod Overload Discard Policy data based on the query parameters.

If no query parameter is provided, all the Discard Policy data is returned.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy

Table 2-198 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
thresholdLevel	String	M	Indicates the name of a threshold level, for example, MINOR, MAJOR, WARN, and CRITICAL. This is the threshold level for which the query is being triggered. This returns the overload Discard policy configuration for the queried threshold level.

Table 2-199 Data Structures Supported by the GET ALL Response Body

Data Type	P	Cardinality	Response Code	Description
List<DiscardPolicyWrapper>	M	1	200 OK	Indicates the list of DiscardPolicyWrapper data.

Table 2-200 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
DiscardPolicyWrapper	M	1	200 OK	Indicates the DiscardPolicyWrapper configuration data. On successful response, returns the overload Discard configuration data.
ProblemDetails	M	1	404 NOT FOUND	Returns error with problem details in case of any issue and if the query is unable to fetch the results. This data type can have 403 response code that indicates operation is not allowed.

Example

Successful response

```
curl -X GET "http://10.75.227.181:30258/ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy?thresholdLevel=CRITICAL" -H "accept: application/json"
```

Response Code: 200 OK

Response Body:

```
{
  "thresholdLevel": "CRITICAL",
  "data": {
    "discardPercentage": 30,
    "sbMsgPriorityDiscardFrom": 4
  }
}
```

```
}  
}
```

PUT REST API

This resource adds or updates the scp-worker Pod Overload Discard Policy configuration data using the request body.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy

Table 2-201 Data Structures Supported by the PUT Response Body

Field Name	P	Response Codes	Description
DiscardPolicyWrapper	M	200 OK	Indicates the DiscardPolicy configuration data. On successful response, returns the overload Discard configuration data.
ProblemDetails	M	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571. This data type can have 403 response code that indicates operation is not allowed. Returns BAD request in case request is incorrect. In response, sends probLemDetails as defined in 29.571.

Example

Successful response

```
curl -X PUT "http://10.75.227.181:30258/ocscp/scpc-configuration/V1/scp-worker/pod-overload-discard-policy" -H "accept: */*" -H "Content-Type: application/json" -d "{\"data\": {\"discardPercentage\":40,\"sbiMsgPriorityDiscardFrom\":19},\"thresholdLevel\":\"LEVEL1\"}"
```

```
Response Code: 201 OK  
Response Body:  
{  
  "thresholdLevel": "LEVEL1",  
  "data": {  
    "discardPercentage": 40,  
    "sbiMsgPriorityDiscardFrom": 19  
  }  
}
```

DELETE REST API

This resource removes the scp-worker Pod Overload Discard Policy configuration data based on the query parameters.

Resource URI: /ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy

Table 2-202 URI Query Parameters Supported by the DELETE Method

Field Name	Data Type	P	Cardinality	Description
thresholdLevel	String	M	1	Indicates the name of a threshold level, for example, MINOR, MAJOR, WARN, and CRITICAL. This is the threshold level for which the query is being triggered. This returns the overload Discard policy configuration for the queried threshold level.

Note

thresholdLevel is a valid combination of query parameters.

Table 2-203 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			200 OK	Returns the successful response in case deletion of record is successful.
ProblemDetails	M	1	404 NOT FOUND	Returns when no matching entry is found. This data type can have 403 response code that indicates operation is not allowed.

Example

Successful response

```
curl -X DELETE "http://10.75.227.181:30258/ocscp/scpc-configuration/v1/scp-worker/pod-overload-discard-policy?thresholdLevel=LEVEL1" -H "accept: application/json"
```

Response Code: 204 No Content

2.25 Configuring SEPP InterPlmn Info

This section provides SEPP InterPlmn Info REST API configurations to enable SCP integration with Security Edge Protection Proxy (SEPP) to route 5G Service Based Interface (SBI) roaming subscriber traffic outside the network to the required Public Land Mobile Network (PLMN).

Resources

The following table describes the resource name to retrieve, add, update, and remove SEPP Info based on the query parameters.

Table 2-204 Resource Name

Resource Name	Resource URI	HTTP Method	Description
sepp-config	/ocscp/scpc-configuration/v1/sepp-config	GET	Retrieves all the SEPP Info configured list at SCP or specific records based on the query parameters.
sepp-config	/ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}	GET	Retrieves SEPP Info records based on nfInstanceId as a path variable.
sepp-config	/ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}	PUT	Adds or updates SEPP Info details configured in SCP.
sepp-config	/ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}	PATCH	Updates or modifies SEPP Info details configured in SCP.
sepp-config	/ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}	DELETE	Removes the configured SEPP Info details based on nfInstanceId.

Data Model

Request Body

The following table describes the field names of the InterPlmnRoutingInfo data type.

Table 2-205 InterPlmnRoutingInfo

Field Name	Data Type	P	Description
nfInstanceId	String	M	Specifies the identity of the NF instance for which routing information is fetched.
mcc	String	M	Indicates the mobile country code. It is a three digit number ranging from 0 to 9.
mnc	String	M	Indicates the mobile network code. It can be of two or three digits ranging from 0 to 9.
http	String	M	Enables the HTTP connection. The value can be 0 to 65535.
https	String	M	Enables the HTTPS connection. The value can be 0 to 65535.

Response Body

The following table describes response body data models that varies based on the REST operation status.

Table 2-206 Response Body Data Type

Data Type	P	Cardinality	Response Codes	Description
array(InterPlmnRoutingInfo)	M	1	200 OK	Indicates the list of SEPP Info (InterPlmnRoutingInfo) matching criteria.
ProblemDetails	M	1	404 NOT FOUND	Returns when the data is not found for given query parameters.

JSON Format

```
[
  {
    "nfInstanceId" : "1faf1bbc-6e4a-4454-a507-a14ef8e1bc6a",
    "seppInfo": {
      "remotePlmnList": [{
        "mcc": "327",
        "mnc": "15"
      }, {
        "mcc": "328",
        "mnc": "16"
      }, {
        "mcc": "329",
        "mnc": "17"
      }
    ],
    "seppPorts": {
      "http": "8000",
      "https": "8090"
    }
  },
  {
    ....
  }
]
```

Resource Definition

GET REST API

This resource fetches the SEPP Info details (InterPlmnRoutingInfo) based on the query parameters.

If no query parameter is provided, all the SEPP info details are returned.

Resource URI: /ocscp/scpc-configuration/v1/sepp-config

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-207 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Description
nfInstanceId	String	O	Specifies the identity of the NF instance for which routing information is fetched.

Note

nfInstanceId is a valid combination of query parameter or path variable.

Table 2-208 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
array(InterPlmnRoutingInfo)	M	1	200 OK	Indicates the list of SEPP Info (InterPlmnRoutingInfo) or specific record based on the query parameters.
ProblemDetails	M	1	404 NOT FOUND	Returns when the data is not found for given query parameters.

Example

Successful response - 1

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sepp-config" -H "accept: application/json"
[
  {
    "nfInstanceId": "1faf1bbc-6e4a-4454-a507-a14ef8e1bc6a",
    "seppInfo": {
      "remotePlmnList": [{
        "mcc": "327",
        "mnc": "15"
      }, {
        "mcc": "328",
        "mnc": "16"
      }],
      "seppPorts": {
        "http": "8000",
        "https": "8090"
      }
    }
  }
]
```

Successful response - 2

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sepp-config?nfInstanceId=1faf1bbc-6e4a-4454-a507-a14ef8e1bc6a" -H "accept:
```



```
application/json"

{
  "nfInstanceId": "1faf1bbc-6e4a-4454-a507-a14ef8e1bc6a",
  "seppInfo": {
    "remotePlmnList": [{
      "mcc": "327",
      "mnc": "15"
    }, {
      "mcc": "328",
      "mnc": "16"
    }],
    "seppPorts": {
      "http": "8000",
      "https": "8090"
    }
  }
}
```

Successful response - 3

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sepp-
config/1faf1bbc-6e4a-4454-a507-a14ef8e1bc6a" -H "accept: application/json"
```

```
{
  "nfInstanceId": "1faf1bbc-6e4a-4454-a507-a14ef8e1bc6a",
  "seppInfo": {
    "remotePlmnList": [{
      "mcc": "327",
      "mnc": "15"
    }, {
      "mcc": "328",
      "mnc": "16"
    }],
    "seppPorts": {
      "http": "8000",
      "https": "8090"
    }
  }
}
```

Failure case 1

```
$ curl -X GET "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sepp-
config?nfInstanceId=4faf1bbc-5e4a-4454-a507-a14ef8e1bc6a" -H "accept:
application/json"
```

Response Body:

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "Sepp Info configuration data not found against given query
parameter(s), Please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/sepp-config?"
}
```

```

nfInstanceId=4faf1bbc-5e4a-4454-a507-a14ef8e1bc6a",
  "cause": "DATA_NOT_FOUND"
}

```

PUT REST API

This resource adds or updates the SEPP Info configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}

Table 2-209 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
InterPlmnRoutingInfo	M	1	200 OK	Indicates the InterPlmn RoutingInfo configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571 section 5.2.4.1.

Example

Successful response

```

$ curl -X PUT "http://10.75.226.108:32466/ocscp/scpc-configuration/v1/sepp-config/2faf1bbc-6e4a-4454-a507-a14ef8e1bc6a" -H "accept: */*" -H "Content-Type: application/json" -d "{ \"nfInstanceId\": \"9faf1bbc-6e4a-4454-a507-aef01a101a06\", \"seppInfo\": { \"remotePlmnList\": [{ \"mcc\": \"267\", \"mnc\": \"321\" }], \"seppPorts\": { \"http\": \"8000\", \"https\": \"4430\" } } }"

```

```

{
  "nfInstanceId": "2faf1bbc-6e4a-4454-a507-a14ef8e1bc6a",
  "seppInfo": {
    "remotePlmnList": [{
      "mcc": "267",
      "mnc": "321"
    }],
    "seppPorts": {
      "http": "8000",
      "https": "4430"
    }
  }
}

```

200 OK

PATCH REST API

This resource adds or updates the SEPP Info configuration using the request body.

Resource URI: /ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}

Table 2-210 URI Query Parameters Supported by the PATCH method

Name	Data Type	P	Cardinality	Description
nfInstanceId	String	M	1	Specifies the identity of the NF instance for which routing information is fetched.
patchDocument	String	M	1	Indicates the patchDocument to be sent. Example: [{"op":"replace","path":"/seppInfo/seppPorts/http","value":"8000"} {"op":"replace","path":"/seppInfo/seppPorts/https","value":"9000"}]

Successful response: Request Body

```
$ curl -X PATCH "http://10.75.226.108:32551/ocscp/scpcconfiguration/v1/sepp-config/2faf1bbc-6e4a-4454-a507-a14ef8e1bc6a" -H "accept: application/json" -H "Content-Type: application/merge-patch+json" -d "[{"op":"replace","path":"/seppInfo/seppPorts/https","value":"9010"}, {"op":"replace","path":"/seppInfo/seppPorts/http","value":"9100"}]"
```

Table 2-211 PATCH Response Body

Data Type	P	Cardinality	Response Code	Description
InterPlmnRoutingInfo	M	1	200 OK	Indicates the InterPlmn RoutingInfo configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571 section 5.2.4.1.

Response body

```
{
  "nfInstanceId": "2faf1bbc-6e4a-4454-a507-a14ef8e1bc6a",
  "seppInfo": {
    "remotePlmnList": [{
      "mcc": "327",
      "mnc": "15"
    }, {
      "mcc": "328",
      "mnc": "16"
    }],
    "seppPorts": {
      "http": "9010",
      "https": "9000"
    }
  }
}
```

```
}
}
```

DELETE REST API

This resource removes the SEPP Info configuration data based on query parameters.

Resource URI: /ocscp/scpc-configuration/v1/sepp-config/{nfInstanceId}

Table 2-212 URI Query Parameters Supported by the DELETE method

Name	Data Type	P	Cardinality	Description
nfInstanceId	String	O	1	Specifies the identity of the NF instance for which routing information is fetched.

Note

nfInstanceId is a valid combination of query parameter or path variable.

Table 2-213 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Code	Description
None			204 OK	In successful scenarios, only response code is returned.
ProblemDetails	M	1	404 NOT FOUND	When no matching entry is found.

Example

Successful response - 1

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sepp-config/2faf1bbc-6e4a-4454-a507-a14ef8e1bc6a" -H "accept: application/json" */**
```

204 OK

Failure case 1: When no matching entry is found.

```
$ curl -X DELETE "http://10.75.226.108:32551/ocscp/scpc-configuration/v1/sepp-config/4faf1bbc-5e4a-4454-a507-a14ef8e1bc6a" -H "accept: application/json"
```

Response Body:

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "Sepp Info configuration data not found against given query parameter(s), Please refer to the User Guide",
  "instance": "/ocscp/scpc-configuration/v1/sepp-config4faf1bbc-5e4a-4454-a507-a14ef8e1bc6a",
```

```
"cause": "DATA_NOT_FOUND"
}
```

2.26 Configuring App Routing Options

The following section provides configuration details about routing options applicable for Mediation.

Resources

The following table describes the resource name to retrieve, add, update, and remove App routing options.

Table 2-214 Resource Name

Resource Name	Resource URI	HTTP Method	Description
approutingoptions	/ocscp/scpc-configuration/{version}/approutingoptions	GET ALL	Retrieves all configured App routing options.
approutingoptions	/ocscp/scpc-configuration/{version}/approutingoptions/{appname}	GET	Retrieves the configured App routing options specified using the field appname. Note: Routing options can be specified only for Mediation, therefore only "mediation" appname is supported.
approutingoptions	/ocscp/scpc-configuration/{version}/approutingoptions/{appname}	PUT	Updates the configured App routing options specified using the field appname. Note: You cannot create new routing options but you can only update them. Routing options for appname Mediation can only be updated.
approutingoptions	/ocscp/scpc-configuration/{version}/approutingoptions/{appname}	DELETE	Removes the configured App routing options specified using the appname field. Note: DELETE method is not supported.

Data Model

The following table describes the supported data type.

Table 2-215 approutingoptions

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Value
appName	String	M	1	Indicates the name of the application for which the routing option has to be configured.	mediation	mediation

Table 2-215 (Cont.) approutingoptions

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Value
routingOptions	JSON	M	1	Indicates the JSON structure to store the routing options.	NA	{ "appName": "mediation", "routingOptions": { "v1": { "retry": true, "maxRetryAttempts": 2, "responseTimeout": "1s", "exceptionErrorResponse": [{ "statusCode": ["DEFAULT"], "action": "continue_processing" }] } } }

Table 2-216 approutingOptions

Field Name	Data Type	P	Description	Default Value
retry	boolean	O	Indicates whether to attempt retry or not when the routing fails.	true
maxRetryAttempts	INT	O	Indicates the maximum number of retry attempts. Minimum value is 1, Maximum value is 0.	2
responseTimeout	String	O	Indicates the allotted time to respond to a message request. This value must be in seconds.	1s

Table 2-216 (Cont.) approutingOptions

Field Name	Data Type	P	Description	Default Value
exceptionErrorResponses	JSON	O	Specifies the methods to handle exceptions in case of routing failures. Note: exceptionErrorResponses is used to specify how exceptions are to be handled. By default, one exception configuration is created during deployment where statusCode is DEFAULT and action is continue_processing, this means, if during mediation invocation, if any exception occurs it is continue_processing. To change this behavior, you can create own exceptionConfiguration by specifying action on specific statusCodes.	"exceptionErrorResponses": [{ "statusCode": ["DEFAULT"] , "action": "continue_processing" }]

Table 2-217 exceptionErrorResponses

Field Name	Data Type	P	Cardinality	Description	Default Value
statusCode	List<String>	M	1..N	Indicates the list of status codes that matches with the status code received from the application. The required action specified by action field is taken.	HTTP Status Codes, HTTP Status with other defined custom status (RESPONSE_TIMEOUT and CONNECTION_FAILURE)
action	String	M	1	Indicates the action to be taken when the above mentioned status code is received.	send_error_response: Error to be sent if the received status code from application is present in the statusCode list. continue_processing: Continue with processing of message if the received status code from application is present in the statusCode list.
errorProfileConfiguration	JSON	C (mandatory when action=send_error_response)	1	The error profile to be sent when the action to perform is send_error_response when the statusCode matches.	NA

Table 2-218 errorProfileConfiguration

Field Name	Data Type	P	Description	Default Value
errorCode	Int	O	Indicates configurable error codes to be sent by SCP to consumer NFs.	Valid HTTP status codes include 5xx and 4xx error codes, as well as custom error codes such as DEFAULT, RESPONSE_TIMEOUT, and CONNECTION_FAILURE. For example, 500, 502, 400, 404 and so on.

Table 2-218 (Cont.) errorProfileConfiguration

Field Name	Data Type	P	Description	Default Value
errorCause	String	O	Indicates the error cause that is specific to the occurrence of the problem.	NA
errorTitle	String	O	Indicates the title of the error.	NA
errorDescription	String	O	Indicates an explanation specific to the occurrence of the problem.	NA
retryAfter	String	C	Indicates the retry interval.	Mandatory if ERROR code is 3xx series and action is send_error_response. The time unit supported is seconds. Example: 2s, 3s, and so on.
redirectUrl	String	C	Indicates the AbsoluteURL of the resource to which the message is redirected to.	Mandatory if ERROR code is 3xx series and action is send_error_response.

Default Routing Options

```

{
  "appName": "mediation",
  "routingOptions": {
    "retry": true,
    "maxRetryAttempts": "2",
    "serviceTimeout": "1s",
    "exceptionErrorResponses": [
      {
        "statusCode": [
          "DEFAULT"
        ],
        "action": "continue_procesing"
      }
    ]
  }
}

```

Request or Response Body

The following table describes response body based on the REST operation status.

RoutingOptions

```

{
  "appname": "mediation"
  "routingOptions":
  {
    "retry": true,
    "maxRetryAttempts": 4,
    "serviceTimeout": 5 s,
    "exceptionErrorResponses": [{
      "statusCode": ["501", "504", "connection_failure",

```



```
"response_timeout", "SERVICE_UNAVAILABLE" ]
  "action": "send_error",
  "errorProfileConfiguration": {
    "errorCode": 503,
    "errorCause": "MEDIATION_NOT_REACHABLE",
    "errorTitle": "Mediation service unreachable",
    "errorDescription": "Mediation service is not reachable",
    "retryAfter": "5",
    "redirectUrl": ""
  }
}
}]
}
```

Resource Definition

GET REST API

This resource retrieves routing options for all the applications.

Resource URI: /ocscp/scpc-configuration/{version}/approutingoptions

The following table describes the data structure supported by the GET method on this resource.

Table 2-219 Data Structure Supported by the GET Method

Data Type	P	Cardinality	Response Codes	Description
approutingoptions	M	1..N	200 OK	Routing options configuration for the Application.

This resource retrieves routing options for the application specified by appname.

Resource URI: /ocscp/scpc-configuration/{version}/approutingoptions/{appname}

The following table describes the path parameters supported by the GET method on this resource.

Table 2-220 Path Parameters Supported by the GET Method

Name	Data Type	P	Description
appname	String	M	Fetches configurations on app name. The supported value is "mediation".

Table 2-221 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
approutingoptions	M	1	200 OK	Indicates the routing options configuration for the Application.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Success response for GET and GET ALL

```
curl -X GET "http://10.75.175.233:30953/ocscp/scpc-configuration/v1/
approutingoptions" -H "accept: application/json"
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:08:49 GMT
```

```
[
  {
    "appName": "mediation",
    "routingOptions": {
      "retry": false,
      "maxRetryAttempts": 6,
      "responseTimeout": "10",
      "exceptionErrorResponses": [
        {
          "statusCode": [
            "DEFAULT"
          ],
          "action": "continue_processing"
        },
        {
          "statusCode": [
            "501"
          ],
          "action": "send_error_response",
          "errorProfileConfiguration": {
            "errorCode": 501,
            "errorCause": "NOT FOUND",
            "errorTitle": "NOT FOUND ",
            "errorDescription": "NOT FOUND",
            "retryAfter": "",
            "redirectUrl": ""
          }
        }
      ]
    }
  }
]
```

Success response 2

```
curl -X GET "http://10.75.175.233:30953/ocscp/scpc-configuration/v1/
approutingoptions/mediation" -H "accept: application/json"
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:08:49 GMT
```

```

{
  "appName": "mediation",
  "routingOptions": {
    "retry": false,
    "maxRetryAttempts": 6,
    "responseTimeout": "10",
    "exceptionErrorResponses": [
      {
        "statusCode": [
          "DEFAULT"
        ],
        "action": "continue_processing"
      },
      {
        "statusCode": [
          "501"
        ],
        "action": "send_error_response",
        "errorProfileConfiguration": {
          "errorCode": 501,
          "errorCause": "NOT FOUND",
          "errorTitle": "NOT FOUND ",
          "errorDescription": "NOT FOUND",
          "retryAfter": "",
          "redirectUrl": ""
        }
      }
    ]
  }
}

```

Failure response

```
curl -X GET "http://10.75.175.233:30953/ocscp/scpc-configuration/v1/approutingoptions/med" -H "accept: application/json"
```

```

HTTP/1.1 404 Not Found
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:08:49 GMT

```

```

{
  "title": "Not Found",
  "status": "404",
  "detail": "App Routing Options response data not found against given query parameter(s)",
  "instance": "/ocscp/scpc-configuration/v1/approutingoptions/med",
  "cause": "DATA_NOT_FOUND"
}

```

PUT REST API

This resource configures routing options for the application.

Resource URI: /ocscp/scpc-configuration/{version}/approutingoptions/{appname}

Table 2-222 Data Structures Supported by the PUT Request Body on this Resource

Data Type	P	Cardinality	Description
approutingoptions	M	1	Indicates the routing options configuration for the Application.

Table 2-223 Data Structures Supported by the PUT Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
approutingoptions	M	1	200 OK	Indicates the routing options configuration for the Application.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.

Example

Success response

```
curl -X PUT "http://10.75.175.233:30953/ocscp/scpc-configuration/v1/
approutingoptions/mediation" -H "accept: application/json" -H "Content-Type:
application/json" -d '{"appName\":\"mediation\",\"routingOptions\":
{"retry\":false,\"maxRetryAttempts\":6,\"responseTimeout\":\"10\",\"exception
ErrorResponses\":[{"statusCode":
["DEFAULT"],\"action\":\"continue_processing\"},{\"statusCode\":
[\"501\"],\"action\":\"send_error_response\",\"errorProfileConfiguration\":
{"errorCode\":501,\"errorCause\":\"NOT FOUND\",\"errorTitle\":\"NOT FOUND
\",\"errorDescription\":\"NOT
FOUND\",\"retryAfter\":\"\",\"redirectUrl\":\"\"}]}}']}]}'
```

```
HTTP/1.1 201 Ok
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:08:49 GMT
```

```
{
  "appName": "mediation",
  "routingOptions": {
    "retry": false,
    "maxRetryAttempts": 6,
    "responseTimeout": "10",
    "exceptionErrorResponses": [
      {
        "statusCode": [
          "DEFAULT"
        ],
        "action": "continue_processing"
      }
    ]
  }
}
```

```

    },
    {
      "statusCode": [
        "501"
      ],
      "action": "send_error_response",
      "errorProfileConfiguration": {
        "errorCode": 501,
        "errorCause": "NOT FOUND",
        "errorTitle": "NOT FOUND ",
        "errorDescription": "NOT FOUND",
        "retryAfter": "",
        "redirectUrl": ""
      }
    }
  ]
}

```

Failure response

```

curl -X PUT "http://10.75.175.233:30953/ocscp/scpc-configuration/v1/approutingoptions/med" -H "accept: application/json" -H "Content-Type: application/json" -d '{"appName":"mediation","routingOptions":{"retry":false,"maxRetryAttempts":6,"responseTimeout":"10","exceptionErrorResponses":[{"statusCode":["DEFAULT"],"action":"continue_processing"}, {"statusCode":["501"],"action":"send_error_response","errorProfileConfiguration":{"errorCode":501,"errorCause":"NOT FOUND","errorTitle":"NOT FOUND","errorDescription":"NOT FOUND","retryAfter":"","redirectUrl":""}}]}'

```

```

HTTP/1.1 400 Bad Request
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:08:49 GMT

```

```

{
  "title": "Bad Request",
  "status": "400",
  "detail": "App Name must always be mediation",
  "instance": "/ocscp/scpc-configuration/v1/approutingoptions/med",
  "cause": "INVALID_QUERY_PARAM"
}

```

DELETE REST API

This resource removes all the application routing options based on ruleName.

Note

DELETE method is not supported.

Resource URI: /ocscp/scpc-configuration/{version}/approutingoptions/{appname}

Table 2-224 Path Parameters Supported by the DELETE Response Body on this Resource

Name	Data Type	P	Description
appname	String	M	Removes configurations on app name.

Table 2-225 Data Structures Supported by the DELETE Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.

2.27 Configuring Mediation Trigger Point

This section describes the trigger points configurations to define the filter criteria for a message to decide whether to invoke mediation or not.

Resources

The following table describes the resource name to retrieve, add, update, and remove Mediation trigger points.

Table 2-226 Resource Name

Resource Name	Resource URI	HTTP Method	Description
mediation-trigger-point-config	/ocscp/scpc-configuration/{version}/mediation-trigger-point-config	GET	Retrieves all Mediation trigger point configurations.
mediation-trigger-point-config	/ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}	GET	Retrieves Mediation trigger point configuration for the specified ruleName.
mediation-trigger-point-config	/ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}	PUT	Configures Mediation trigger point configuration for the specified data.
mediation-trigger-point-config	/ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}	PATCH	Updates the Mediation trigger point configuration by ruleName.
mediation-trigger-point-config	/ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}	DELETE	Removes the Mediation trigger point configuration for the specified ruleName.

Data Model

The following table describes the supported data type.

Table 2-227 MediationTriggerPointConfig

Field Name	Data Type	P	Cardinality	Description
ruleName	String	M	1	Unique rule name for each mediation configuration. It is a unique primary key.
triggerPoints	Array(TriggerPoint)	M	1..N	List of trigger points to be enabled if matches. One or more of the following trigger points: "requestIngress", "requestEgress", "responseIngress", "responseEgress"
nfType	NFType	C	1	NFType for which mediation configuration is required. NFType is as per 3GPP TS 29.510 Section 6.1.6.3.3 Enumeration: NFType.
serviceName	String	C	1	The service of NFType for which mediation configuration is required. NFType is as per 3GPP TS29.510 Section 6.1.6.3.11 Enumeration: ServiceName.
match	Array(Match)	O	1..N	List of match blocks to be satisfied for the rule to be activated. The list of match blocks have OR semantics. Minimum number of blocks is 1. Maximum number of blocks is 20.
groupId	String	O	1	groupId for which mediation configuration is required. Mediation configuration for a specific group is applicable to the mediation requests or responses received only from the same group. HTTP Mediation service consumer NFs which requires the same mediation rules can be grouped together using this groupId.
httpMethods	Array(String)	O	1..N	HTTP methods (GET,POST,PUT,PATCH,DELETE,OPTIONS)

Note

For each trigger point configuration, the combination of NFType, serviceName, and httpMethods methods must be unique. No new records can be added with the same combination.

For example, if a configuration exists with the following values: ruleName=medRule1, nfType=UDM, serviceName=nudm-uecm, httpMethod = {PUT, POST}, then adding a similar configuration with the same combination of nfType, serviceName, and httpMethods with a different rule name as specified are not allowed: ruleName=medRule2, nfType=UDM, serviceName=nudm-uecm, httpMethod = {PUT, POST}.

Table 2-228 TriggerPoint

Enumeration value	Description
"requestIngress"	Mediation invocation after receiving the ingress 5G SBI request message.
"requestEgress"	Mediation invocation before forwarding the 5G SBI request message.
"responseIngress"	Mediation invocation after receiving the ingress 5G SBI response message.
"responseEgress"	Mediation invocation before forwarding the 5G SBI response message.

Table 2-229 Match

Field Name	Data Type	Description	Required
headers	HeaderBodyMatch[]	List of header name and header value to match using the MatchType comparison. All conditions inside a single header block have AND semantics. Minimum number of elements or conditions is 1. Maximum number of elements or conditions is 5.	anyOf
body	HeaderBodyMatch[]	List of the "body IE" JSON Pointer and value at that Pointer to match using the MatchType comparison. All conditions inside a single body block have AND semantics. Minimum number of elements or conditions is 1. Maximum number of elements or condition is 5.	anyOf

Table 2-230 HeaderBodyMatch

Field Name	Data Type	P	Cardinality	Description
name	String	M	1	Name of the header or the bodyIE JSON Pointer. Note: List of predefined headers available at in this section. JSON Pointer must point to basic data types. Arrayed and Object values are not supported.
match_type	MatchType	M	1	One of the supported match operators.
value	String	C	0..1	Value of the header or bodyIE to be matched. The value is only required if match_type is not range.
range	Range	C	0..1	Range start (inclusive). It is used only when match_type is range.

Note

Either the value or the range attribute must be present.

Table 2-231 MatchType

Field Name	Data Type	Description	Required
exact	String	Matching is performed using the exact comparison.	oneOf
prefix	String	Matching is performed using the prefix comparison.	oneOf
range	String	Matching is performed using the range comparison.	oneOf
regex	String	Matching is performed using the ECMAScript Regular Expression comparison.	oneOf

Table 2-232 Range

Field Name	Data Type	P	Cardinality	Description
start	String	O	0..1	The first value, that is, range start inclusive, identifying the start of the range. This string consists of only digits. Pattern: "^[0-9]+\$"
end	String	O	0..1	The last value, that is, range end inclusive, identifying the end of the range. This string consists of only digits. Pattern: "^[0-9]+\$"

Examples

Request body

```

{
  "groupId": "string",
  "ruleName": "string",
  "match": [
    {
      "body": [
        {
          "range": {
            "start": 0,
            "end": 0
          },
          "match-type": "exact",
          "name": "string",
          "value": "string"
        }
      ],
      "headers": [
        {
          "range": {
            "start": 0,
            "end": 0
          },
          "match-type": "exact",
          "name": "string",
          "value": "string"
        }
      ]
    }
  ]
}

```

```

        }
      ],
    }
  ],
  "serviceName": "5g-sbi-notification",
  "httpMethods": ["PUT", "POST"]
  "nfType": "5G_EIR",
  "triggerPoints": [
    "requestEgress"
  ]
}

```

Response body:

The response body for GET is the list of the following JSON structure.

The response body of PUT and PATCH is the following JSON structure.

```

{
  "groupId": "string",
  "ruleName": "string",
  "match": [
    {
      "body": [
        {
          "range": {
            "start": 0,
            "end": 0
          },
          "match-type": "exact",
          "name": "string",
          "value": "string"
        }
      ],
      "headers": [
        {
          "range": {
            "start": 0,
            "end": 0
          },
          "match-type": "exact",
          "name": "string",
          "value": "string"
        }
      ],
    }
  ],
  "serviceName": "5g-sbi-notification",
  "httpMethods": [ "PUT", "POST" ]
  "nfType": "5G_EIR",
  "triggerPoints": [
    "requestEgress"
  ]
}

```

Resource Definition**GET REST API**

This resource retrieves all the Mediation trigger point configurations.

Resource URI: /ocscp/scpc-configuration/{version}/mediation-trigger-point-config

Table 2-233 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationTriggerPointConfig	M	1..N	200 OK	Indicates Mediation trigger point configurations.

This resource retrieves all the Mediation trigger point configurations based on ruleName.

Resource URI: /ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}

Table 2-234 Path Parameters Supported by the GET Response Body on this Resource

Field Name	Data Type	P	Description
ruleName	String	M	Fetches configurations on ruleName

Table 2-235 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationTriggerPointConfig	M	1	200 OK	Indicates Mediation trigger point configurations.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Success response for GET and GET ALL

```
curl -X GET "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config" -H "accept: application/json"
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:06:48 GMT
```

```
[
  {
    "ruleName": "Mediation_rule1",
    "nfType": "UDR",
    "serviceName": "nudr-group-id-map",
    "httpMethods": [
      "PUT"
    ],
  },
]
```

```

    "match": [
      {
        "headers": [
          {
            "name": "api-version",
            "value": "v2",
            "match-type": "exact"
          }
        ],
        "body": [
          {
            "name": "amfId",
            "value": "100",
            "match-type": "prefix"
          }
        ]
      }
    ],
    "triggerPoints": [
      "requestEgress",
      "requestIngress",
      "responseEgress"
    ],
    "groupId": "group1"
  }
]

```

Success response 2

```
curl -X GET "http://10.75.215.251:30131/ocscf/scpc-configuration/v1/mediation-
trigger-point-config/Mediation_rule1" -H "accept: application/json"
```

```

HTTP/1.1 200 OK
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:08:49 GMT

```

```

{
  "ruleName": "Mediation_rule1",
  "nfType": "UDR",
  "serviceName": "nudr-group-id-map",
  "httpMethods": [
    "PUT"
  ],
  "match": [
    {
      "headers": [
        {
          "name": "api-version",
          "value": "v2",
          "match-type": "exact"
        }
      ]
    }
  ],

```

```

        "body": [
          {
            "name": "amfId",
            "value": "100",
            "match-type": "prefix"
          }
        ]
      },
      "triggerPoints": [
        "requestEgress",
        "requestIngress",
        "responseEgress"
      ],
      "groupId": "group1"
    }
  }

```

Failure response

```
url -X GET "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/med" -H "accept: application/json"
```

```

HTTP/1.1 404 Not Found
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/problem+json
Date: Tue, 24 May 2022 12:07:30 GMT

```

```

{
  "title": "Not Found",
  "status": "404",
  "detail": "Mediation_Configuration for given RuleName not found . Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/mediation-trigger-point-config/med",
  "cause": "DATA_NOT_FOUND"
}

```

PUT REST API

This resource configures Mediation trigger points for the specified data.

Resource URI: /ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}

Table 2-236 Data Structures Supported by the PUT Request Body on this Resource

Data Type	P	Cardinality	Description
MediationTriggerPointConfig	M	1	Indicates Mediation trigger point configurations to be added.

Table 2-237 Data Structures Supported by the PUT Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationTriggerPointConfig	M	1	200 OK	Indicates Mediation trigger point configurations.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.

Example

Success response

```

curl -X 'PUT' \
  'http://<SCP configuration FQDN>:30446/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule1' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "ruleName": "Mediation_rule1",
    "nfType": "NEF",
    "serviceName": "3gpp-as-session-with-qos",
    "httpMethods": [
      "PUT"
    ],
    "match": [
      {
        "headers": [
          {
            "name": "api-version",
            "value": "v2",
            "match-type": "exact"
          }
        ],
        "body": [
          {
            "name": "amfId",
            "value": "100",
            "match-type": "prefix"
          }
        ]
      }
    ],
    "triggerPoints": [
      "requestEgress",
      "requestIngress",
      "responseEgress"
    ],
    "groupId": "group1"
  }'
```

Failure response

```
curl -X PUT "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/med" -H "accept: application/json" -H "Content-Type: application/json" -d '{"nfType":"udr","serviceName":"nudr-group-id-map","groupId":"group1","ruleName":"Mediation_rule1","httpMethods":["PUT"],"match":[{"headers":[{"match-type":"exact","name":"api-version","value":"v2"}],"body":[{"match-type":"prefix","name":"amfId","value":"100"}]}],"triggerPoints":["requestEgress","requestIngress","responseEgress"]}' -v
```

```
HTTP/1.1 400 Bad Request
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/problem+json
Date: Tue, 24 May 2022 12:03:14 GMT
```

```
* Connection #0 to host 10.75.215.251 left intact
```

```
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Api ruleName and request body ruleName must be same.",
  "instance": "/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule",
  "cause": "INVALID_KEY"
}
```

PATCH REST API

This resource updates the Mediation trigger point configuration for the specified data.

Resource URI: /ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}

Table 2-238 Data Structures Supported by the PATCH Request Body on this Resource

Data Type	P	Cardinality	Description
string	M	1	The patch body in the string format that must be updated.

Table 2-239 Data Structures Supported by the PATCH Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationTriggerPointConfig	M	1	200 OK	Indicates Mediation trigger point configurations.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Success response:

```
curl -X PATCH "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule1" -H "Content-Type: application/merge-patch+json" -d '[{"op": "replace", "path": "/match/0/headers/0/name", "value": "amfId" }]'
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/json
Date: Tue, 24 May 2022 12:26:55 GMT
```

```
* Connection #0 to host 10.75.215.251 left intact
{"ruleName": "Mediation_rule1", "nfType": "UDR", "serviceName": "nudr-group-id-map", "httpMethods": ["PUT"], "match": [{"headers": [{"name": "amfId", "value": "v2", "match-type": "exact"}], "body": [{"name": "amfId", "value": "100", "match-type": "prefix"}]}], "triggerPoints": [{"requestEgress", "requestIngress", "responseEgress"}, {"groupId": "group1"}]}
```

Failure response -1

```
curl -X PATCH "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule1" -H "Content-Type: application/merge-patch+json" -d '[{"op": "replace", "path": "/match/0/headers/0/name", "value": "amfId" }]'
```

```
HTTP/1.1 404 Not Found
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/problem+json
Date: Tue, 24 May 2022 12:23:18 GMT
```

```
* Connection #0 to host 10.75.215.251 left intact
{"title": "Not Found", "status": "404", "detail": "Mediation_Configuration for given RuleName not found . Please refer to the User Guide.'ruleName': Mediation_rule1", "instance": "/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule1", "cause": "DATA_NOT_FOUND"}
```

Failure response -2

```
curl -X PATCH "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule1" -H "Content-Type: application/merge-patch+json" -d '[{"op": "replace", "path": "match/0/headers/match-type", "value": "prefix" }]'
```

```
HTTP/1.1 400 Bad Request
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/problem+json
Date: Tue, 24 May 2022 12:26:21 GMT
```



```
* Connection #0 to host 10.75.215.251 left intact
{"title":"Bad Request","status":"400","detail":"Invalid Patch Document","instance":"/ocscp/scpc-configuration/v1/mediation-trigger-point-config/Mediation_rule1","cause":"INVALID_REQUEST_BODY"}
```

DELETE REST API

This resource retrieves all the Mediation trigger point configuration based on ruleName.

Resource URI: /ocscp/scpc-configuration/{version}/mediation-trigger-point-config/{ruleName}

Table 2-240 Path Parameters Supported by the DELETE Response Body on this Resource

Field Name	Data Type	P	Description
ruleName	String	M	Removes configurations on ruleName

Table 2-241 Data Structures Supported by the DELETE Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Success response

```
curl -X DELETE "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/med1" -H "accept: application/json"
```

```
HTTP/1.1 204 No Content
Date: Tue, 24 May 2022 12:22:00 GMT
```

Failure response

```
curl -X DELETE "http://10.75.215.251:30131/ocscp/scpc-configuration/v1/mediation-trigger-point-config/med1" -H "accept: application/json"
```

```
HTTP/1.1 404 Not Found
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: application/problem+json
Date: Tue, 24 May 2022 12:05:38 GMT
```

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "Mediation_Configuration for given RuleName not found . Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/mediation-trigger-point-config/"
```

```
med1",
  "cause": "DATA_NOT_FOUND"
}
```

2.28 Configuring Mediation Rule

Section Title

This section describes the configuration of mediation rules for creating, modifying, and deleting Mediation rules using the Rest API.

Resources

The following table describes the resource name to retrieve, add, update, and remove Mediation rules.

Table 2-242 Resource Name

Resource Name	Resource URI	HTTP Method	Description
HTTP Mediation	<code>\${mediationConfig.baseUrl}/mediation/v1/rules</code> <code>\${mediationConfig.baseUrl}/mediation/v1/rules/</code>	GET	Retrieves all Mediation rules.
HTTP Mediation	<code>\${mediationConfig.baseUrl}/mediation/v1/rules/{ruleName}</code>	GET	Retrieves Mediation rule for the specified ruleName.
HTTP Mediation	<code>\${mediationConfig.baseUrl}/mediation/v1/rules/{ruleName}</code>	PUT	Creates or updates Mediation rule.
HTTP Mediation	<code>\${mediationConfig.baseUrl}/mediation/v1/rules/{ruleName}</code>	DELETE	Removes the Mediation rule.

Note

As mediation can be used by other NFs, a base URL is needed. This is defined in properties as `${mediationConfig.baseUrl}`. In the case of SCP, the value is: `/ocscp/scpc-configuration`, creating the URL like this: `/ocscp/scpc-configuration/mediation/v1/rules`

Data Model

The following table describes the supported data type.

Table 2-243 MediationRulesConfig

Field Name	Data Type	P	Cardinality	Description
ruleName	String	M	1	Unique rule name for each mediation rule. It is a unique primary key.
format	String	M	1	Indicates the Format in which the rules are defined, such as DRL.

Table 2-243 (Cont.) MediationRulesConfig

Field Name	Data Type	P	Cardinality	Description
status	String	M	1	Indicates the status of the rule. It can have the following values: - DRAFT - APPLIED The following fields are allowed to be modified in DRAFT status: Mediation Mode, Code, and State. The valid values for state are SAVE, CLONE, COMPILE, and APPLY. The Mediation Mode can only be modified in APPLIED status. The valid values for state are SAVE, CLONE, or DRAFT.
mode	String	M	1	Indicated whether the rule applies to mediation active or mediation test. - Mediation Active allows actual messages to be manipulated according to configured mediation rules. - Mediation Test executes the mediation rule on message copy instead of the actual message and verifies the behavior of the mediation rule.
state	String	M	1	Indicates the action to be applied to the rule. The default value is SAVE Note: The DRAFT state is an invalid transition that could lead to an error.
code	String	M	1	Indicates the configurable drool expression that matches the request/response headers and body sent by SCP.
New Rule Name	String	M	1	Indicates the new name of the rule. This field appears when a CLONE state is selected.

Note

For each mediation rule configuration, the rule name must be unique. No new rules can be added with the same name.

Request Body JSON Format

```
{
  "name": "string",
  "format": "DRL",
  "status": ["DRAFT", "APPLIED"],
  "mode": ["MEDIATION_ACTIVE", "MEDIATION_TEST"],
  "state": ["SAVE", "APPLY", "DRAFT", "COMPILE", "CLONE"],
  "code": "string"
}
```

Example

```
{
  "name": "ruleTest1",
  "format": "DRL",
  "status": "DRAFT",
  "mode": "MEDIATION_TEST",
  "state": "SAVE",
  "code": "package com.oracle.cgbu.ocmediation.nfmediation;\n \nimport
com.oracle.cgbu.ocmediation.factdetails.Request;\nimport
com.oracle.cgbu.ocmediation.factdetails.Response;\nimport
java.util.Map;\nimport java.util.HashMap; \ndialect \"mvel\"\n\nrule
\"ruleTest1\"\nwhen\n  req : Request(headers.has(\"Header1\") == true)\nthen
\n  req.headers.add(\"NewHeader1\", \"132465\")\nend"
}
```

Response Body JSON Format

```
{
  "name": "string",
  "format": "DRL",
  "mode": ["MEDIATION_ACTIVE", "MEDIATION_TEST"],
  "status": ["DRAFT", "APPLIED"],
  "code": "string"
}
```

Example

```
{
  "name": "ruleTest1",
  "format": "DRL",
  "mode": "MEDIATION_ACTIVE",
  "status": "DRAFT",
  "code": "package com.oracle.cgbu.ocmediation.nfmediation;\n \nimport
com.oracle.cgbu.ocmediation.factdetails.Request;\nimport
com.oracle.cgbu.ocmediation.factdetails.Response;\nimport
java.util.Map;\nimport java.util.HashMap; \ndialect \"mvel\"\n\nrule
\"ruleTest1\"\nwhen\n  req : Request(headers.has(\"Header1\") == true)\nthen
\n  req.headers.add(\"NewHeader1\", \"132465\")\nend"
}
```

Resource Definition

GET REST API

This resource retrieves all the Mediation rules.

Resource URI: /ocscp/scpc-configuration/mediation/v1/rules

Table 2-244 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationRules	M	1..N	200 OK	Indicates Mediation rules.

This resource retrieves all the Mediation rules based on ruleName.

Resource URI: /ocscp/scpc-configuration/mediation/v1/rules/{ruleName}

Table 2-245 Path Parameters Supported by the GET Response Body on this Resource

Field Name	Data Type	P	Description
ruleName	String	M	Fetches rule by ruleName

Table 2-246 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationRule	M	1	200 OK	Indicates Mediation rules.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Success response for GET ALL

```
curl -X GET "http://10.75.213.183:31612/ocscp/scpc-configuration/mediation/v1/rules"
-H "accept: application/json"
```

```
[
  {
    "name": "ruleTest0",
    "format": "DRL",
    "mode": "MEDIATION_ACTIVE",
    "status": "DRAFT",
    "code": "package com.oracle.cgbu.ocmediation.nfmediation; import
com.oracle.cgbu.ocmediation.factdetails.Request; dialect \"mvel\" rule
\"ruleTest0\" when req : Request(headers.has(\"NewTest0\") == true) then
req.headers.add(\"Test0\", \"0\") end"
  },
  {
    "name": "ruleTest1",
    "format": "DRL",
    "mode": "MEDIATION_ACTIVE",
    "status": "DRAFT",
    "code": "package com.oracle.cgbu.ocmediation.nfmediation; import
com.oracle.cgbu.ocmediation.factdetails.Request; dialect \"mvel\" rule
\"ruleTest1\" when req : Request(headers.has(\"NewTest1\") == true) then
req.headers.add(\"Test1\", \"1\") end"
  }
]
```

Success response for GET

```
curl -X GET "http://10.75.213.183:31612/ocscp/scpc-configuration/mediation/v1/
rules/ruleTest0" -H
    "accept: application/json"
```

```
{
  "name": "ruleTest0",
  "format": "DRL",
  "mode": "MEDIATION_ACTIVE",
  "status": "DRAFT",
  "code": "package com.oracle.cgbu.ocmediation.nfmediation; import
com.oracle.cgbu.ocmediation.factdetails.Request; dialect \"mvel\" rule
\"ruleTest0\" when req : Request(headers.has(\"NewTest0\") == true) then
req.headers.add(\"Test0\", \"0\") end"
}
```

Failure response

```
curl -X GET "http://10.75.213.183:31612/ocscp/scpc-configuration/mediation/v1/
rules/ruleTest$" -H
    "accept: application/json"
```

```
{
  "title": "NOT_FOUND",
  "status": 404,
  "detail": "Rule: ruleTest$ was not found",
  "cause":
"com.oracle.cgbu.ocmediationconfig.service.RulesConfigService.lambda$findByName$0(RulesConfigService.java:45)\njava.base/
java.util.Optional.orElseThrow(Optional.java:403)\ncom.oracle.cgbu.ocmediation
config.service.RulesConfigService.findByName(RulesConfigService.java:45)\ncom.
oracle.cgbu.ocmediationconfig.controller.RulesConfigController.getRuleByName(R
ulesConfigController.java:45)\njava.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
\njava.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.
java:77)\njava.base/
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAcces
sorImpl.java:43)\njava.base/
java.lang.reflect.Method.invoke(Method.java:568)\norg.springframework.web.meth
od.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:205)\norg.
springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(
InvocableHandlerMethod.java:150)\norg.springframework.web.servlet.mvc.method.a
nnotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandle
rMethod.java:117)\norg.springframework.web.servlet.mvc.method.annotation.Reque
stMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:
895)\norg.springframework.web.servlet.mvc.method.annotation.RequestMappingHand
lerAdapter.handleInternal(RequestMappingHandlerAdapter.java:808)\norg.springfr
amework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHan
dlerMethodAdapter.java:87)\norg.springframework.web.servlet.DispatcherServlet.
doDispatch(DispatcherServlet.java:1072)\norg.springframework.web.servlet.Dispa
tcherServlet.doService(DispatcherServlet.java:965)\norg.springframework.web.se
```

```

rvlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)\norg.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:898)\njavax.servlet.http.HttpServlet.service(HttpServlet.java:497)\norg.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)\njavax.servlet.http.HttpServlet.service(HttpServlet.java:584)\nio.undertow.servlet.handlers.ServletHandler.handleRequest(ServletHandler.java:74)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:129)\norg.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springframework.boot.actuate.metrics.web.servlet.WebMvcMetricsFilter.doFilterInternal(WebMvcMetricsFilter.java:96)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\nio.undertow.servlet.handlers.FilterHandler.handleRequest(FilterHandler.java:84)\nio.undertow.servlet.handlers.security.ServletSecurityRoleHandler.handleRequest(ServletSecurityRoleHandler.java:62)\nio.undertow.servlet.handlers.ServletChain$1.handleRequest(ServletChain.java:68)\nio.undertow.servlet.handlers.ServletDispatchingHandler.handleRequest(ServletDispatchingHandler.java:36)\nio.undertow.servlet.handlers.RedirectDirHandler.handleRequest(RedirectDirHandler.java:68)\nio.undertow.servlet.handlers.security.SSLInformationAssociationHandler.handleRequest(SSLInformationAssociationHandler.java:117)\nio.undertow.servlet.handlers.security.ServletAuthenticationCallHandler.handleRequest(ServletAuthenticationCallHandler.java:57)\nio.undertow.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.security.handlers.AbstractConfidentialityHandler.handleRequest(AbstractConfidentialityHandler.java:46)\nio.undertow.servlet.handlers.security.ServletConfidentialityConstraintHandler.handleRequest(ServletConfidentialityConstraintHandler.java:64)\nio.undertow.security.handlers.AuthenticationMechanismsHandler.handleRequest(AuthenticationMechanismsHandler.java:60)\nio.undertow.servlet.handlers.security.CachedAuthenticatedSessionHandler.handleRequest(CachedAuthenticatedSessionHandler.java:77)\nio.undertow.security.handlers.AbstractSecurityContextAssociationHandler.handleRequest(AbstractSecurityContextAssociationHandler.java:43)\nio.undertow.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.servlet.handlers.SendErrorPageHandler.handleRequest(SendErrorPageHandler.java:52)\nio.undertow.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.servlet.handlers.ServletInitialHandler.handleFirstRequest(ServletInitialHandler.java:275)\nio.undertow.servlet.handlers.ServletInitialHandler.access$100(ServletInitialHandler.java:79)\nio.undertow.servlet.handlers.ServletInitialHandler$2.call(ServletInitialHandler.java:134)\nio.undertow.servlet.handlers.ServletInitialHandler$2.call(ServletInitialHandler.java:131)\nio.undertow.servlet.core.ServletRequestContextThreadSetupAction$1.call(ServletRequestContextThreadSetupAction.java:48)\nio.undertow.servlet.core.ContextClassLoaderSetupAction$1.call(ContextClassLoaderSetupAction.java:43)\nio.undertow.servlet.handlers.ServletInitialHandler

```

```
.dispatchRequest(ServletInitialHandler.java:255)\nio.undertow.servlet.handlers
.ServletInitialHandler.access$000(ServletInitialHandler.java:79)\nio.undertow.
servlet.handlers.ServletInitialHandler$1.handleRequest(ServletInitialHandler.j
ava:100)\nio.undertow.server.Connectors.executeRootHandler(Connectors.java:387
)
\nio.undertow.server.HttpServerExchange$1.run(HttpServerExchange.java:852)\nor
g.jboss.threads.ContextClassLoaderSavingRunnable.run(ContextClassLoaderSavingR
unnable.java:35)\norg.jboss.threads.EnhancedQueueExecutor.safeRun(EnhancedQueue
Executor.java:2019)\norg.jboss.threads.EnhancedQueueExecutor$ThreadBody.doRun
Task(EnhancedQueueExecutor.java:1558)\norg.jboss.threads.EnhancedQueueExecutor
$ThreadBody.run(EnhancedQueueExecutor.java:1449)\norg.xnio.XnioWorker$WorkerTh
readFactory$1$1.run(XnioWorker.java:1282)\njava.base/
java.lang.Thread.run(Thread.java:842)"
}
```

PUT REST API

This resource configures Mediation rules for the specified data.

Resource URI: /ocscp/scpc-configuration/mediation/v1/rules/{ruleName}

Table 2-247 Path Parameters Supported by the PUT Response Body on this Resource

Field Name	Data Type	P	Description
ruleName	String	M	Modify rule by ruleName

Table 2-248 Data Structures Supported by the PUT Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationRule	M	1	200 OK	Modify Mediation rules.
MediationRule	M	1	201 CREATED	Create Mediation rules.
ProblemDetails	M	1	404 NOT FOUND	Indicates that there is no matching entry found.

Example

Success response for PUT

```
curl -X PUT "http://10.75.213.183:31612/ocscp/scpc-configuration/mediation/v1/
rules" -H "accept: application/json"
```

```
[
  {
    "name": "ruleTest0",
    "format": "DRL",
    "mode": "MEDIATION_ACTIVE",
    "status": "DRAFT",
    "code": "package com.oracle.cgbu.ocmediation.nfmediation; import
com.oracle.cgbu.ocmediation.factdetails.Request; dialect \"mvel\" rule
\"ruleTest0\" when req : Request(headers.has(\"NewTest0\") == true) then
req.headers.add(\"Test0\", \"0\") end"
```



```

    },
    {
        "name": "ruleTest1",
        "format": "DRL",
        "mode": "MEDIATION_ACTIVE",
        "status": "DRAFT",
        "code": "package com.oracle.cgbu.ocmediation.nfmediation; import
com.oracle.cgbu.ocmediation.factdetails.Request; dialect \"mvel\" rule
\"ruleTest1\" when req : Request(headers.has(\"NewTest1\") == true) then
req.headers.add(\"Test1\", \"1\") end"
    }
]

```

Success response for PUT

```

curl -X PUT "http://10.75.213.183:31612/ocscp/scpc-configuration/mediation/v1/
rules/ruleTest0" -H "accept: application/json" -d '{"name":
"ruleTest0","format": "DRL","status": "DRAFT","mode":
"MEDIATION_TEST","state": "SAVE","code": "package
com.oracle.cgbu.ocmediation.nfmediation;\n \nimport
com.oracle.cgbu.ocmediation.factdetails.Request;\nimport
com.oracle.cgbu.ocmediation.factdetails.Response;\nimport
java.util.Map;\nimport java.util.HashMap; \ndialect \"mvel\"\n\nrule
\"rule_test456\"\nwhen\n  req : Request(headers.has(\"OtherStuff\") == true)
\nthen\n  req.headers.add(\"TEST\", \"132465\")\nend"}'

```

```

{
    "name": "ruleTest0",
    "format": "DRL",
    "mode": "MEDIATION_ACTIVE",
    "status": "DRAFT",
    "code": "package com.oracle.cgbu.ocmediation.nfmediation;\n \nimport
com.oracle.cgbu.ocmediation.factdetails.Request;\nimport
com.oracle.cgbu.ocmediation.factdetails.Response;\nimport
java.util.Map;\nimport java.util.HashMap; \ndialect \"mvel\"\n\nrule
\"rule_test456\"\nwhen\n  req : Request(headers.has(\"OtherStuff\") == true)
\nthen\n  req.headers.add(\"TEST\", \"132465\")\nend"
}

```

Failure response

```

curl -X PUT "http://10.75.213.183:31612/ocscp/scpc-configuration/mediation/v1/
rules/ruleTest0" -H "accept: application/json" -d '{"name":
"ruleTest0","format": "DRL","status": "DRAFT","mode":
"MEDIATION_TEST","state": "SAVE"}'

```

```

{
    "title": "BAD_REQUEST",
    "status": 400,
    "detail": "Fields: [code], are required and missing for rules with state:
SAVE",
    "cause":
"com.oracle.cgbu.ocmediationconfig.validator.RuleConfigValidator.validateRequi

```

```

redFields(RuleConfigValidator.java:40)\ncom.oracle.cgbu.ocmediationconfig.serv
ice.RulesConfigService.saveRuleByName(RulesConfigService.java:59)\ncom.oracle
.cgbu.ocmediationconfig.controller.RulesConfigController.saveRuleByName(RulesCo
nfigController.java:67)\njava.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
\njava.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.
java:77)\njava.base/
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAcces
sorImpl.java:43)\njava.base/
java.lang.reflect.Method.invoke(Method.java:568)\norg.springframework.web.meth
od.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:205)\no
rg.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(
InvocableHandlerMethod.java:150)\norg.springframework.web.servlet.mvc.method.a
nnotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandle
rMethod.java:117)\norg.springframework.web.servlet.mvc.method.annotation.Reque
stMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:
895)\norg.springframework.web.servlet.mvc.method.annotation.RequestMappingHand
lerAdapter.handleInternal(RequestMappingHandlerAdapter.java:808)\norg.springfr
amework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHan
dlerMethodAdapter.java:87)\norg.springframework.web.servlet.DispatcherServlet.
doDispatch(DispatcherServlet.java:1072)\norg.springframework.web.servlet.Dispa
tcherServlet.doService(DispatcherServlet.java:965)\norg.springframework.web.se
rvlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)\norg.springf
ramework.web.servlet.FrameworkServlet.doPut(FrameworkServlet.java:920)\njavax.
servlet.http.HttpServlet.service(HttpServlet.java:520)\norg.springframework.we
b.servlet.FrameworkServlet.service(FrameworkServlet.java:883)\njavax.servlet.h
ttp.HttpServlet.service(HttpServlet.java:584)\nio.undertow.servlet.handlers.Se
rvletHandler.handleRequest(ServletHandler.java:74)\nio.undertow.servlet.handle
rs.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:129)\norg.springf
ramework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter
.java:100)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OnceP
erRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(Man
agedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImp
l.doFilter(FilterHandler.java:131)\norg.springframework.web.filter.FormContent
Filter.doFilterInternal(FormContentFilter.java:93)\norg.springframework.web.fi
lter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow
.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servl
et.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\nor
g.springframework.boot.actuate.metrics.web.servlet.WebMvcMetricsFilter.doFilde
rInternal(WebMvcMetricsFilter.java:96)\norg.springframework.web.filter.OncePer
RequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.cor
e.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers
.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springfram
ework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFil
ter.java:201)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(On
cePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(
ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChain
Impl.doFilter(FilterHandler.java:131)\nio.undertow.servlet.handlers.FilterHand
ler.handleRequest(FilterHandler.java:84)\nio.undertow.servlet.handlers.securit
y.ServletSecurityRoleHandler.handleRequest(ServletSecurityRoleHandler.java:62)
\nio.undertow.servlet.handlers.ServletChain$1.handleRequest(ServletChain.java:
68)\nio.undertow.servlet.handlers.ServletDispatchingHandler.handleRequest(Serv
letDispatchingHandler.java:36)\nio.undertow.servlet.handlers.RedirectDirHandle
r.handleRequest(RedirectDirHandler.java:68)\nio.undertow.servlet.handlers.secu
rity.SSLInformationAssociationHandler.handleRequest(SSLInformationAssociationH

```

```

andler.java:117)\nio.undertow.servlet.handlers.security.ServletAuthenticationC
allHandler.handleRequest(ServletAuthenticationCallHandler.java:57)\nio.undertow
w.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio
.undertow.security.handlers.AbstractConfidentialityHandler.handleRequest(Abstr
actConfidentialityHandler.java:46)\nio.undertow.servlet.handlers.security.Serv
letConfidentialityConstraintHandler.handleRequest(ServletConfidentialityConstr
aintHandler.java:64)\nio.undertow.security.handlers.AuthenticationMechanismsHa
ndler.handleRequest(AuthenticationMechanismsHandler.java:60)\nio.undertow.serv
let.handlers.security.CachedAuthenticatedSessionHandler.handleRequest(CachedAu
thenticatedSessionHandler.java:77)\nio.undertow.security.handlers.AbstractSecu
rityContextAssociationHandler.handleRequest(AbstractSecurityContextAssociation
Handler.java:43)\nio.undertow.server.handlers.PredicateHandler.handleRequest(P
redicateHandler.java:43)\nio.undertow.servlet.handlers.SendErrorPageHandler.ha
ndleRequest(SendErrorPageHandler.java:52)\nio.undertow.server.handlers.Predica
teHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.servlet.handler
s.ServletInitialHandler.handleFirstRequest(ServletInitialHandler.java:275)\nio
.undertow.servlet.handlers.ServletInitialHandler.access$100(ServletInitialHand
ler.java:79)\nio.undertow.servlet.handlers.ServletInitialHandler$2.call(Servle
tInitialHandler.java:134)\nio.undertow.servlet.handlers.ServletInitialHandler$
2.call(ServletInitialHandler.java:131)\nio.undertow.servlet.core.ServletReques
tContextThreadSetupAction$1.call(ServletRequestContextThreadSetupAction.java:4
8)\nio.undertow.servlet.core.ContextClassLoaderSetupAction$1.call(ContextClass
LoaderSetupAction.java:43)\nio.undertow.servlet.handlers.ServletInitialHandler
.dispatchRequest(ServletInitialHandler.java:255)\nio.undertow.servlet.handlers
.ServletInitialHandler.access$000(ServletInitialHandler.java:79)\nio.undertow.
servlet.handlers.ServletInitialHandler$1.handleRequest(ServletInitialHandler.j
ava:100)\nio.undertow.server.Connectors.executeRootHandler(Connectors.java:387
)
\nio.undertow.server.HttpServerExchange$1.run(HttpServerExchange.java:852)\nor
g.jboss.threads.ContextClassLoaderSavingRunnable.run(ContextClassLoaderSavingR
unnable.java:35)\norg.jboss.threads.EnhancedQueueExecutor.safeRun(EnhancedQueu
eExecutor.java:2019)\norg.jboss.threads.EnhancedQueueExecutor$ThreadBody.doRun
Task(EnhancedQueueExecutor.java:1558)\norg.jboss.threads.EnhancedQueueExecutor
$ThreadBody.run(EnhancedQueueExecutor.java:1449)\norg.xnio.XnioWorker$WorkerTh
readFactory$1$1.run(XnioWorker.java:1282)\njava.base/
java.lang.Thread.run(Thread.java:842)"
}

```

DELETE REST API

This resource retrieves all the Mediation rules based on ruleName.

Resource URI: /ocscp/scpc-configuration/mediation/v1/rules/{ruleName}

Table 2-249 Path Parameters Supported by the DELETE Response Body on this Resource

Field Name	Data Type	P	Description
ruleName	String	M	Deletes Mediation rules by ruleName

Table 2-250 Data Structures Supported by the DELETE Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
MediationRule	M	1	204	Deleted Mediation rule.
ProblemDetails	M	1	404	Indicates that there is no matching entry found.

Example

Success response for DELETE

```
curl -X DELETE "http://10.75.213.183:31612/ocscp/scpc-configuration/
mediation/v1/rules/ruleTest999" -H
    "accept: application/json"
```

Failure response

```
curl -X DELETE "http://10.75.213.183:31612/ocscp/scpc-configuration/
mediation/v1/rules/ruleTest$" -H
    "accept: application/json"
```

```
{
  "title": "NOT_FOUND",
  "status": 404,
  "detail": "Rule: ruleTest$ was not found",
  "cause":
    "com.oracle.cgbu.ocmediationconfig.service.RulesConfigService.lambda$deleteByN
ame$1(RulesConfigService.java:52)\njava.base/
java.util.Optional.orElseThrow(Optional.java:403)\ncom.oracle.cgbu.ocmediation
config.service.RulesConfigService.deleteByName(RulesConfigService.java:52)\nco
m.oracle.cgbu.ocmediationconfig.controller.RulesConfigController.deleteRuleByN
ame(RulesConfigController.java:52)\njava.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
\njava.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.
java:77)\njava.base/
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAcces
sorImpl.java:43)\njava.base/
java.lang.reflect.Method.invoke(Method.java:568)\norg.springframework.web.meth
od.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:205)\nno
rg.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(
InvocableHandlerMethod.java:150)\norg.springframework.web.servlet.mvc.method.a
nnotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandle
rMethod.java:117)\norg.springframework.web.servlet.mvc.method.annotation.Reque
stMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:
895)\norg.springframework.web.servlet.mvc.method.annotation.RequestMappingHand
lerAdapter.handleInternal(RequestMappingHandlerAdapter.java:808)\norg.springfr
amework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHan
dlerMethodAdapter.java:87)\norg.springframework.web.servlet.DispatcherServlet.
doDispatch(DispatcherServlet.java:1072)\norg.springframework.web.servlet.Dispa
tcherServlet.doService(DispatcherServlet.java:965)\norg.springframework.web.se
```

```

rvlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)\norg.springframework.web.servlet.FrameworkServlet.doDelete(FrameworkServlet.java:931)\njavax.servlet.http.HttpServlet.service(HttpServlet.java:523)\norg.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)\njavax.servlet.http.HttpServlet.service(HttpServlet.java:584)\nio.undertow.servlet.handlers.ServletHandler.handleRequest(ServletHandler.java:74)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:129)\norg.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springframework.boot.actuate.metrics.web.servlet.WebMvcMetricsFilter.doFilterInternal(WebMvcMetricsFilter.java:96)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\norg.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201)\norg.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:117)\nio.undertow.servlet.core.ManagedFilter.doFilter(ManagedFilter.java:61)\nio.undertow.servlet.handlers.FilterHandler$FilterChainImpl.doFilter(FilterHandler.java:131)\nio.undertow.servlet.handlers.FilterHandler.handleRequest(FilterHandler.java:84)\nio.undertow.servlet.handlers.security.ServletSecurityRoleHandler.handleRequest(ServletSecurityRoleHandler.java:62)\nio.undertow.servlet.handlers.ServletChain$1.handleRequest(ServletChain.java:68)\nio.undertow.servlet.handlers.ServletDispatchingHandler.handleRequest(ServletDispatchingHandler.java:36)\nio.undertow.servlet.handlers.RedirectDirHandler.handleRequest(RedirectDirHandler.java:68)\nio.undertow.servlet.handlers.security.SSLInformationAssociationHandler.handleRequest(SSLInformationAssociationHandler.java:117)\nio.undertow.servlet.handlers.security.ServletAuthenticationCallHandler.handleRequest(ServletAuthenticationCallHandler.java:57)\nio.undertow.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.security.handlers.AbstractConfidentialityHandler.handleRequest(AbstractConfidentialityHandler.java:46)\nio.undertow.servlet.handlers.security.ServletConfidentialityConstraintHandler.handleRequest(ServletConfidentialityConstraintHandler.java:64)\nio.undertow.security.handlers.AuthenticationMechanismsHandler.handleRequest(AuthenticationMechanismsHandler.java:60)\nio.undertow.servlet.handlers.security.CachedAuthenticatedSessionHandler.handleRequest(CachedAuthenticatedSessionHandler.java:77)\nio.undertow.security.handlers.AbstractSecurityContextAssociationHandler.handleRequest(AbstractSecurityContextAssociationHandler.java:43)\nio.undertow.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.servlet.handlers.SendErrorPageHandler.handleRequest(SendErrorPageHandler.java:52)\nio.undertow.server.handlers.PredicateHandler.handleRequest(PredicateHandler.java:43)\nio.undertow.servlet.handlers.ServletInitialHandler.handleFirstRequest(ServletInitialHandler.java:275)\nio.undertow.servlet.handlers.ServletInitialHandler.access$100(ServletInitialHandler.java:79)\nio.undertow.servlet.handlers.ServletInitialHandler$2.call(ServletInitialHandler.java:134)\nio.undertow.servlet.handlers.ServletInitialHandler$2.call(ServletInitialHandler.java:131)\nio.undertow.servlet.core.ServletRequestContextThreadSetupAction$1.call(ServletRequestContextThreadSetupAction.java:48)\nio.undertow.servlet.core.ContextClassLoaderSetupAction$1.call(ContextClassLoaderSetupAction.java:43)\nio.undertow.servlet.handlers.ServletInitialHan

```

```

dler.dispatchRequest(ServletInitialHandler.java:255)\nio.undertow.servlet.handlers.ServletInitialHandler.access$000(ServletInitialHandler.java:79)\nio.undertow.servlet.handlers.ServletInitialHandler$1.handleRequest(ServletInitialHandler.java:100)\nio.undertow.server.Connectors.executeRootHandler(Connectors.java:387)\nio.undertow.server.HttpServerExchange$1.run(HttpServerExchange.java:852)
)\norg.jboss.threads.ContextClassLoaderSavingRunnable.run(ContextClassLoaderSavingRunnable.java:35)\norg.jboss.threads.EnhancedQueueExecutor.safeRun(EnhancedQueueExecutor.java:2019)\norg.jboss.threads.EnhancedQueueExecutor$ThreadBody.doRunTask(EnhancedQueueExecutor.java:1558)\norg.jboss.threads.EnhancedQueueExecutor$ThreadBody.run(EnhancedQueueExecutor.java:1449)\norg.xnio.XnioWorker$WorkerThreadFactory$1$1.run(XnioWorker.java:1282)\njava.base/java.lang.Thread.run(Thread.java:842)"
}

```

2.29 Configuring Route Groups

This section describes REST API configurations required for Route Groups.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the route-groups resource type.

Table 2-251 Resource Name

Resource Name	Resource URI	HTTP Method	Description
route-groups	/ocscpsc-configuration/v1/route-groups	GET	- Reads a collection of route groups. - Reads the route group configuration of a given route group name. - Retrieves configured route groups based on the supplied query parameters as filtering criteria.
route-groups	/ocscpsc-configuration/v1/route-groups	PUT	Configures a new route group or replaces the configuration of an existing route group by providing a route group configuration in the request body.
route-groups	/ocscpsc-configuration/v1/route-groups	DELETE	Removes the configuration of an existing route group.

Resource: route-groups

Resource URI: /ocscpsc-configuration/v1/route-groups

Resource Definition

This section describes GET, PUT, and DELETE resource types supported by Route Group.

GET REST API

The following table describes the URI query parameters supported by the GET method on this resource.

Note

- The names of the query parameters in the following tables are case sensitive.
- The combination of query parameters are not supported. If no query parameter is specified, it retrieves all the records. Otherwise, only one query parameter at a time is supported.

Table 2-252 URI Query Parameters Supported by the GET Method

Field Name	Data Type	P	Cardinality	Description
routeGroupId	string	O	0..1	Indicates the unique route group ID.
routeGroupType	RouteGroupType	O	0..1	Indicates all route groups configured using specified addressing parameters such as fqdn, nfiInstanceId, or ipv4address.
primaryRoute	PrimaryRoute	O	0..1	Indicates specific route group configuration for the specified fqdn, nfiInstanceId, or ipv4address. For IP, only the primaryRoute query parameter with only one element (ipv4Address and port) in the list is supported. Note: As this query parameter considers the JSON format as an input string, you must use the "data-urleencode" annotation in the curl command.

Note

To get all route groups, do not provide any query parameters.

The following table describes the data structure supported by the GET response body on this resource:

Table 2-253 Data Structure Supported by the GET Response Body

Data Type	P	Cardinality	Response Code	Description
array(routeGroupRecord)	M	1	200 OK	The response body contains a list of route group configuration equivalent to the criteria for received requests.
ProblemDetails	M	1	404 NOT FOUND	This data structure is sent when no matching entry is found. For information about the ProblemDetails structure, see 3GPP TS 29.571.

Note

All the supported HTTP error status is applicable with a ProblemDetails data type as described in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. For more information, see Clause 5.2.7 of 3GPP TS 29.500.

The following example is of a successful response.

```
curl -v -X PUT "http://10.75.215.87:30287/ocscp/scpc-configuration/v1/route-groups" -H "accept: */*" -H "Content-Type: application/json" -d'{"routeGroupId":"udm1","routeGroupType":"IPV4","primaryRoute":{"ipEndpoints":[{"ipV4Address":"200.200.200.210","port":80}]},"alternateRouteList":[{"apiPrefix":"USEast","capacity":10,"ipV4Addresses":["200.200.200.220"],"port":80,"priority":10,"scheme":"http"}, {"apiPrefix":"USEast","capacity":10,"ipV4Addresses":["200.200.200.230","200.200.200.235"],"port":80,"priority":10,"scheme":"http"}]}'
```

Response:

201 OK

```
{"routeGroupId":"udm1","routeGroupType":"IPV4","primaryRoute":{"ipEndpoints":[{"ipV4Address":"200.200.200.210","port":80}]},"alternateRouteList":[{"ipV4Addresses":["200.200.200.220"],"port":80,"priority":10,"capacity":10,"apiPrefix":"USEast","scheme":"http"}, {"ipV4Addresses":["200.200.200.230","200.200.200.235"],"port":80,"priority":10,"capacity":10,"apiPrefix":"USEast","scheme":"http"}]}
```

PUT REST API

There are no URI query parameters supported by the PUT method on this resource.

The following table describes the data structure supported by the PUT request body on this resource:

Table 2-254 Data Structure Supported by the PUT Request Body

Data Type	P	Cardinality	Description
routeGroupRecord	M	1	Indicates the route group configuration data.

The following table describes the data structures supported by the PUT response body on this resource:

Table 2-255 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Code	Description
routeGroupRecord	M	1	200 OK	Indicates the updated or replaced existing route group configuration data equivalent to the criteria for received requests.
routeGroupRecord	M	1	201 Created	Indicates the successful creation of new route group configuration data as per received requests.
ProblemDetails	M	1	400 BAD REQUEST	This response is used when the request body validation fails. For example, when serviceProtoName is missing in the request body. For information about the ProblemDetails structure, see 3GPP TS 29.571.

Note

All supported HTTP error status is applicable with a ProblemDetails data type. For more information, see Clause 5.2.7 of 3GPP TS 29.500.

The following example is of a successful response.

```
curl -X GET "http://10.75.215.87:30287/ocscp/scpc-configuration/v1/route-groups" -H "accept: application/json"
```

Response:

```
200 OK
[{"routeGroupId":"udm1","routeGroupType":"IPV4","primaryRoute":{"ipEndPoints":
[{"ipv4Address":"200.200.200.210","port":80}]},"alternateRouteList":
[{"ipv4Addresses":
["200.200.200.220"],"port":80,"priority":10,"capacity":10,"apiPrefix":"USEast",
"scheme":"http"}, {"ipv4Addresses":
["200.200.200.230","200.200.200.235"],"port":80,"priority":10,"capacity":10,"a
piPrefix":"USEast","scheme":"http"}]}][root@master ocscp]
```

DELETE REST API

The following table describes the URI query parameters supported by the DELETE method on this resource:

Table 2-256 URI Query Parameters Supported by the DELETE Method

Name	Data Type	P	Cardinality	Description
routeGroupId	string	M	1	Indicates the unique route group ID.

Note

All the supported HTTP error status is applicable with a ProblemDetails data type. For more information, see Clause 5.2.7 of 3GPP TS 29.500.

The following example is of a successful response.

```
curl -v -X DELETE "http://10.75.215.87:30287/ocscp/scpc-configuration/v1/route-groups?routeGroupId=udm1" -H "accept: application/json"
```

204 No Content

Data Model

The following tables describe different data models required for configuring Route Group.

Table 2-257 routeGroupRecord

Name	Data Type	P	Cardinality	Description
routeGroupId	string	M	1	Indicates the unique route group name or ID.
routeGroupType	RouteGroupType	M	1	Addresses parameters such as fqdn, nfInstanceId, or ipv4address, used in route group configuration.
primaryRoute	PrimaryRoute	C	1	Indicates the target endpoint information for the first routing attempt of 5G SBI message. - At least one of the first attempt route information parameters is included in the route configuration. - If the primaryRoute parameter is present, then the alternateRouteList parameter is also present. - If the primaryRouteList parameter is present, then the alternateRouteList parameter is absent. - The valid combinations are primaryRoute and alternateRouteList, primaryRouteList, All other combinations are invalid.
alternateRouteList	array(RouteRecord)	C	0..N	Indicates the route (target endpoint info) information to be used in alternate NF selection and load-balancing at SCP in alternate routing of 5G SBI message.

Table 2-258 PrimaryRoute

Name	Data Type	P	Cardinality	Description
fqdn	Fqdn	C	0..1	Indicates the FQDN of primary route, that is, for the first routing attempt of a 5G SBI message request.
port	integer	C	0..1	Indicates the port number. The minimum value is 0 and the maximum value is 65535. Port is defined if FQDN is present.

Table 2-258 (Cont.) PrimaryRoute

Name	Data Type	P	Cardinalit y	Description
nfInstanceId	NfInstanceId	C	0..1	Indicates the NF instance ID of primary route, that is, for the first routing attempt of a 5G SBI message request.
ipEndPoints	array(IpEndPoint)	C	0..1	Indicates the list of all IPv4 addresses of primary route, that is, for the first routing attempt of a 5G SBI message request.

Note

- At least one of the primary route addressing parameters such as fqdn, nfInstanceId, or ipEndPoints must be included in the route configuration.
- The primary route has the authority, FQDN or IP and port information, which is matched with ":authority" pseudo header of the first routing attempt to select a producer NF. Note that the scheme and apiPrefix are not considered.
- The port is defined if FQDN is present.

Table 2-259 IpEndPoint

Attribute Name	Data Type	P	Cardinalit y	Description
ipv4Address	Ipv4Addr	C	0..1	Indicates the IPv4 address.
port	integer	M	1	Indicates the port number. The minimum value is 0 and the maximum value is 65535.

Note

At most only one occurrence of ipv4Address is included in this data structure.

Table 2-260 RouteRecord

Name	Data Type	P	Cardinalit y	Description
fqdn	Fqdn	C	0..1	Indicates the FQDN of primary route, that is, for the first routing attempt of a 5G SBI message request.
nfInstanceId	NfInstanceId	C	0..1	Indicates the NF instance ID of primary route, that is, for the first routing attempt of a 5G SBI message request.
ipv4Addresses	array(Ipv4Addr)	C	0..N	Indicates the list of all IPv4 addresses of primary route, that is, for the first routing attempt of a 5G SBI message request.
port	integer	O	0..1	Indicates the port number. The minimum value is 0 and the maximum value is 65535.

Table 2-260 (Cont.) RouteRecord

Name	Data Type	P	Cardinality	Description
priority	integer	O	0..1	Indicates the priority (relative to other NFs of the same route list) within the range of 0 to 65535 for NF selection and alternate routing. The lower values indicate a higher priority.
capacity	integer	O	0..1	Indicates the static capacity information within the range of 0 to 65535. It is expressed as a weight relative to other NF instances of the same route list.
apiPrefix	string	O	0..1	Indicates the optional path segments to construct the {apiRoot} variable of the different API URIs as described in Clause 4.4.1 of 3GPP TS 29.501.
scheme	UriScheme	M	1	Indicates the URI scheme, for example, "http" or "https".

Note

- At least one of the primary route addressing parameters such as fqdn, nfInstanceId, or ipv4address, must be included in the route configuration.
- If the port number is absent, SCP uses the default HTTP port number, that is, TCP port 80 for "http" URIs or TCP port 443 for "https" URIs as specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 7540.

Table 2-261 Enumeration: RouteGroupType

Enumeration Value	Description
"FQDN"	Route group with FQDN in route group configuration.
"NFINSTANCEID"	Route group with NF instance ID in route group configuration.
"IPV4"	Route group with IPv4 addresses in route group configuration.

Table 2-262 Simple Data Types

Type Name	Type Definition	Description
Fqdn	string	Indicates the FQDN of the NF service.
Ipv4Addr	string	Indicates the string identifying an IPv4 address formatted in the "dotted decimal" notation as defined in IETF RFC 1166. Pattern: '^([0-9] [1-9][0-9] 1[0-9][0-9] 2[0-4][0-9] 25[0-5])\.([0-9] [1-9][0-9] 1[0-9][0-9] 2[0-4][0-9] 25[0-5])\$'
NfInstanceId	string	Indicates the string uniquely identifying an NF instance. The format of the NF Instance ID is a Universally Unique Identifier (UUID) version 4 as described in IETF RFC 4122.

Table 2-263 ProblemDetails

Attribute Name	Data Type	P	Cardinalit y	Description
type	Uri	O	0..1	Identifies the problem type. A URI reference according to IETF RFC 3986.
title	string	O	0..1	Indicates a short human-readable summary of the problem type. It should not change from occurrence to occurrence of the problem.
status	integer	O	0..1	Indicates the HTTP status code for the occurrence of the problem.
detail	string	O	0..1	Indicates a human-readable explanation specific to the occurrence of the problem.
instance	Uri	O	0..1	Indicates a URI reference that identifies the specific occurrence of the problem.
cause	string	C	0..1	Indicates a machine-readable application error cause specific to the occurrence of the problem. It should be present and provide application-related error information if available.
invalidParams	array(InvalidParam)	O	1..N	Indicates the description of invalid parameters for a request rejected due to invalid parameters.

For more information about the ProblemDetails structure, see Section 5.2.4.1 of 3GPP TS 29.571.

2.30 Configuring Consumer NF Info

This section describes Consumer NF Info parameters that are used to determine the identity of consumer NFs that send message requests to SCP.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the ConsumerInfo resource type.

Table 2-264 Resources

Resource Name	Resource URI	HTTP Method	Description
ConsumerInfo	/ocscp/scpc-configuration/{version}/consumerNfInfo/headerInfo	GET	Retrieves consumerInfo data
ConsumerInfo	/ocscp/scpc-configuration/{version}/consumerNfInfo/headerInfo	PUT	Configures ConsumerInfo data

Data Model

Request Body

The following table describes ConsumerInfo name and data type.

Table 2-265 ConsumerInfo

Name	Data Type	P	Cardinality	Description
primaryHeaderName	String	M	1	The header name to identify the consumer NF according to the ingress rate limiting configurations. This is a mandatory parameter. This parameter is given priority over the secondaryHeaderName parameter. The default value is "X-Forwarded-Client-Cert". It can use the following values: "User-Agent" "X-Forwarded-Client-Cert"
secondaryHeaderName	String	O	1	The header name to identify the consumer NF according to the ingress rate limiting configurations. This is an optional parameter. The default value is "". It can use the following values: "User-Agent" "X-Forwarded-Client-Cert"
format	String	M	1	The header format to identify the consumer NF according to the ingress rate limiting configurations. It supports the following formats: - Format1: NFTYPE-NFINSTANCEID FQDN or NFTYPE-NFINSTANCEID-FQDN - Format2: NFTYPE-FQDN NFINSTANCEID or NFTYPE-FQDN-NFINSTANCEID - Format3: NFTYPE-NFINSTANCEID - Format4: NFTYPE-FQDN - Format5: NFTYPE Where, - NFTYPE indicates the type of consumer NF. - NFINSTANCEID indicates the instance ID of the consumer NF. - FQDN indicates the FQDN of the consumer NF. In the aforementioned example, "-" is a separator and NFInstanceId, FQDN, and Hostname are supported IDs.
separator	String	M	1	This is the separator that the User-Agent header uses to separate NFINSTANCEID and FQDN. The default value is space ().
certExtractIndex	String	M	1	The certificate extract index contains certificate information in the XFCC header. This parameter is used to decode "X-Forwarded-Client-Cert" for the FQDN. The default value is 0.
extractField	String	M	1	This is the name of the field that has to be retrieved from the XFCC header. The default value is DNS.

Table 2-265 (Cont.) ConsumerInfo

Name	Data Type	P	Cardinality	Description
extractIndex	String	M	1	Index where the Field configured in 'extractField' is present in the XFCC header for extraction. The default value is 0.

Json Format:

```
[
  {
    "primaryHeaderName": "string",
    "secondaryHeaderName": "string",
    "format": "string",
    "separator": "string",
    "certExtractIndex": "string",
    "extractField": "string",
    "extractIndex": "string"
  }
]
```

Response Body

Response body data model:

Data Type	Description
ConsumerInfo	Determines the header type such as XFCC or User-Agent, in the ingress message request.
ProblemDetails	Returns when an invalid combination or more than two query parameters are provided.

Resource Definition:

This section describes GET and PUT resource types supported by ConsumerInfo.

GET API

This section describes the resource to fetch the existing ConsumerInfo configuration.

Resource URI: /ocscp/scpc-configuration/v1/consumerNFInfo/headerInfo

Table 2-266 Data structures supported by the GET Response Body on this resource

Field Name	P	Cardinality	Response Code	Description
consumerInfo	M	1	200 OK	Determines the header type such as XFCC or User-Agent, in the ingress message request.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than two query parameters are provided.

```
curl -X GET "http://10.75.237.50:31578/ocscp/scpc-configuration/v1/consumerNFInfo/headerInfo" -H "accept: application/json"
```

```
[
  {
    "primaryHeaderName": "User-Agent",
    "format": "<NFType>-<NFInstanceID>-<FQDN>",
  }
]
```

PUT API

This resource configures the use of Ingress Rate Limiting Configuration header using the Request Body.

Resource URI: /ocscp/scpc-configuration/v1/consumerNFInfo/headerInfo

Table 2-267 Data structures supported by the PUT Response Body on this resource

Data Type	P	Cardinality	Response Code	Description
consumerInfo	M	1	200 OK	Determines the header type such as XFCC or User-Agent, in the ingress message request.
ProblemDetails	M	1	400 BAD REQUEST	Returns when an invalid combination or more than two query parameters are provided.

Success Response

```
curl -X PUT "http://10.75.237.50:31337/ocscp/scpc-configuration/v1/consumerNfInfo/headerInfo" -H "accept: */*" -H "Content-Type: application/json"
{
  "primaryHeaderName": "X-Forwarded-Client-Cert",
  "secondaryHeaderName": "User-Agent",
  "userAgentHeaderFormat": "NFType,NFInstanceID,FQDN",
  "userAgentHeaderSeparator": "SPACE",
  "xfccHeaderCertExtractIndex": "0",
  "xfccHeaderExtractField": "DNS",
  "xfccHeaderExtractIndex": "0"
}
Response body
[
  {
    "primaryHeaderName": "X-Forwarded-Client-Cert",
    "secondaryHeaderName": "User-Agent",
    "userAgentHeaderFormat": "NFType-NFInstanceID FQDN",
    "userAgentHeaderSeparator": "SPACE",
    "xfccHeaderCertExtractIndex": "0",
    "xfccHeaderExtractField": "DNS",
    "xfccHeaderExtractIndex": "0"
  }
]
```

2.31 Configuring SCP Services

This section provides configuration information about thread watchdog and queue alerts threshold required for SCP microservices.

Resources

The following table describes the resource name to retrieve and update configuration at the SCP microservices level.

Table 2-268 Resource Name

Resource Name	Resource URI	HTTP Method	Description
scp-service-config	/ocscp/scpc-configuration/{version}/scp-service-config	GET ALL	Retrieves all the SCP microservices configurations.
scp-service-config	/ocscp/scpc-configuration/{version}/scp-service-config/{serviceName}	GET	Retrieves SCP microservices configurations based on servicename.
scp-service-config	/ocscp/scpc-configuration/{version}/scp-service-config/{serviceName}	PUT	Updates all the SCP microservices configurations based on servicename.

Data Model

This REST API is used to update microservice level configurations for SCP, therefore the data model is generic.

Generic Data Model

Table 2-269 ScpServiceConfigs

Field Name	Data Type	P	Cardinality	Description	Allowed Values
serviceName	String	M	1	Indicates the SCP microservice name.	Valid microservice names of SCP, for example, • scpc-notification • scp-worker • scp-nrfproxy • scpc-subscription • scpc-alternate-resolution • scpc-audit • scpc-configuration • scp-cache • scp-load-manager
scpServiceConfigs	Map<String, IScpServiceConfigValue>	M	1	Contains microservice level configurations provided with the type of configurations and value in the JSON structure.	-

Specific Data Model

TaskInfoScpConfig

The following data model is defined to specify thread related configurations.

Table 2-270 ScpServiceConfigValue

Field Name	Data Type	P	Cardinalit y	Description	Allowed Values	Default Values
type	Type	M	1	Indicates the type of configuration to identify whether the value is single or range.	VALUE	VALUE
value	List<TaskInfoScpConfig>	M	1	Indicates the list of values that specify the thread information configurations.	List of TaskInfoScpConfig. For more information, see Table 2-271 .	For default values, see Table 2-271 .

Table 2-271 TaskInfoScpConfig

Field Name	Data Type	P	Cardinalit y	Description	Allowed Value	Default Value
queueName	String	NA	1	Indicates the name of the queue for which these configurations are applicable.	The set of allowed values for each supported micro-service, for example, serviceName, is as follows: serviceName: scpc-notification - notificationQueue - waitingQueue - runQueue serviceName: scp-worker - scpDownstreamExecutorQueue - scpNrfProxyDownstreamExecutorQueue - scpUpstreamExecutorQueue - scpClientExecutorQueue - scpUpdateSLCertsQueue - scpMediationDownstreamExecutorQueue - scpReconfigureEgressRLExecutorQueue - scpTrafficFedExecutorQueue serviceName: scp-nrfproxy - scpDownstreamExecutorQueue - scpUpstreamExecutorQueue	The set of default values for each supported micro-service, for example, serviceName, is as follows: serviceName: scpc-notification - notificationQueue - waitingQueue - runQueue serviceName: scp-worker - scpDownstreamExecutorQueue - scpNrfProxyDownstreamExecutorQueue - scpUpstreamExecutorQueue - scpClientExecutorQueue - scpUpdateSLCertsQueue - scpMediationDownstreamExecutorQueue - scpReconfigureEgressRLExecutorQueue - scpTrafficFedExecutorQueue serviceName: scp-nrfproxy - scpDownstreamExecutorQueue - scpUpstreamExecutorQueue serviceName: scp-cache

Table 2-271 (Cont.) TaskInfoScpConfig

Field Name	Data Type	P	Cardinalit y	Description	Allowed Value	Default Value
					serviceName: scp-cache - accessTokenCohEvExecutorQueue - accessTokenAppEvExecutorQueue - scpCacheExecutorQueue serviceName: scp-load-manager - sutLciCohEvExecutorQueue - sutLciAppEvExecutorQueue - peerLciCohEvExecutorQueue - peerLciAppEvExecutorQueue - loadCohEvExecutorQueue - loadAppEvExecutorQueue	- accessTokenCohEvExecutorQueue - accessTokenAppEvExecutorQueue - scpCacheExecutorQueue serviceName: scp-load-manager - sutLciCohEvExecutorQueue - sutLciAppEvExecutorQueue - peerLciCohEvExecutorQueue - peerLciAppEvExecutorQueue - loadCohEvExecutorQueue - loadAppEvExecutorQueue
criticalQLogThreshold	String	O	1	Indicates the percentage (%) value for queue usage threshold upon reaching which a "critical" alert is raised.	0-100%	85%
majorQLogThreshold	String	O	1	Indicates the percentage (%) value for queue usage threshold upon reaching which a "major" alert is raised.	0-100%	75%
minorQLogThreshold	String	O	1	Indicates the percentage (%) value for queue usage threshold upon reaching which a "minor" alert is raised.	0-100%	65%

Queue names and Usages

The following lists the queue names and their usages:

Worker queue names

- `scpDownstreamExecutorQueue`: Downstream (message received from consumer) message handling thread pool queue
- `scpNrfProxyDownstreamExecutorQueue`: Downstream message handling thread pool queue for `nrfProxy`
- `scpUpstreamExecutorQueue`: Upstream (response received) message handling thread pool queue
- `scpClientExecutorQueue`: Currently not in use
- `scpUpdateSSLCertsQueue`: Thread pool queue for all the ssl certificate related threads
- `scpMediationDownstreamExecutorQueue`: Downstream message handling thread pool queue for mediation
- `scpReconfigureEgressRLExecutorQueue`: RateLimiter thread pool queue
- `scpTrafficFeedExecutorQueue`: Traffic feed thread pool queue

NRF Proxy Queue Names

- `scpDownstreamExecutorQueue`: Downstream(message received from Worker) message handling thread pool queue
- `scpUpstreamExecutorQueue`: Upstream (response received) message handling thread pool queue

Notification Queue Names

- `notificationQueue`: If a notification arrives at SCP, it is placed in the notification queue, which has a capacity of 5000
- `waitingQueue`: The notification is removed from the notification queue and added to the waiting queue, which has a capacity of 5000 for each `nf` type
- `runQueue`: Finally, the notification is moved from `waitingQueue` to `runQueue`. The notification is processed from `runQueue`; capacity is 40.

Cache Queue Names

- `accessTokenCohEvExecutorQueue`: A queue the cache service uses to service access token coherence requests.
- `accessTokenAppEvExecutorQueue`: A queue the cache service uses to serve access token application requests.
- `scpCacheExecutorQueue`: SCP cache executor queue for the thread pool used to serve global rate-limiting coherence requests.

Load Manager Names

- `sutLciCohEvExecutorQueue`: A queue the Load Manager service uses to service LCI coherence event requests.
- `sutLciAppEvExecutorQueue`: A queue the Load Manager service uses to service LCI application event requests.
- `peerLciCohEvExecutorQueue`: A queue that the Load Manager service uses to service requests for peer LCI coherence events.
- `peerLciAppEvExecutorQueue`: A queue that the Load Manager service uses to service requests for peer LCI application event services.
- `loadCohEvExecutorQueue`: A queue that the Load Manager service uses to service load coherence event requests.

- `loadAppEvExecutorQueue`: A queue that the Load Manager service uses to service load application event requests.

Note

All queue capacities are 10,000 for worker and NRF queues. These queue capacities are not configurable and only allow threshold value updates.

The following data model is defined to specify thread related configurations.

Table 2-272 ThreadWatchDogScpServiceConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Values
type	Type	M	1	Indicates the type of configuration to identify whether the value is single or range.	VALUE	VALUE
value	List<ThreadWatchDogConfig>	M	1	Indicates the list of values that specify the thread information configurations.	List of ThreadWatchDogConfig. For more information, see Table 2-272 .	For information about default values, see Table 2-272 .

Table 2-273 ThreadWatchDogConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Value
enableThreadWatchDog	Boolean	M	1	Specifies whether to enable or disable liveness failures. If this parameter is set to true, liveness fails whenever the watchdog reports a stuck or deadlocked thread.	true or false	true
watchDogMonitoringInterval	int	O	1	Indicates the time interval used by watchdog to monitor if any threads are stuck. The time interval is in milliseconds.	500-10000	3000
watchDogInterval	int	O	1	Indicates the maximum time allowed for threads to be nonresponsive. Watchdog uses this time to determine if a thread is stuck. The time interval is in milliseconds. For example, if watchDogInterval is 10s and a thread does not respond for 10s, then watchdog marks that thread as stuck or nonresponsive.	5000-90000	9000 Note: Default value for scpc-notification micro-service for r15 deployment is 15m, for example, 900000

Table 2-273 (Cont.) ThreadWatchDogConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Value
watchDogFailureCount	int	O	1	Indicates the maximum number of times threadWatchDog attempts to check if a thread is stuck before marking the thread as hung or stuck. For instance, if this value is 3, then the watchdog will check if a thread is stuck for 3 times continuously before marking it as stuck/hung.	1-25	5

The following data model is defined to specify inter pod resiliency configurations.

Table 2-274 ConnectivityWatchDogServiceConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Values
type	Type	M	1	Indicates the type of configuration to identify whether the value is single or range.	VALUE	VALUE
value	List<ConnectivityWatchDogConfig>	M	1	Indicates the list of values that specify the pod resiliency configurations.	List of ConnectivityWatchDogConfig. For more information, see Table 2-274 .	For information about default values, see Table 2-274 .

Table 2-275 ConnectivityWatchDogConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Value
enableConnectivityWatchDog	Boolean	M	1	Specifies whether to enable or disable interpod resiliency check.	true or false	true
connectivityMonitoringInterval	int	O	1	Indicates the time interval for resiliency in milliseconds.	500-10000	1000
connectivityRetryThreshold	int	O	1	Indicates the maximum number of attempts to be made if any pod is not reachable.	0-5	2
connectivityResponseTimeout	int	O	1	Indicates the maximum response timeout in milliseconds for the client to error out.	500-10000	2000
connectivityRetryInterval	int	O	1	Indicated the time interval between retries in milliseconds	500-10000	500

The following data model is defined to specify routing options configurations.

Table 2-276 RoutingOptionsScpServiceConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Values
type	Type	M	1	Indicates the type of configuration to identify whether the value is single or range.	VALUE	VALUE
value	List<RoutingOptionsConfig>	M	1	Indicates the list of values that specify the pod resiliency configurations.	List of RoutingOptionsConfig. For more information, see Table 2-277 .	For information about default values, see Table 2-277 .

Table 2-277 RoutingOptionsConfig

Field Name	Data Type	P	Cardinality	Description	Allowed Values	Default Value
responseTimeout	int	M	1	Indicates the maximum response timeout in seconds.	0-10	1
maxRetryAttempts	int	M	1	Indicates the maximum number of attempts to establish the connection.	0-5	0

Micro-service data model

The list of service specific data model are as follows:

SCPC-NOTIFICATION

The SCP service configuration API uses the following data models for scpc-notification service:

- ScpServiceConfigValue
- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig

Request Body

```
{
  "serviceName": "scpc-notification",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "notificationQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "waitingQueue",
```



```

        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    },
    {
        "queueName": "runQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    }
]
},
"connectivityWatchDogInfo": {
    "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
    }
},
"notificationThreadWatchDogInfo": {
    "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
    }
}
}
}
}

```

Response Body

```

{
  "serviceName": "scpc-notification",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "notificationQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "waitingQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "runQueue",
          "criticalQLogThreshold": "85%",

```

```

        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    }
  ],
  },
  "connectivityWatchDogInfo": {
    "value": {
      "connectivityMonitoringInterval": 1000,
      "enableConnectivityWatchDog": true,
      "connectivityRetryThreshold": 3,
      "connectivityResponseTimeout": 5000,
      "connectivityRetryInterval": 1000
    }
  },
  "notificationThreadWatchDogInfo": {
    "value": {
      "enableThreadWatchDog": true,
      "watchDogMonitoringInterval": 1000,
      "watchDogInterval": 9000,
      "watchDogFailureCount": 1
    }
  }
}
}
}

```

SCPC-WORKER

The SCP service configuration API uses the following data models for the scp-worker service:

- ScpServiceConfigValue
- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig
- RoutingOptionsScpServiceConfig

Request Body

```

{
  "serviceName": "scp-worker",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "scpDownstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpNrfProxyDownstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpUpstreamExecutorQueue",

```

```

        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    },
    {
        "queueName": "scpClientExecutorQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    },
    {
        "queueName": "scpUpdateSSLCertsQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    },
    {
        "queueName": "scpMediationDownstreamExecutorQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    },
    {
        "queueName": "scpReconfigureEgressRLExecutorQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    }
]
},
"routingOptions": {
    "value": {
        "scpc-notification": {
            "responseTimeout": "1s",
            "maxRetryAttempts": 0
        }
    }
},
"threadWatchDogInfo": {
    "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
    }
},
"connectivityWatchDogInfo": {
    "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
    }
},
"podOverloadControl": {

```

```

    "cpuOverloadConfig": {
      "enabled": true
    },
    "pendingTransactionOverloadConfig": {
      "enabled": true
    }
  }
}

```

Response Body

```

{
  "serviceName": "scp-worker",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "scpDownstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpNrfProxyDownstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpUpstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpClientExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpUpdateSSLCertsQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpMediationDownstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        }
      ]
    }
  }
}

```

```

        "queueName": "scpReconfigureEgressRLExecutorQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    }
  ],
  "routingOptions": {
    "value": {
      "scpc-notification": {
        "responseTimeout": "1s",
        "maxRetryAttempts": 0
      }
    }
  },
  "threadWatchDogInfo": {
    "value": {
      "enableThreadWatchDog": true,
      "watchDogMonitoringInterval": 1000,
      "watchDogInterval": 9000,
      "watchDogFailureCount": 1
    }
  },
  "connectivityWatchDogInfo": {
    "value": {
      "connectivityMonitoringInterval": 1000,
      "enableConnectivityWatchDog": true,
      "connectivityRetryThreshold": 3,
      "connectivityResponseTimeout": 5000,
      "connectivityRetryInterval": 1000
    }
  },
  "podOverloadControl": {
    "cpuOverloadConfig": {
      "enabled": true
    },
    "pendingTransactionOverloadConfig": {
      "enabled": true
    }
  }
}

```

SCPC-NRFPROXY

The SCP service configuration API uses the following data models for scp-nrfproxy service:

- ScpServiceConfigValue
- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig

Request Body

```

{
  "serviceName": "scp-nrfproxy",
  "scpServiceConfigs": {

```

```

"taskInfo": {
  "type": "VALUE",
  "value": [
    {
      "queueName": "scpDownstreamExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    },
    {
      "queueName": "scpUpstreamExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    }
  ]
},
"nrfThreadWatchDogInfo": {
  "value": {
    "enableThreadWatchDog": true,
    "watchDogMonitoringInterval": 1000,
    "watchDogInterval": 9000,
    "watchDogFailureCount": 1
  }
},
"connectivityWatchDogInfo": {
  "value": {
    "connectivitytMonitoringInterval": 1000,
    "enableConnectivityWatchDog": true,
    "connectivityRetryThreshold": 3,
    "connectivityResponseTimeout": 5000,
    "connectivityRetryInterval": 1000
  }
}
}
}

```

Response Body

```

{
  "serviceName": "scp-nrfproxy",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "scpDownstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpUpstreamExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        }
      ]
    }
  }
}

```

```

        "minorQLogThreshold": "65%"
    }
  ],
  "nrfThreadWatchDogInfo": {
    "value": {
      "enableThreadWatchDog": true,
      "watchDogMonitoringInterval": 1000,
      "watchDogInterval": 9000,
      "watchDogFailureCount": 1
    }
  },
  "connectivityWatchDogInfo": {
    "value": {
      "connectivitytMonitoringInterval": 1000,
      "enableConnectivityWatchDog": true,
      "connectivityRetryThreshold": 3,
      "connectivityResponseTimeout": 5000,
      "connectivityRetryInterval": 1000
    }
  }
}

```

SCPC-CONFIGURATION

The SCP service configuration API uses the following data models for scp-nrfproxy service:

- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig

Request Body

```

{
  "serviceName": "scpc-configuration",
  "scpServiceConfigs": {
    "connectivityWatchDogInfo": {
      "value": {
        "connectivitytMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    },
    "configurationThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    }
  }
}

```

Response Body

```
{
  "serviceName": "scpc-configuration",
  "scpServiceConfigs": {
    "connectivityWatchDogInfo": {
      "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    },
    "configurationThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    }
  }
}
```

SCPC-SUBSCRIPTION

The SCP service configuration API uses the following data models for scpc-subscription service:

- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig

Request Body

```
{
  "serviceName": "scpc-subscription",
  "scpServiceConfigs": {
    "connectivityWatchDogInfo": {
      "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    },
    "subscriptionThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    }
  }
}
```



```
}
}
```

Response Body

```
{
  "serviceName": "scpc-subscription",
  "scpServiceConfigs": {
    "connectivityWatchDogInfo": {
      "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    },
    "subscriptionThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    }
  }
}
```

SCPC-AUDIT

The SCP service configuration API uses the following data models for scpc-subscription service:

- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig

Request Body

```
{
  "serviceName": "scpc-audit",
  "scpServiceConfigs": {
    "auditThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    },
    "connectivityWatchDogInfo": {
      "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    }
  }
}
```

```

    }
  }
}

```

Response Body

```

{
  "serviceName": "scpc-audit",
  "scpServiceConfigs": {
    "auditThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    },
    "connectivityWatchDogInfo": {
      "value": {
        "connectivitytMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    }
  }
}

```

SCPC-ALTERNATE-RESOLUTION

The SCP service configuration API uses the following data models for scp-nrfproxy service:

- ThreadWatchDogScpServiceConfig
- ConnectivityWatchDogServiceConfig

Request Body

```

{
  "serviceName": "scpc-alternate-resolution",
  "scpServiceConfigs": {
    "connectivityWatchDogInfo": {
      "value": {
        "connectivitytMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    }
  },
  "alternateResolutionThreadWatchDogInfo": {
    "value": {
      "enableThreadWatchDog": true,
      "watchDogMonitoringInterval": 1000,
      "watchDogInterval": 9000,

```

```

        "watchDogFailureCount": 1
    }
}
}

```

Response Body

```

{
  "serviceName": "scpc-alternate-resolution",
  "scpServiceConfigs": {
    "connectivityWatchDogInfo": {
      "value": {
        "connectivityMonitoringInterval": 1000,
        "enableConnectivityWatchDog": true,
        "connectivityRetryThreshold": 3,
        "connectivityResponseTimeout": 5000,
        "connectivityRetryInterval": 1000
      }
    },
    "alternateResolutionThreadWatchDogInfo": {
      "value": {
        "enableThreadWatchDog": true,
        "watchDogMonitoringInterval": 1000,
        "watchDogInterval": 9000,
        "watchDogFailureCount": 1
      }
    }
  }
}

```

SCP-CACHE

The SCP service configuration API uses the following data models for scp-cache service:

- ScpServiceConfigValue

Request Body

```

{
  "serviceName": "scp-cache",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "accessTokenCohEvExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "accessTokenAppEvExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        }
      ]
    }
  }
}

```

```

        {
            "queueName": "scpCacheExecutorQueue",
            "criticalQLogThreshold": "85%",
            "majorQLogThreshold": "75%",
            "minorQLogThreshold": "65%"
        }
    ]
}
}
}

```

Response Body

```

{
  "serviceName": "scp-cache",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "accessTokenCohEvExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "accessTokenAppEvExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        },
        {
          "queueName": "scpCacheExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        }
      ]
    }
  }
}

```

SCP-LOAD-MANAGER

The SCP service configuration API uses the following data models for scp-load-manager service:

- ScpServiceConfigValue

Request Body

```

{
  "serviceName": "scp-load-manager",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [

```

```

    {
      "queueName": "sutLciCohEvExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    },
    {
      "queueName": "sutLciAppEvExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    },
    {
      "queueName": "peerLciCohEvExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    },
    {
      "queueName": "peerLciAppEvExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    },
    {
      "queueName": "loadCohEvExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    },
    {
      "queueName": "loadAppEvExecutorQueue",
      "criticalQLogThreshold": "85%",
      "majorQLogThreshold": "75%",
      "minorQLogThreshold": "65%"
    }
  ]
}
}
}

```

Response Body

```

{
  "serviceName": "scp-load-manager",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": [
        {
          "queueName": "sutLciCohEvExecutorQueue",
          "criticalQLogThreshold": "85%",
          "majorQLogThreshold": "75%",
          "minorQLogThreshold": "65%"
        }
      ]
    }
  }
}

```

```

{
  {
    "queueName": "sutLciAppEvExecutorQueue",
    "criticalQLogThreshold": "85%",
    "majorQLogThreshold": "75%",
    "minorQLogThreshold": "65%"
  },
  {
    "queueName": "peerLciCohEvExecutorQueue",
    "criticalQLogThreshold": "85%",
    "majorQLogThreshold": "75%",
    "minorQLogThreshold": "65%"
  },
  {
    "queueName": "peerLciAppEvExecutorQueue",
    "criticalQLogThreshold": "85%",
    "majorQLogThreshold": "75%",
    "minorQLogThreshold": "65%"
  },
  {
    "queueName": "loadCohEvExecutorQueue",
    "criticalQLogThreshold": "85%",
    "majorQLogThreshold": "75%",
    "minorQLogThreshold": "65%"
  },
  {
    "queueName": "loadAppEvExecutorQueue",
    "criticalQLogThreshold": "85%",
    "majorQLogThreshold": "75%",
    "minorQLogThreshold": "65%"
  }
}
]
}
}

```

Resource Definition

GET REST API

This resource retrieves routing options for all the applications.

Resource URI: /ocscp/scpc-configuration/{version}/scp-service-config

Table 2-278 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
scpServiceConfigs	M	1..N	200 OK	Retrieves configurations for SCP microservices.

This resource retrieves routing options for the application specified by serviceName.

Resource URI: /ocscp/scpc-configuration/{version}/scp-service-config/{serviceName}

Table 2-279 Path Parameters

Name	Data Type	P	Description
serviceName	String	M	Retrieves configurations on microserviceName. The supported values are worker, notification, and nrproxy.

Table 2-280 Data Structures Supported by the GET Response Body on this Resource

Data Type	P	Cardinality	Response Code	Description
scpServiceConfigs	M	1	200 OK	Indicates service configurations for SCP microservices.
ProblemDetails	M	1	404	Returns when an invalid combination or more than two query parameters are provided.

Curl GET/GET ALL command**GET ALL**

Success Response

```
curl -X GET http://10.75.213.144:31343/ocscp/scpc-configuration/v1/scp-
service-config -H 'accept: application/json' -v
```

```
* About to connect() to 10.75.213.144 port 31343 (#0)
* Trying 10.75.213.144...
* Connected to 10.75.213.144 (10.75.213.144) port 31343 (#0)
> GET /ocscp/scpc-configuration/v1/scp-service-config HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 10.75.213.144:31343
> accept: application/json
>
< HTTP/1.1 200 OK
< Connection: keep-alive
< Transfer-Encoding: chunked
< Content-Type: application/json
< Date: Thu, 17 Nov 2022 06:12:26 GMT
<
```

```
{
  "serviceName": "scp-nrproxy",
  "scpServiceConfigs": {
    "taskInfo": {
      "type": "VALUE",
      "value": {
        [
          {
            "queueName": "scpDownstreamExecutorQueue",
            "criticalQLogThreshold": "85%",
            "majorQLogThreshold": "75%",
            "minorQLogThreshold": "65%",
            "queueName": "scpUpstreamExecutorQueue",
            "criticalQLogThreshold": "85%",
            "majorQLogThreshold": "75%",
            "minorQLogThreshold": "65%"
          }
        ],
        "nrfThreadWatchDogInfo": {
          "value": {
            "enableThreadWatchDog": true,
            "watchDogMonitoringInterval": 1000,
            "watchDogInterval": 9000,
            "watchDogFailureCount": 1,
            "connectivityWatchDogInfo": {
              "value": {
                "connectivityMonitoringInterval": 1000,
                "enableConnectivityWatchDog": true,
                "connectivityRetryThreshold": 3,
                "connectivityResponseTimeout": 5000,
                "connectivityRetryInterval": 1000
              }
            }
          }
        }
      }
    },
    "serviceName": "scp-worker",
    "scpServiceConfigs": {
```

```

{"taskInfo":{"type":"VALUE","value":
[{"queueName":"scpDownstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpNrFProxyDownstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpUpstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpClientExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpUpdateSSLCertsQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpMediationDownstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpReconfigureEgressRLExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"}]}, "routingOptions":
{"value":{"scpc-notification":
{"responseTimeout":"1s","maxRetryAttempts":0}}, "threadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1}}, "connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}}}, {"serviceName":"scpc-alternate-resolution","scpServiceConfigs":{"connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}, "alternateResolutionThreadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1}}}}, {"serviceName":"scpc-audit","scpServiceConfigs":{"auditThreadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1}}, "connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}}}, {"serviceName":"scpc-configuration","scpServiceConfigs":
{"connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}, "configurationThreadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1}}}}, {"serviceName":"scpc-notification","scpServiceConfigs":{"taskInfo":{"type":"VALUE","value":
[{"queueName":"notificationQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"waitingQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"runQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"}]}, "connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}, "notificationThreadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1}}}}, {"serviceName":"scpc-subscription","scpServiceConfigs":{"connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}, "subscriptionThreadWatchDogInfo":{"value":

```



```
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1}}}]}
```

GET Command

Success Response

```
curl -X GET http://10.75.213.144:31343/ocscp/scpc-configuration/v1/scp-  
service-config/scp-worker -H 'accept: application/json' -v
```

```
* About to connect() to 10.75.213.144 port 31343 (#0)
* Trying 10.75.213.144...
* Connected to 10.75.213.144 (10.75.213.144) port 31343 (#0)
> GET /ocscp/scpc-configuration/v1/scp-service-config/scp-worker HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 10.75.213.144:31343
> accept: application/json
>
< HTTP/1.1 200 OK
< Connection: keep-alive
< Transfer-Encoding: chunked
< Content-Type: application/json
< Date: Thu, 17 Nov 2022 06:17:08 GMT
<
{"serviceName":"scp-worker","scpServiceConfigs":{"taskInfo":
{"type":"VALUE","value":
[{"queueName":"scpDownstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpNrFProxyDownstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpUpstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpClientExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpUpdateSSLCertsQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpMediationDownstreamExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"},
{"queueName":"scpReconfigureEgressRLExecutorQueue","criticalQLogThreshold":"85%","majorQLogThreshold":"75%","minorQLogThreshold":"65%"}]},
"routingOptions":
{"value":{"scpc* Connection #0 to host 10.75.213.144 left intact
-notification":
{"responseTimeout":"1s","maxRetryAttempts":0}}},"threadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterval":9000,"watchDogFailureCount":1},"connectivityWatchDogInfo":{"value":
{"connectivityMonitoringInterval":1000,"enableConnectivityWatchDog":true,"connectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRetryInterval":1000}}}]}
```

Failure Response

```
curl -X 'GET' 'http://10.75.224.107:31368/ocscp/scpc-configuration/v1/scp-
service-config/Worker1' -H 'accept: application/json' -v
```

```
* About to connect() to 10.75.224.107 port 31368 (#0)
* Trying 10.75.224.107...
* Connected to 10.75.224.107 (10.75.224.107) port 31368 (#0)
> GET /ocscp/scpc-configuration/v1/scp-service-config/Worker1 HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 10.75.224.107:31368
> accept: application/json
>
< HTTP/1.1 404 Not Found
< Connection: keep-alive
< Transfer-Encoding: chunked
< Content-Type: application/problem+json
< Date: Thu, 18 Aug 2022 09:08:36 GMT
<
* Connection #0 to host 10.75.224.107 left intact
{"title":"Not Found","status":"404","detail":"Scp_Service_Configuration for
given serviceName not found . Please refer to the User Guide.,"instance":"/
ocscp/scpc-configuration/v1/scp-service-config/
Worker1","cause":"DATA_NOT_FOUND"}
```

PUT REST API

This resource configures routing options for the application.

Resource URI: /ocscp/scpc-configuration/{version}/scp-service-config/{appname}

Table 2-281 Data Structures Supported by the PUT Request Body on this Resource

Data Type	P	Cardinalit y	Description
scpSserviceConfigs	1	M	scp-service-configs for the application.

Table 2-282 Data structures supported by the PUT Response Body on this resource

Data Type	P	Cardinality	Response Code	Description
scpServiceConfigs	M	1	200 OK	Indicates service configurations for SCP microservices.
ProblemDetails	M	1	400/404	Returns when an invalid combination or more than two query parameters are provided.

Curl PUT Command

Success Response

```
curl -X 'PUT' 'http://10.75.213.144:31343/ocscp/scpc-configuration/v1/scp-
service-config/scpc-alternate-resolution' \
    "connectivityRetryInterval": 1000

> -H 'accept: application/json' \
> -H 'Content-Type: application/json' \
> -d '{
>   "serviceName": "scpc-alternate-resolution",
>   "scpServiceConfigs": {
>     "connectivityWatchDogInfo": {
>       "value": {
>         "connectivitytMonitoringInterval": 1000,
>         "enableConnectivityWatchDog": true,
>         "connectivityRetryThreshold": 3,
>         "connectivityResponseTimeout": 5000,
>         "connectivityRetryInterval": 1000
>       }
>     },
>     "alternateResolutionThreadWatchDogInfo": {
>       "value": {
>         "enableThreadWatchDog": true,
>         "watchDogMonitoringInterval": 1000,
>         "watchDogInterval": 9000,
>         "watchDogFailureCount": 1
>       }
>     }
>   }
> }'
```

```
{"serviceName":"scpc-alternate-resolution","scpServiceConfigs":
{"connectivityWatchDogInfo":{"value":
{"connectivitytMonitoringInterval":1000,"enableConnectivityWatchDog":true,"con
nectivityRetryThreshold":3,"connectivityResponseTimeout":5000,"connectivityRet
ryInterval":1000}},"alternateResolutionThreadWatchDogInfo":{"value":
{"enableThreadWatchDog":true,"watchDogMonitoringInterval":1000,"watchDogInterv
al":9000,"watchDogFailureCount":1}}}}
```

Failure Response 1

```
curl -X 'PUT' 'http://10.75.224.107:31368/ocscp/scpc-configuration/v1/scp-
service-config/Notification' -H 'accept: application/json' -H 'Content-
Type: application/json' -d '{
```

```
"serviceName": "NOTIFICATION",
"scpServiceConfigs": {
  "TaskInfoScpConfig": {
    "type": "VALUE",
    "value": [
      {
        "queueName": "notificationQueue",
        "criticalQLogThreshold": "86%",
```

```

        "majorQLogThreshold": "76%",
        "minorQLogThreshold": "66%"
    },
    {
        "queueName": "waitingQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    },
    {
        "queueName": "runQueue",
        "criticalQLogThreshold": "85%",
        "majorQLogThreshold": "75%",
        "minorQLogThreshold": "65%"
    }
  ]
}
}
>
> '
{"timestamp":"2022-08-18T09:13:28.253+00:00","status":400,"error":"Bad
Request","path":"/ocscp/scpc-configuration/v1/scp-service-config/
Notification"}

```

Failure Response 2

```
curl -X 'PUT' 'http://10.75.224.107:31368/ocscp/scpc-configuration/v1/scp-
service-config/Subscription' \
```

```

> -H 'accept: application/json' \
> -H 'Content-Type: application/json' \
> -d '{
>   "serviceName": "subscription",
>   "scpServiceConfigs": {
>     "TaskInfoScpConfig": {
>       "type": "VALUE",
>       "value": [
>         {
>           "queueName": "notificationQueue",
>           "criticalQLogThreshold": "86%",
>           "majorQLogThreshold": "76%",
>           "minorQLogThreshold": "66%"
>         },
>         {
>           "queueName": "waitingQueue",
>           "criticalQLogThreshold": "85%",
>           "majorQLogThreshold": "75%",
>           "minorQLogThreshold": "65%"
>         }
>       ]
>     }
>   }
> }
>
>   "criticalQLogThreshold": "85%",
>   "majorQLogThreshold": "75%",
>   "minorQLogThreshold": "65%"
> },
> {
>   "queueName": "runQueue",
>   "criticalQLogThreshold": "85%",

```

```

>         "majorQLogThreshold": "75%",
>         "minorQLogThreshold": "65%"
>     }
> ]
> }
> }
> }'
{"title":"Not Found","status":"404","detail":"Scp_Service_Configuration for
given serviceName not found . Please refer to the User Guide.,"instance":"/
ocscp/scpc-configuration/v1/scp-service-config/
Subscription","cause":"DATA_NOT_FOUND"}

```

2.32 Configuring Load Control Information

This section describes REST API configurations required for the Load Control based on the Load Control Information (LCI) Header feature:

Resource

The following table describes the resource URIs and the corresponding HTTP methods for the to retrieve, add, or update SCP features.

Table 2-283 Resources

Resource Name	Resource URI	HTTP Method	Description
scp-features	/ocscp/scpc-configuration/v1/scp-features/lci	GET	Retrieves records based on featureName as a path variable.
scp-features	/ocscp/scpc-configuration/v1/scp-features/lci	PUT	To enable/disable the scp feature and its parameters.

Data Model

Request Body

The following table describes LCISpecificConfig data types.

Table 2-284 LCISpecificConfig

Field Name	Data Type	P	Default Value	Range	Description
scpLciConveyanceEnable	Boolean	M	false	NA	This parameter enables or disables the addition of SCP LCI.
relayPeerLci	Boolean	M	true	NA	This parameter enables or disables the relay of the peer's LCI.
scpLciConveyanceInterval	Integer	O	5000 milliseconds	1000 milliseconds - 3600000 milliseconds	This parameter governs the periodicity of LCI conveyance. After the duration specified in this parameter, SCP LCI is transmitted to peers.
scpLciConveyanceMinLoadChange	Integer	M	5	5 - 25	This parameter indicates the minimum eligible change in load while conveying LCI.

Table 2-284 (Cont.) LCISpecificConfig

Field Name	Data Type	P	Default Value	Range	Description
scpLciConveyanceMinLoadThreshold	Integer	M	30	0-60	This parameter allows SCP to define a minimum load change threshold that can trigger the generation of an LCI header and report it to peers if allowed.
scpLciConveyancetoUnknownPeer	Boolean	M	false	NA	This parameter indicates whether SCP can send its LCI to an unknown peer NF.
peerLciProcessingMinLoadChange	Integer	M	5	0-25	This parameter allows SCP to define a minimum load change in a peer NF's load as indicated in LCI, which can trigger a re-evaluation of routing rules.
unknownPeerLciExpiry	Integer	M	300 seconds	30 seconds - 900 seconds	This parameter specifies the minimum number of seconds required to remove an unknown peer's LCI from cache.

Response Body

The following table describes response body data models that vary based on the REST operation status.

Table 2-285 Response Body Data Type

Data Type	P	Cardinality	Response Codes	Description
array(SCPFeaturesWrapper)	M	1	200 OK	Indicates the list of SCP features (SCPFeaturesWrapper) matching criteria.
ProblemDetails	M	1	404 NOT FOUND	Returns when the data is not found for given query parameters.

JSON Format

Current JSON Format

```
{
  "featureName": "lci",
  "enabled": false,
  "featureSpecificConfig": {
    "scpLciConveyanceEnable": false,
    "relayPeerLci": true,
    "scpLciConveyanceInterval": 2000,
    "scpLciConveyanceMinLoadChange": 5,
    "scpLciConveyanceMinLoadThreshold": 30,
    "scpLciConveyancetoUnknownPeer": false,
    "peerLciProcessingMinLoadChange": 5,
    "unknownPeerLciExpiry": 300
  }
}
```

```
}
}
```

Resource Definition

GET REST API

This section describes the resource to fetch all the SCP feature details (SCPFeaturesWrapper) based on the query parameters.

If no query parameter is provided, all the SCP feature detail are returned.

Resource URI: `ocscp/scpc-configuration/v1/scp-features/lci`

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-286 Parameters Supported by the GET Method

Field Name	Data Type	P	Description
featureName	String	O	Specifies the identity of featureName for which SCP features are fetched.

Note

featureName is a valid combination of query parameter or path variable.

Table 2-287 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
array(SCPFeaturesWrapper)	M	1	200 OK	Indicates the list of LCI header Info (SCPFeaturesWrapper) (or) Get specific record based on query parameters.
ProblemDetails	M	1	404 NOT FOUND	Returns when the data is not found for given query parameters.

Example

Successful response - 1

```
curl -X GET "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/scp-features/lci" -H "accept: application/json"
```

```
Code: 200 {
  {
    "featureName": "lci",
    "enabled": false,
    "featureSpecificConfig": {
      "scpLciConveyanceEnable": false,
      "relayPeerLci": true,
```

```

        "scpLciConveyanceInterval": 2000,
        "scpLciConveyanceMinLoadChange": 5,
        "scpLciConveyanceMinLoadThreshold": 30,
        "scpLciConveyanceToUnknownPeer": false,
        "peerLciProcessingMinLoadChange": 5,
        "unknownPeerLciExpiry": 300
    }
}

```

Failure case 1

```

curl -X GET "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/scp-features/lciheader_1" -H "accept: application/json"
Response Body:
{
  "title": "Not Found",
  "status": "404",
  "detail": "SCP Features configuration data not found against given query parameter(s), Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/scp-features/lciheader_1",
  "cause": "DATA_NOT_FOUND"
}

```

PUT REST API

This resource adds or updates the SCP feature interplmn routing configuration using the request body.

Resource URI: ocscp/scpc-configuration/v1/scp-features/lci

Table 2-288 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
SCPFeaturesWrapper	M	1	200 OK	Indicates the SCP feature lciheader configuration data.
ProblemDetails	M	1	400 BAD REQUEST	Returns the ProblemDetails structure as defined in 3GPP TS 29.571 section 5.2.4.1.

Example

Successful response:

```

curl -X PUT "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/scp-features/lciheader" -H "accept: */*" -H "Content-Type: application/json" -d
"
{
  "featureName": "lci",
  "enabled": false,
  "featureSpecificConfig": {
    "scpLciConveyanceEnable": false,
    "relayPeerLci": true,
    "scpLciConveyanceInterval": 2000,
    "scpLciConveyanceMinLoadChange": 5,
    "scpLciConveyanceMinLoadThreshold": 30,

```



```

    "scpLciConveyancetoUnknownPeer": false,
    "peerLciProcessingMinLoadChange": 5,
    "unknownPeerLciExpiry": 300
  }
} 200 OK

```

Failure case 1:**Note**

In case SCP is not configured with local or foreign PLMNs and invalid NF type is configured for this feature, you receive a Bad Request 400 with error message.

```

curl -X PUT "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/scp-features/lci"-H "accept: */*" -H "Content-Type: application/json"-d "
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Unknown Feature: lxi not supported. Please refer to the User Guide.",
  "instance": "/ocscp/scpc-configuration/v1/scp-features/lxi",
  "cause": "MANDATORY_IE_INCORRECT"
}
400 Bad Request

```

Failure case 2:

```

curl -X PUT "http://10.75.214.171:30970/ocscp/scpc-configuration/v1/scp-features/lci"-H "accept: */*" -H "Content-Type: application/json"-d "
{
  "title": "Bad Request",
  "status": "400",
  "detail": "SCP conveyance interval range should be between 100ms to 3600ms",
  "instance": "/ocscp/scpc-configuration/v1/scp-features/lci",
  "cause": "MANDATORY_IE_INCORRECT"
}
400 Bad Request

```

2.33 Message Feed Configurations

This section provides information about message feed Data Director configurations at SCP.

2.33.1 Configuring Traffic Feed Data Director

This section describes the Traffic Feed Data Director configurations.

Table 2-289 Resources

Resource name	Resource URI	HTTP method or custom operation	Description
5gsbi-traffic-feed/data-director-config	/ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/data-director-config	GET	Retrieves Traffic Feed Data Director Config configured at SCP.
5gsbi-traffic-feed/data-director-config	/ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/data-director-config	PUT	Adds Traffic Feed Data Director Config configured at SCP.
5gsbi-traffic-feed/data-director-config	/ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/data-director-config	PATCH	Updates Traffic Feed Data Director Config configured at SCP.

Data Model

Request Body

Table 2-290 trafficFeedDataDirectorConfig

Field Name	Data Type	Default Value	Description
kafkaPartitionSelectionLogic	String	RoundRobin	Indicates the logic to select Kafka partitions to route messages. RoundRobin: All the messages are distributed across all the available partitions in a round-robin order. KeyBased: Messages with the same correlation-id are routed to the same partition. This ensures the same transaction messages are routed to the same partition.
deliveryTimeoutMs	Integer	5000 milliseconds	Indicates an upper bound on the time to report success or failure to the SCP application from the Kafka Producer Library. When this period expires, the Kafka producer reports a failure to application. The value of this configuration should be greater than or equal to the sum of requestTimeoutMs and lingerMs.
trafficFeedBootstrapServer	Object with host and port info host String port Integer	NA	A list of host or port pairs to use for establishing the initial connection to the Kafka cluster.
topic	String	NA	Topic name that SCP uses to write on Kafka Broker.
securityProtocol	String	None	Protocol used to communicate with brokers. The values are: PLAINTEXT, SSL, SASL_PLAINTEXT, SASL_SSL.

Table 2-290 (Cont.) trafficFeedDataDirectorConfig

Field Name	Data Type	Default Value	Description
saslMechanism	String	None Recommended: PLAIN	SASL mechanism used for client connections. The values are: PLAIN.
keySerializer	String	Json	Key serialization Two Serialization option supported: JSON and STRING.
valueSerializer	String	Json	Value serialization Two Serialization option Supported JSON,STRING
acks	String	0	The number of acknowledgments the producer NF requires the leader to have received before considering a request complete. Available options: 0 - The producer NF never waits for an acknowledgment from the server at all. 1 - The producer NF responds after the leader write without waiting for acknowledgment from all the followers. all - The producer NF waits for the full set of in-sync replicas to acknowledge the record. Note: Parameter to change the behavior of underlying kafka library.
retryCount	Integer	0	Number of times producer NFs send data to broker in case of error. Note: Parameter to change the behavior of underlying kafka library.
retryBackoffMs	Long	100	The amount of time to wait before attempting to retry a failed request to a given topic partition. Note: Parameter to change the behavior of underlying kafka library.
requestTimeoutMs	Integer	1000	The maximum amount of time the client waits for the response of a request. Note: Parameter to change the behavior of underlying kafka library. Oracle Support shall be consulted before modifying the default value. The value of this parameter must not be more than the threadWatchDog time of the scp-worker microservice.
trafficfeedBlockingSendTimeoutMs	Integer	500	The amount of time for which the producer will block sending messages to the broker when the producer is not able to connect to the broker. maxValue: 200000, minValue: 100 Note: Parameter to change the behavior of underlying kafka library. Increasing this value more than the threadWatchDog time of the worker microservice can result in a worker pod crash.

Table 2-290 (Cont.) trafficFeedDataDirectorConfig

Field Name	Data Type	Default Value	Description
trafficfeedDegradationperiod	Integer	1000	The amount of time the producer waits before sending to the broker when a previous attempt to connect to the broker has failed. max Value : 10000, min Value : 10 Note : Parameter to change the behavior of underlying kafka library.
trafficfeedConsecutiveFailures	Integer	10	The number of consecutive failures allowed by SCP before blocking the producer from sending messages. max Value : 100, min Value : 1 Note : Parameter to change the behavior of underlying kafka library.
batchSize	Integer	16384	It specifies the batch size in bytes based on which records are collected together into fewer requests and sent. Note : Parameter to change the behavior of underlying kafka library.
lingerMs	Long	2	It specifies the amount of time for which the producer will wait to allow other records to be sent so that the sends can be batched together. Note : Parameter to change the behavior of underlying kafka library.
trafficfeedMaxBlockMsConfig	Long	10	The configuration controls how long the KafkaProducer's send() method will block. Note : Parameter to change the behavior of underlying kafka library.
bufferMemory	Long	33554432	The total bytes of memory the producer can use to buffer records waiting to be sent to the server. Note : Parameter to change the behavior of underlying kafka library.

Response body data model varies based on Rest operation status. Details can be found in the subsequent sections.

Response Body

Table 2-291 Response Body

Data Type	P	Cardinality	Response codes	Description
trafficFeedDataDirectorConfig	M	1	200 OK	List of Producer Configuration matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when invalid input are provided.

JSON Format

```
{
  "kafkaPartitionSelectionLogic":"RoundRobin",
  "trafficFeedBootStrapServerList": [
    {
      "host": "10.75.212.228",
      "port": 31215
    }
  ],
  "securityProtocol": "none",
  "saslmMechanism": "none",
  "keySerializer": "json",
  "valueSerializer": "json",
  "acks": "0",
  "retryCount": 0,
  "deliveryTimeoutMs":120000,
  "retryBackoffMs": 100,
  "requestTimeoutMs": 1001000,
  "trafficfeedBlockingSendTimeoutMs": 500,
  "trafficfeedDegradationperiod": 1000,
  "trafficfeedConsecutiveFailures": 10,
  "batchSize": 16384,
  "lingerMs": 2,
  "trafficfeedMaxBlockMsConfig": 10,
  "bufferMemory": 33554432
}
```

Resource Definition

GET REST API:

Resource to fetch the Traffic server Configuartion Info Details based on the json version.

Resource URI: /ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/
data-director-config

Table 2-292 Data structures supported by the GET Response Body

Data Type	P	Cardina lity	Response codes	Description
trafficFeedDataDire ctorConfig	M	1	200 OK	Producer Configuration Info Data

PUT REST API:

Resource to add or update the Traffic server of Producer Configuration using the Request Body.

Resource URI: /ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/
data-director-config

Table 2-293 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response codes	Description
trafficFeedDataDirectorConfig(json)	M	1	200 OK	A list of host or port pairs to use for establishing the initial connection to the Kafka cluster.
String	M	1	400 BAD REQUEST	Returns Problem description when invalid input is provided.

PATCH REST API:

Resource to add or update the Traffic server Configuration using the Request Body.

Resource URI: /ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/data-director-config

Table 2-294 URI Query Parameters Supported by the PATCH Method

Name	Data Type	P	Cardinality	Description
patchDocument	String	M	1	patchDocument need to be send Example: [{"op":"add","path": "/keySerializer", "value": "JSON"}], [{"op":"add","path": "/topic", "value": "scpTopic1"}], [{ "op":"replace", "path":"/trafficFeedBootstrapServer", "value": [{"host":"12.11.11.11", "port":8095 } }]
String	M	1	400 BAD REQUEST	Returns Problem description when invalid input is provided.

2.33.2 Configuring Traffic Feed Trigger Point Config

This section describes the Traffic Feed Trigger Point configurations.

Table 2-295 Resources

Resource name	Resource URI	HTTP method or custom operation	Description
5gsbi-traffic-feed/trigger-point	/ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/trigger-point	GET	Retrieves all the Traffic Feed Trigger Point configuration at SCP.
5gsbi-traffic-feed/trigger-point	/ocscp/scpc-configuration/{version}/5gsbi-traffic-feed/trigger-point/{ruleName}	GET	Retrieves Traffic Feed Trigger Point configurations at SCP for given ruleName.

Table 2-295 (Cont.) Resources

Resource name	Resource URI	HTTP method or custom operation	Description
5gsbi-traffic-feed/ trigger-point	/ocscp/scpc-configuration/ {version}/5gsbi-traffic-feed/trigger-point/{ruleName}	PUT	Updates Traffic Feed Trigger Point configuration at SCP for given ruleName.
5gsbi-traffic-feed/ trigger-point	/ocscp/scpc-configuration/ {version}/5gsbi-traffic-feed/trigger-point/{ruleName}	PATCH	Updates Traffic Feed Trigger Point configuration at SCP for given ruleName.
5gsbi-traffic-feed/ trigger-point	/ocscp/scpc-configuration/ {version}/5gsbi-traffic-feed/trigger-point/{ruleName}	DELETE	Removes Traffic Feed Trigger Point configurations at SCP for given ruleName.

Data Model**Request Body****Table 2-296 trafficFeedTriggerPointConfig**

Field Name	Data Type	P	Description
ruleName	String	M	The rule's name must be in string format.It must have a unique rule name.

Table 2-296 (Cont.) trafficFeedTriggerPointConfig

Field Name	Data Type	P	Description
serviceName	String	O	The name of the services for which rule is applied: nnrf-nfm, nnrf-disc, nudm-sdm, nudm-uecm, nudm-ueau, nudm-ee, nudm-pp, namf-comm, namf-evts, namf-mt, namf-loc, nsmf-pdusession, nsmf-event-exposure, nausf-auth, nausf-sorprotection, nausf-upuprotection, nnef-pfdmanagement, npcfc-am-policy-control, npcfc-smpolicycontrol, npcfc-policyauthorization, npcfc-bdtpolicycontrol, nsmsf-sms, nssf-nssselection, nssf-nssaiavailability, nudr-dr, nudr-group-id-map, nlmf-loc, n5g-eir-eic, nbsf-management, nchf-spendinglimitcontrol, nnwdaf-eventssubscription, nnwdaf-analyticsinfo, npcfc-eventexposure, npcfc-ue-policy-control, nchf-convergedcharging, 5g-sbi-notification, nnef-eventexposure, nnef-afsessionwithqos
allowedtrafficPercentage	Integer	M	0-100% of traffic can be sent to traffic feed.
triggerPoints	Array(TriggerPoint)	M	List of trigger points to be enabled if matches. One or more of following: - RxRequest - TxRequest - RxResponse - TxResponse

Response Body

Response body data model varies based on Rest operation status. Details can be found in the subsequent sections.

Table 2-297 Response Body

Data Type	P	Cardinality	Response codes	Description
array (trafficFeedTriggerPoint config)	M	1	200 OK	List of traffic Feed configuration matching criteria.
ProblemDetails	M	1	400 BAD REQUEST	Returns when invalid input are provided.

JSON Format

```
{
  "ruleName": "string",
  "serviceName": "string",
  "trafficFeedTriggerPointConfigData":
  {
    "allowedTrafficPercentage": 0,
    "triggerPoints": [
      "RxRequest"
    ]
  }
}
```

Resource Definition**GET REST API**

Resource to fetch the message-copy-traffic-config details based on the json version.

Resource URI: /ocscp/scpc-configuration/v1/5gsbi-traffic-feed/trigger-point

Table 2-298 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
trafficFeedTriggerPointConfig	M	1	200 OK	configuration for Traffic Feed

PUT REST API

Resource to put the message-copy-traffic-config details based on the json version.

Resource URI: /ocscp/scpc-configuration/v1/5gsbi-traffic-feed/trigger-point/ruleName

Successful Response:

```
curl -X 'PUT' \
  'http://<SCP configuration FQDN>:30446/ocscp/scpc-configuration/v1/5gsbi-traffic-feed/trigger-point/nef_trafficfeed_rule' \
  -H 'accept: */*' \
  -H 'Content-Type: application/json' \
  -d '{
    "ruleName": "nef_trafficfeed_rule",
    "serviceName": "nnef-eventexposure",
    "trafficFeedTriggerPointConfigData": {
      "allowedTrafficPercentage": 70,
      "triggerPoints": [
        "RxRequest"
      ]
    }
  }'
```

Table 2-299 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response codes	Description
trafficFeedTriggerPointConfig	M	1	200 OK	configuration for Traffic Feed

PATCH REST API

Resource to add or update the message-copy-traffic-config using the Request Body.

Resource URI: /ocscp/scpc-configuration/v1/5gsbi-traffic-feed/trigger-point

Table 2-300 Data Structures Supported by the PATCH Response Body

Name	Data Type	P	Cardinality	Description
ruleName	String	M	1	Rule name for which Ingress and Egress Traffic configuration can be modified.
serviceName	String	O	1	Update serviceName for provided ruleName [{"op": "replace", "path": "/serviceName", "value": "nausf-auth"}]
trafficFeedTriggerPointConfig	Json	O	1	patchDocument need to be send example: [{"op": "replace", "path": "/trafficFeedTriggerPointConfigData/allowedTrafficPercentage", "value": "50"}] [{"op": "replace", "path": "/trafficFeedTriggerPointConfigData/triggerPoints", "value": ["RxRequest", "TxRequest"]}]

2.34 Congestion Control Configurations

This REST API is used to configure the congestion control configuration rules. The user uses this API to configure congestion control configurations, and the name of this rule is provided in Routing Options at the service level.

Resources

The following table describes the resource name to retrieve, add, update, and remove the congestion control configuration based on the query parameters.

Table 2-301 Resource Name

Resource Name	Resource URI	HTTP Method	Description
congestion-control	ocscp/scpc-configuration/{version}/congestion-control/{ruleName}	GET	Retrieves congestion control configuration rules for a given rulename.
congestion-control	ocscp/scpc-configuration/{version}/congestion-control	GET	Retrieves all congestion control configuration rules.
congestion-control	ocscp/scpc-configuration/{version}/congestion-control/{ruleName}	PUT	Updates the congestion control configuration rule.
congestion-control	ocscp/scpc-configuration/{version}/congestion-control/{ruleName}	DELETE	Deletes the congestion control configuration rule.

Data Model

Request Body

The following table describes the field names of the CongestionControlConfig data type.

Table 2-302 CongestionControlConfig

Field Name	Data Type	P	Default Value	Description
ruleName	String	M	"ruleName": "defaultRule"	Name of the rule to identify the congestion control configuration.
congestionControlConfigData	NFServiceLoadBased CongestionControl	M	-	NFServiceLoadBased CongestionControl

Table 2-303 NFServiceLoadBasedCongestionControl

Field Name	Data Type	P	Allowed Value	Description
alternateRoutingOnsetThresholdPercent	Integer	M	0-100	This field indicates the threshold percentage for onset alternate routing.

Table 2-303 (Cont.) NFSerAviceloadBasedCongestionControl

Field Name	Data Type	P	Allowed Value	Description
alternateRoutingAbatementThresholdPercent	Integer	M	0-100	This field indicates the threshold percentage for alternate routing abatement.
throttleOnsetThresholdPercent	Integer	M	0-100	This field indicates threshold percentage for onset throttling.
throttleAbatementThresholdPercent	Integer	M	0-100	This field indicates the threshold percentage for throttle abatement.
sbiMsgPriorityDiscardFrom	Integer	M	0-31	This field indicates the priority of the message, after which the message is discarded. For example, if the value is 30, then messages with priority 0-29 are high priority, and other low-priority messages are throttled.
errorProfileConfiguration	ErrorProfile Configuration	M		-

Table 2-304 ErrorProfileConfiguration

Field Name	Data Type	P	Default Value	Allowed Value	Description
ErrorCode	Integer	M	-	Valid HTTP status codes like 5xx, 4xx error codes.	Indicates configurable error codes to be sent by SCP to consumer NFs.
errorCause	String	O	-	-	Indicates the error cause that is specific to the occurrence of the problem.
errorTitle	String	O	-	-	Indicates the title of the error.
errorDescription	String	O	-	-	Indicates an explanation specific to the occurrence of the problem.
retryAfter	String	O	-	-	Indicates the retry interval. Note: The retryAfter header is applicable only for 429, 503, and 307 errors.
redirectUrl	String	O	-	-	Indicates the absolute URL of the resource to which the message is redirected.

Request/Response Body JSON Format (GET)

Response Body, Example:

```

{
  "ruleName": defaultRule
  "congestionControlConfigData": {
    "alternateRoutingOnsetThresholdPercent": 80,
    "alternateRoutingAbatementThresholdPercent": 75,
    "throttleOnsetThresholdPercent": 90,
    "throttleAbatementThresholdPercent": 85,
    "sbiMsgPriorityDiscardFrom": 24,
    "errorProfileConfiguration": {

```

```

        "errorCode": 503,
        "errorCause": "NF_CONGESTION",
        "errorTitle": "NF service is overloaded/congested",
        "errorDescription": "NF service is overloaded/congested",
        "retryAfter": "5",
        "redirectUrl": ""
    }
}
}

```

Request/Response Body JSON Format (PUT)

Request Body, Example:

```

{
  "ruleName": defaultRule
  "congestionControlConfigData": {
    "alternateRoutingOnsetThresholdPercent": 80,
    "alternateRoutingAbatementThresholdPercent": 75,
    "throttleOnsetThresholdPercent": 90,
    "throttleAbatementThresholdPercent": 85,
    "sbiMsgPriorityDiscardFrom": 24,
    "errorProfileConfiguration": {
      "errorCode": 503,
      "errorCause": "NF_CONGESTION",
      "errorTitle": "NF service is overloaded/congested",
      "errorDescription": "NF service is overloaded/congested",
      "retryAfter": "5",
      "redirectUrl": ""
    }
  }
}

```

Response body, Example:

```

{
  "ruleName": defaultRule
  "congestionControlConfigData": {
    "alternateRoutingOnsetThresholdPercent": 80,
    "alternateRoutingAbatementThresholdPercent": 75,
    "throttleOnsetThresholdPercent": 90,
    "throttleAbatementThresholdPercent": 85,
    "sbiMsgPriorityDiscardFrom": 24,
    "errorProfileConfiguration": {
      "errorCode": 503,
      "errorCause": "NF_CONGESTION",
      "errorTitle": "NF service is overloaded/congested",
      "errorDescription": "NF service is overloaded/congested",
      "retryAfter": "5",
      "redirectUrl": ""
    }
  }
}

```

Resource Definition**GET REST API:**

This resource fetches all the congestion control configurations rules.

Resource URI: /ocscp/scpc-configuration/{version}/congestion-control/

The following table describes the data structure supported by the GET method on this resource.

Table 2-305 Data structures supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
List<CongestionControlConfig>	M	1	200 OK	The congestion control configuration with a rule name.

Example

```
{
  "ruleName": defaultRule
  "congestionControlConfigData": {
    "alternateRoutingOnsetThresholdPercent": 80,
    "alternateRoutingAbatementThresholdPercent": 75,
    "throttleOnsetThresholdPercent": 90,
    "throttleAbatementThresholdPercent": 85,
    "sbiMsgPriorityDiscardFrom": 24,
    "errorProfileConfiguration": {
      "errorCode": 503,
      "errorCause": "NF_CONGESTION",
      "errorTitle": "NF service is overloaded/congested",
      "errorDescription": "NF service is overloaded/congested",
      "retryAfter": "5",
      "redirectUrl": ""
    }
  }
}
```

GET REST API:

This resource fetches the congestion control configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/congestion-control/{ruleName}

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-306 URI query parameters

Field Name	Data Type	P	Description
ruleName	String	O	The name of the congestion control rule used to retrieve the respective configurations.

The following table describes the data structure supported by the GET method on this resource.

Table 2-307 Data structures supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
CongestionControl Config	M	1..N	200 OK	The congestion control configuration with a rule name.
Problem details	M	1	404 NOT Found	Problem details

Curl Example for GET

Successful response

```
curl -v -H "Content-Type: application/json" --request GET http://localhost:8081/ocscp/scpc-configuration/v1/congestion-control/defaultrule
```

HTTP/1.1 200 OK

```
{
  "ruleName": "defaultRule",
  "congestionControlConfigData": {
    "alternateRoutingOnsetThresholdPercent": 80,
    "alternateRoutingAbatementThresholdPercent": 75,
    "throttleOnsetThresholdPercent": 90,
    "throttleAbatementThresholdPercent": 85,
    "sbiMsgPriorityDiscardFrom": 24,
    "errorProfileConfiguration": {
      "errorCode": 503,
      "errorCause": "NF_CONGESTION",
      "errorTitle": "NF service is overloaded/congested",
      "errorDescription": "NF service is overloaded/congested",
      "retryAfter": "5",
      "redirectUrl": ""
    }
  }
}
```

Failure case

```
curl -v -H "Content-Type: application/json" --request GET http://localhost:8081/ocscp/scpc-configuration/v1/congestion-control/rx
```

HTTP/1.1 404 Not Found

```
{
  "title": "Not Found",
  "status": "404",
  "detail": "Congestion control configuration data not found for provided ruleName in path parameter(s)",
  "instance": "/ocscp/scpc-configuration/v1/congestion-control/rx",
  "cause": "DATA_NOT_FOUND"
}
```

PUT REST API:

This resource adds or updates the congestion control configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/congestion-control/{ruleName}

Table 2-308 URI query parameters

Field Name	Data Type	P	Description
ruleName	String	O	The name of the congestion control rule used to add the respective configurations.

Table 2-309 Data structures

Data Type	P	Cardinality	Response codes	Description
CongestionControlConfig	M	1	200 OK	CongestionControlConfiguration with the rule name when an existing record is updated.
CongestionControlConfig	M	1	201	CongestionControlConfiguration with the rule name when an existing record is updated.
Problem details	M	1	404 NOT Found	Problem details

Curl Example for PUT

Success response:

```
curl -v -H "Content-Type: application/json" --request PUT -d '{
>   "ruleName": "r2",
>   "congestionControlConfigData": {
>     "alternateRoutingOnsetThresholdPercent": 80,
>     "alternateRoutingAbatementThresholdPercent": 75,
>     "throttleOnsetThresholdPercent": 90,
>     "throttleAbatementThresholdPercent": 85,
>     "sbiMsgPriorityDiscardFrom": 24,
>     "errorProfileConfiguration": {
>       "errorCode": 503,
>       "errorCause": "NF_CONGESTION",
>       "errorTitle": "NF service is overloaded/congested",
>       "errorDescription": "NF service is overloaded/congested",
>       "retryAfter": "5",
>       "redirectUrl": ""
>     }
>   }
> }' http://localhost:8081/ocscp/scpc-configuration/v1/congestion-control/r2
*   Trying 127.0.0.1...
* TCP_NODELAY set
* Connected to localhost (127.0.0.1) port 8081 (#0)
> PUT /ocscp/scpc-configuration/v1/congestion-control/r2 HTTP/1.1
> Host: localhost:8081
> User-Agent: curl/7.61.1
> Accept: */*
> Content-Type: application/json
> Content-Length: 560
```



```

>
* upload completely sent off: 560 out of 560 bytes
< HTTP/1.1 201 Created
< Connection: keep-alive
< Transfer-Encoding: chunked
< Content-Type: application/json
< Date: Fri, 18 Aug 2023 10:50:12 GMT
<
* Connection #0 to host localhost left intact

{
  "ruleName": "r2",
  "congestionControlConfigData": {
    "alternateRoutingOnsetThresholdPercent": 80,
    "alternateRoutingAbatementThresholdPercent": 75,
    "throttleOnsetThresholdPercent": 90,
    "throttleAbatementThresholdPercent": 85,
    "sbiMsgPriorityDiscardFrom": 24,
    "errorProfileConfiguration": {
      "errorCode": 503,
      "errorCause": "NF_CONGESTION",
      "errorTitle": "NF service is overloaded/congested",
      "errorDescription": "NF service is overloaded/congested",
      "retryAfter": "5",
      "redirectUrl": ""
    }
  }
}

```

Failure case 1

```

curl -X 'PUT' \
  'http://10.75.226.21:32474/ocscp/scpc-configuration/v1/congestion-
control/r2' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "ruleName": "r1",
    "congestionControlConfigData": {
      "alternateRoutingOnsetThresholdPercent": 30,
      "alternateRoutingAbatementThresholdPercent": 20,
      "throttleOnsetThresholdPercent": 50,
      "throttleAbatementThresholdPercent": 60,
      "sbiMsgPriorityDiscardFrom": 20,
      "errorProfileConfiguration": {
        "errorCause": "string",
        "errorTitle": "string",
        "errorDescription": "string",
        "retryAfter": "string",
        "redirectUrl": "string"
      }
    }
  }'
HTTP/1.1 400 Bad Request
{

```

```

    "title": "Bad Request",
    "status": "400",
    "detail": "Rule name should be same in path parameter and request body.",
    "instance": "/ocscp/scpc-configuration/v1/congestion-control/r1",
    "cause": "INVALID_KEY"
  }

```

Failure case 2

```

curl -X 'PUT' \
  'http://10.75.226.21:32474/ocscp/scpc-configuration/v1/congestion-
control/r1' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "ruleName": "r1",
    "congestionControlConfigData": {
      "alternateRoutingOnsetThresholdPercent": 30,
      "alternateRoutingAbatementThresholdPercent": 20,
      "throttleOnsetThresholdPercent": 50,
      "throttleAbatementThresholdPercent": 60,
      "sbiMsgPriorityDiscardFrom": 20,
      "errorProfileConfiguration": {
        "errorCause": "string",
        "errorTitle": "string",
        "errorDescription": "string",
        "retryAfter": "string",
        "redirectUrl": "string"
      }
    }
  }'
HTTP/1.1 400 Bad Request
{
  "title": "Bad Request",
  "status": "400",
  "detail": "Invalid errorCode configured in section
errorProfileConfiguration. Please refer user guide.",
  "instance": "/ocscp/scpc-configuration/v1/congestion-control/r1",
  "cause": "MANDATORY_IE_INCORRECT"
}

```

DELETE REST API:

This resource deletes the congestion control configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/congestion-control/{ruleName}

Table 2-310 URI query parameters

Field Name	Data Type	P	Description
ruleName	String	O	The name of the congestion control rule that needs to be deleted.

Table 2-311 Data structures supported by the Delete Response Body on this resource

Data Type	P	Cardinalit y	Response codes	Description
Default	M	1	204 OK	-
ProblemDetails	M	1	400/404	Problem details.

Curl Example for Delete

Successful response

```
curl -v -H "Content-Type: application/json" --request DELETE http://localhost:8081/ocscp/scpc-configuration/v1/congestion-control/r2
```

```
HTTP/1.1 204 No Content
< Date: Fri, 18 Aug 2023 10:55:57 GMT
<
* Connection #0 to host localhost left intact
```

Failure case

```
curl -v -H "Content-Type: application/json" --request DELETE http://localhost:8081/ocscp/scpc-configuration/v1/congestion-control/rx
```

```
HTTP/1.1 404 Not Found

{
  "title": "Not Found",
  "status": "404",
  "detail": "Congestion control configuration data Not Found for the given
ruleName in path parameter(s)",
  "instance": "/ocscp/scpc-configuration/v1/congestion-control/rx",
  "cause": "DATA_NOT_FOUND"
}
```

2.35 Circuit Breaking Configurations

This REST API is used to configure the circuit-breaking configuration rules. The user will use this API to configure CB configurations, and the name of this rule will be provided in Routing Options at the service level and System Options at the global level for inter-SCP and SEPP.

Resources

The following table describes the resource name to retrieve, add, update, and remove the circuit breaking configuration based on the query parameters.

- Resource URI Structure: `http://<authority>:<port>/ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}`
- Authority: loadbalancer or fqdn
- Port: nodeport(lp address) or internal port (For fqdn)
- loadbalancerip: 10.75.225.111

- Example : `http://10.75.225.111:32456/ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}` or
`http://ocscp-scpc-configuration:8081/ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}`

Table 2-312 Resource Name

Resource Name	Resource URI	HTTP Method	Description
circuit-breaking	<code>ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}</code>	GET	Retrieves the circuit breaking configuration rule.
circuit-breaking	<code>ocscp/scpc-configuration/{version}/circuit-breaking</code>	GET	Retrieves all circuit breaking configuration rules.
circuit-breaking	<code>ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}</code>	PUT	creates a circuit breaking configuration rule if not present; otherwise, it updates the existing one.
circuit-breaking	<code>ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}</code>	DELETE	Deletes the circuit breaking configuration rule.

Data Model

Request Body

The following table describes the field names of the CircuitBreakingConfig data type.

Table 2-313 CircuitBreakingConfig

Field Name	Data Type	P	Default Value	Description
ruleName	String	M	-	The rule name to identify the circuit breaker configuration.
CircuitBreakingConfig	CircuitBreakingConfig	M	-	circuitBreakingConfigData

Table 2-314 CircuitBreakingConfigData

Field Name	Data Type	P	Allowed Value	Description
http2MaxRequests	Integer	M	1000	Maximum number of requests SCP routes to a NF service instance, waiting for a response before stopping further routing requests to it.

Request/Response Body JSON Format (GET)

Response Body, Example:

```
{
  "ruleName": "newCBRule",
  "circuitBreakingConfigData": {
```

```

    "http2MaxRequests": 1200
  }
}

```

Request/Response Body JSON Format (PUT)

Request Body, Example:

```

{
  "ruleName": "newCBRule",
  "circuitBreakingConfigData": {
    "http2MaxRequests": 1200
  }
}

```

Response body, Example:

```

{
  "ruleName": "newCBRule",
  "circuitBreakingConfigData": {
    "http2MaxRequests": 1200
  }
}

```

Resource Definition

GET REST API:

This resource fetches the circuit breaking configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-315 URI query parameters

Field Name	Data Type	P	Description
ruleName	String	O	The name of the circuit breaking rule used to retrieve the respective configurations.

The following table describes the data structure supported by the GET method on this resource.

Table 2-316 Data structures supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
CircuitBreakingConfig	M	1	200 OK	The circuit breaking configuration with a rule name.
ProblemDetails	M	1	404	Problem details

Example

Success response

```
curl -v -H "Content-Type: application/json" --request GET http://localhost:8081/ocscp/scpc-configuration/v1/circuit-breaking/defaultRule
```

```
HTTP/1.1 200 OK
{
  "ruleName": "defaultRule",
  "circuitBreakingConfigData": {
    "http2MaxRequests": 1000
  }
}
```

Failure case

```
curl -v -H "Content-Type: application/json" --request GET http://localhost:8081/ocscp/scpc-configuration/v1/circuit-breaking/defaultRule1
```

```
HTTP/1.1 404 Not Found

{
  "title": "Not Found",
  "status": "404",
  "detail": "Congestion control configuration data not found for provided ruleName in path parameter(s)",
  "instance": "/ocscp/scpc-configuration/v1/circuit-breaking/defaultRule1",
  "cause": "DATA_NOT_FOUND"
}
```

GET REST API:

This resource fetches all circuit breaking configuration rules.

Resource URI: /ocscp/scpc-configuration/{version}/circuit-breaking

The following table describes the data structure supported by the GET method on this resource.

Table 2-317 Data structures supported by the GET Response Body

Data Type	P	Cardinality	Response codes	Description
CircuitBreakingConfig	M	1..N	200 OK	The circuit breaking configuration with a rule name.

Example of Congestion Control Configuration for GET

```
Command : curl -X 'GET' \
  'http://10.75.213.193:30066/ocscp/scpc-configuration/v1/circuit-breaking' \
  -H 'accept: application/json'
```

Response:

```
[
  {
    "ruleName": "defaultRule",
    "circuitBreakingConfigData": {
      "http2MaxRequests": 1000
    }
  }
]
```

PUT REST API:

This resource adds or updates the circuit breaking configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/circuit-breaking/{ruleName}

Table 2-318 URI query parameters

Field Name	Data Type	P	Description
ruleName	String	O	The name of the circuit breaking rule using which the respective configurations will be retrieved.

Table 2-319 Data structures

Data Type	P	Cardinality	Response codes	Description
CircuitBreakingConfig	M	1	200 OK	This response is generated when an existing record is updated.
CircuitBreakingConfig	M	1	201	This response is generated when a new record is created.
CircuitBreakingConfig	M	1	404	Problem details

Example of Congestion control configuration for PUT

Success response:

```
curl -v -H "Content-Type: application/json" -X PUT http://localhost:8081/
ocscp/scpc-configuration/v1/circuit-breaking/defaultRule -d '{
  "ruleName": "defaultRule",
  "circuitBreakingConfigData": {
    "http2MaxRequests": 1000
  }
}'
```

HTTP/1.1 200 OK

```
{"ruleName":"defaultRule","circuitBreakingConfigData":
{"http2MaxRequests":1000}}
```

Failure case 1

```
curl -v -H "Content-Type: application/json" -X PUT http://localhost:8081/
ocscp/scpc-configuration/v1/circuit-breaking/defaultRule1 -d '{
  "ruleName": "defaultRule",
  "circuitBreakingConfigData": {
    "http2MaxRequests": 1000
  }
}'
```

HTTP/1.1 400 Bad Request

```
{"title":"Bad Request","status":"400","detail":"Please provide same ruleName
in Path Variable and Request Body. Please refer to the User
Guide.","instance":"/ocscp/scpc-configuration/v1/circuit-breaking/
defaultRule1","cause":"MANDATORY_IE_MISSING"}
```

DELETE REST API:

This resource deletes the circuit breaking configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/circuit-breaking/
{ruleName}

Table 2-320 URI query parameters

Field Name	Data Type	P	Description
ruleName	String	O	The name of the circuit breaking rule that needs to be deleted.

Table 2-321 Data structures supported by the Delete Response Body on this resource

Data Type	P	Cardinalit y	Response codes	Description
Default	M	1	204 OK	-
ProblemDetails	M	1	403/404	Problem details.

Example

Successful response

```
curl -v -H "Content-Type: application/json" -X DELETE http://localhost:8081/
ocscp/scpc-configuration/v1/circuit-breaking/defaultRuleq
HTTP/1.1 204 No Content
```

Failure case 1

```
curl -v -H "Content-Type: application/json" -X DELETE http://localhost:8081/
ocscp/scpc-configuration/v1/circuit-breaking/defaultRule
HTTP/1.1 403 Forbidden
{"title":"Forbidden","status":"403","detail":"Default rule cannot be deleted."}
```



```
Please refer to the User Guide.", "instance": "/ocscp/scpc-configuration/v1/
circuit-breaking/defaultRule", "cause": "OPERATION_NOT_ALLOWED"}
```

Failure case 2

```
curl -v -H "Content-Type: application/json" -X DELETE http://localhost:8081/
ocscp/scpc-configuration/v1/circuit-breaking/defaultRuleqq
HTTP/1.1 404 Not Found
{"title": "Not Found", "status": "404", "detail": "Circuit Breaking Configuration
data not found against given query parameter(s). Please refer to the User
Guide.", "instance": "/ocscp/scpc-configuration/v1/circuit-breaking/
defaultRule111", "cause": "DATA_NOT_FOUND"}
```

2.36 Routing Config Set

This REST API is used to define custom routing options for notification message only.

The routing configuration set defined using this API is used as a reference in another table, Routing Options Configuration. For more information, see [Routing Options Configurations](#).

Resources

The following table describes the resource name to retrieve, add, update, and remove routing config set configurations based on the query parameters.

Table 2-322 Resource Name

Resource Name	Resource URI	HTTP Method	Query Parameter	Description
routing-config-set	/ocscp/scpc-configuration/v1/routing-config-set/<routingConfigSetName>	GET	None	Get routing configurations based on routingConfigSetName.
routing-config-set	/ocscp/scpc-configuration/v1/routing-config-set/	GET	None	Get all routing configurations.
routing-config-set	/ocscp/scpc-configuration/v1/routing-config-set/<routingConfigSetName>	PUT	None	Updates or creates new routing configurations, similar to routing options.
routing-config-set	/ocscp/scpc-configuration/v1/routing-config-set/<routingConfigSetName>	DELETE	None	Deletes routing option configurations for given names.

Data Model

Request Body (PUT)

The following table describes the field names of the ConfigureRoutingConfigSet data type.

Table 2-323 ConfigureRoutingConfigSet

Field Name	Data Type	P	Default Values	Allowed Values	Description
routingConfigSetName	String	M	-	-	Unique name that identifies the routing rule. This rule name is used in RoutingOptionsConfig as a reference.
configureRoutingOptions	ConfigureRoutingOptions	M	-	-	This field defines the routing option configurations.

Table 2-324 Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
odEnabled	Enables or disables the outlier detection feature.	false	true, false	Yes	Yes
odRuleName	Indicates the name of the rule holding the configuration of outlier detection. The outlier detection feature works based on configuration under this rule.	defaultRule	NA	Yes	Yes
ociEnabled	Enables and disables the Overload Control Information feature.	false	true, false	Yes	Yes
ociRuleName	Indicates the name of the rule holding the configuration of Overload Control Information. The Overload Control Information feature works based on the configuration under this rule.	defaultOciConfigRule	NA	Yes	Yes
responseTimeout	Indicates the allotted time to respond to a message request. When the response timeout expires, SCP performs alternate rerouting to the available alternate NF or pod. If no alternate NFs or pods are available, SCP sends an error message.	1 second	100-10000 ms The supported values can be in 's' or 'ms'. Where, 's' is seconds and 'ms' is milliseconds.	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
totalTransactionLifetime	Indicates the total time allowed to forward a request, including the initial and all subsequent routing attempts. Note: The totalTransactionLifetime value should be greater than the value obtained by multiplying responseTimeout by the total maximum number of attempts (pod level + service level).	6 seconds	100 - 240000 ms	Yes	Yes
max Routing Attempts	Indicates the maximum number of forward routing attempts at a service level. - The maximum number of times SCP is allowed to forward a request message. If the max routing attempts value is set to 1 for both service and pod levels, the total transaction lifetime field value is not required. If the max routing attempts value is set to greater than 1 for both service and pod levels, then the total transaction lifetime field value is considered for rerouting processing. - Rerouting of request messages is always considered as the max routing attempts value minus one (-1), that is, rerouting of request messages = (max routing attempts value) - 1. The default route attempt is 1.	1 for Pod Level. 3 for Service Level	1-5	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
reRouteConditionList	- This parameter lists the HTTP status codes that SCP uses to attempt alternative routing. If the upstream server responds with any of these configured response codes, SCP will try rerouting based on the configured alternate routing mechanism. - In the event of a response timeout, connection failure, refused stream, or GOAWAY frame received on any connection, SCP attempts to reroute the request. These options (events) are not configurable and are supported by SCP.	"reRouteConditionList": [{ "statusCode": "5xx" }, { "statusCode": "429" }, { "statusCode": "307" }, { "statusCode": "308" }]	301, 302, 303, 304, 307, 308, 400, 401, 403, 404, 405, 406, 407, 408, 409 , 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 425, 426, 428, 429, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 510, 511, 5xx	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
actions	Supported actions: - Forwards the ingress service request to the selected egress producer NF. - Sends a response with the configured result code and message. - Abandons or drops the ingress service request.	Forward	NA	Yes	NA
loadBalancingAlgorithm	Priority Only: Use priority as the first-level criteria. Use capacity as a second-level criteria.	Priority_only	NA	Yes	Yes
defaultPriority	- Priority (relative to other NF Services of the same type) in the range of 0–65535 is to be used for NF Service selection; lower values indicate a higher priority. If priority is present in either an NF profile or nfServiceList parameter, those profiles or parameters take precedence over this value. - This default priority value is used for NF service instance selection if priority is not published by producer NFs during registration with NRF in the NF profile, including both NF profile and nfServiceList parameters.	1	NA	Yes	No

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
defaultCapacity	- Capacity information in the range of 0–65535 is expressed as a weight relative to other NF service instances of the same type; if capacity is also present in either an NF profile or nfServiceList parameter, those profiles or parameters take precedence over this value. - This default capacity value shall be used for NF service instance selection if capacity is not published by producer NFs during registration with NRF in the NF profile, including both NF profile and nfServiceList parameters.	65535	NA	Yes	No
reverseProxySupport	Enables reverse proxy support for a service. In reverse proxy mode, all the requests have the same authority as SCP. SCP forwards those requests to the respective producers after making the required authority changes in the requests (both initial and subsequent). Currently, reverse proxy mode is supported only for some interfaces. If the parameter is set to false, then transparent proxy mode is enabled. If the reverseProxySupport parameter is set to true, it supersedes initialServiceRequest.routePolicy even if it is set to 'Forward_Route' and creates rules for initial messages in the Load_balance way. Note: This parameter is not applicable for R16 deployment.	false	true, false	Yes	No

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
exceptionErrorResponses	Resource Exhausted Action: - Action taken when a request cannot be processed due to an internal resource being exhausted - Options: Abandon with no answer Send an answer with the configured HTTP status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Abandon with no Answer	NA	Yes	No
exceptionErrorResponses	No Producer Response Action - Action taken when the routing of a request is abandoned due to a response timeout. - Options: Abandon with no Answer Send Answer with configured http status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Send Answer with configured http status code (Default 504).	NA	Yes	No

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
exceptionErrorResponse	Connection Failure Action: - Action taken when the routing of a request is abandoned when the last egress connection selection fails - Options: Abandon with no Answer Send Answer with configured HTTP status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Send Answer with configured http status code (Default 504).	NA	Yes	No
exceptionErrorResponse	Host not found Action: - Action taken when the routing of a request is abandoned due to FQDN of the host not being found - Options: Abandon with no Answer Send Answer with configured http status code. For more information, see "HTTP Status Code and Applicability for Rerouting" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i>.	Send Answer with configured http status code (Default 504).	NA	Yes	No
exceptionErrorResponse	DB Lookup Error Note: This parameter is not supported.	Send Answer with configured http status code (Default 500).	NA	Yes	No

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
deploymentModel	Indicates deployment model of the NF or NF service. - Default, SITE_WIDE is supported for all NF services. - REGIONAL deployment is supported only for CHF NF in addition to SITE_WIDE. - Limitation: PRIMARY_SECONDARY_PAIR deployment is not supported.	SITE_WIDE	NA	Yes	Yes
assignPreferredLocality	SCP assigns its own locality as a preferred locality for NF discovery if assignPreferredLocality is enabled and the 3gpp-Sbi-Discovery-preferredlocality header is absent in ingress service requests.	false	true, false	Yes	NA
overridePreferredLocality	SCP overrides the 3gpp-Sbi-Discoverypreferred-locality header received in the service request and uses its own locality as preferred-locality for NF discovery if overridePreferredLocality is enabled, and the 3gpp-Sbi-Discoverypreferred-locality header is present in ingress service requests.	false	true, false	Yes	NA
forwardRevisedPreferredLocality	Controls the forwarding of assigned or overridden values of 3gpp-Sbi-Discovery-preferred-locality headers to the next hop SCP.	false	true, false	Yes	NA
initialServiceRequest	Considers routePolicy and reroutePolicy for the initial service request.	NA	NA	Yes	NA
subsequentServiceRequest	Considers routePolicy and reroutePolicy for subsequent service requests. Note: This parameter is not applicable for notification message	NA	NA	NA	NA
service	Name of the NF service.	SCP level config	NA	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSCP.service.maxRoutingAttempts	Indicates the maximum number of reroute attempt (retries) at service level. - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both service and pod level, the total transaction lifetime field value is not required. If the Max Routing attempts value is set to greater than 1 for both service and pod level, then the total transaction lifetime field value is considered for rerouting processing. - Rerouting of request messages is always considered as Max Routing attempts value minus one (-1), that is, Rerouting of request messages = (Max Routing attempts value) - 1 The default routing attempt is 1.	2 attempts	1-5	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSCP.serviceEndpoint.maxRoutingAttempts	Indicates the maximum number of reroute attempts (retries) at NF or pod level. - Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both service and pod level, the total transaction lifetime field value is not required. If the Max Routing attempts value is set to greater than 1 for both service and pod level, then the total transaction lifetime field value is considered for rerouting processing. - Rerouting of request messages is always considered as Max Routing attempts value minus one (-1), that is, Rerouting of request messages = (Max Routing attempts value) - 1 The default routing attempt is 1.	1 attempt	1-5	Yes	Yes
nextHopSCP.responseTimeout	Indicates the allotted time to respond to a message request. When the response timeout expires, SCP performs alternate rerouting to the available alternate NF or pod or sends an error message.	4 seconds	100-10000 ms	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSCP.totalTransactionLifetime	Indicates the total time allowed to forward a request to Next Hop SCP. Note: - The total time consumed in processing all retries should not exceed the total transaction lifetime. - The totalTransactionLifetime value should be greater than the value obtained by multiplying responseTimeout by the total maximum number of attempts (pod level + service level).	7 seconds	100 - 240000 ms	Yes	Yes
nextHopSCP.exceptions	Host not found Action - Action taken when the routing of a request is abandoned due to the FQDN of the host not found. - Options: - Abandon with no answer - Send an answer with the configured http status code. Refer to the HTTP Status Code and applicability for rerouting.	Send Answer with configured http status code (Default 504).	-	Yes	-
nextHopSCP.loadBasedCongestionControlEnabled	Enables and disables load based congestion control for nextHopSCP.	true	true, false	Yes	No
nextHopSCP.nfServiceLoadBasedCongestionControlCfg	Name of the rule holding the configuration of congestion control for nextHopSCP. Based on the configuration under this rule, congestion control works.	defaultRuleForNextHopScp			

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSEPP.totalTransactionLifetime	- The time consumed in processing all retries should not exceed the total transaction lifetime. - The total time allowed to forward a request, including the initial and all subsequent routing attempts. Note: The totalTransactionLifetime value should be greater than the value obtained by multiplying responseTimeout by the total maximum number of attempts (pod level + service level).	7 seconds	100 - 240000	Yes	Yes
nextHopSEPP.responseTimeout	Indicates the allotted time to respond to a message request. When the response timeout expires, SCP performs alternate rerouting to the available alternate NF or pod or sends an error message.	4 seconds	100-10000 ms	Yes	Yes
nextHopSEPP.service.maxRoutingAttempts	- Number of reroute attempts (retries) at the NF/Pod level. - The maximum number of times SCP is allowed to forward a request message. If the max routing attempts value is set to 1 for both service and pod levels, the total transaction lifetime field value is not needed and If the maximum number of routing attempts (including both service and pod levels) is greater than 1, the total transaction lifetime value is considered in rerouting processing.	2	1 to 5	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSEPP.serviceEndpoint.maxRoutingAttempts	- Number of reroute attempts (retries) at the NF/Pod level. - The maximum number of times SCP is allowed to forward a request message. If the max routing attempts value is set to 1 for both service and pod levels, the total transaction lifetime field value is not needed and If the maximum number of routing attempts (including both service and pod levels) is greater than 1, the total transaction lifetime value is considered in rerouting processing.	1	1 to 5	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSEPP.reRouteConditionList	- This parameter lists the HTTP status codes that SCP uses to attempt alternative routing. If the upstream server responds with any of these configured response codes, SCP will try rerouting based on the configured alternate routing mechanism. - In the event of a response timeout, connection failure, refused stream, or GOAWAY frame received on any connection, SCP attempts to reroute the request. These options (events) are not configurable and are supported by SCP.	"reRouteConditionList": [{ "statusCode": "5xx" }, { "statusCode": "429" }, { "statusCode": "307" }, { "statusCode": "308" }]	301, 302, 303, 304, 307, 308, 400, 401, 403, 404, 405, 406, 407, 408, 409 , 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 425, 426, 428, 429, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 510, 511, 5xx	Yes	Yes

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nextHopSEPP.exceptions	Host not found Action - Action taken when the routing of a request is abandoned due to the FQDN of the host not found. - Options: - Abandon with no answer - Send an answer with the configured http status code. Refer to the HTTP Status Code and applicability for rerouting.	Send Answer with configured http status code (Default 504).	Send Answer with configured http status code (Default 504).	Yes	No
nextHopSEPP.loadBasedCongestionControlEnabled	Enables and disables load-based congestion control for the nextHopSEPP.	true	true, false	Yes	No
nextHopSEPP.nfServiceLoadBasedCongestionControlCfg	Name of the rule holding the configuration of congestion control for nexthopSEPP. Based on the configuration under this rule, congestion control will work.	defaultRuleForNextHopSepp	-	Yes	-

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
alternateNFGroup RoutingOptions	This parameter decides the alternate routing mode, depending on which scp-worker derives the alternate producer NF - Different modes are described below NF_SET: SCP performs alternate routing based on the Model C Indirect 5G SBI Communication format. This is the default mode. DNS_SRV: SCP performs alternate routing based on the DNS SRV query. NF_SET_FOLLOWED_BY_DNSSRV: SCP performs alternate routing based on NF Set and then with DNS SRV. STATIC_CONFIG: SCP performs alternate routing based on the static configuration. NF_SET_FOLLOWED_BY_STATIC_CONFIG: SCP performs alternate routing based on NF Set, and then using static configuration.	NF_SET	NF_SET DNS_SRV NF_SET_FOLLOWED_BY_DNSSRV STATIC_CONFIG NF_SET_FOLLOWED_BY_STATIC_CONFIG	Yes	No
cbEnabled	Enables and disables circuit breaking.	false	true, false	Yes	No

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
cbRuleName	Name of the rule holding the configuration of circuit breaking. Based on the configuration under this rule, circuit breaking works. <pre> { "ruleName": "defaultRule", "data": { "v1": { "http2MaxRequests": 1000 } } } </pre>	defaultRule	-		
loadBasedCongestionControlEnabled	Enables and disables load-based congestion control.	true	true, false	Yes	No

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
nfServiceLoadBasedCongestionControlCfg	Name of the rule holding the configuration of congestion control. Based on the configuration under this rule, congestion control works. <pre> { "ruleName": "defaultRule", "congestionControlConfigData": { "v1": { "alternateRoutingOnsetThresholdPercent": 80, "alternateRoutingAbatementThresholdPercent": 75, "throttleOnsetThresholdPercent": 90, "throttleAbatementThresholdPercent": 85, "sbiMsgPriorityDiscardFrom": 24, "errorProfileConfiguration": { "errorCode": 503, "errorCause": "NF_CONGESTION", "errorTitle": "NF service is overloaded/ congested", "errorDescription": "NF service is </pre>	defaultRule			

Table 2-324 (Cont.) Parameters for Configure Routing Options

Parameter Name	Description	Default Values	Value Range	Applicable to NF Service Level	Applicable to Pod Level within NF
	<pre> overloaded/ congested", "retryAfter": "5", "redirectUrl": "" } } }</pre>				

Table 2-325 deploymentCHF

Enumeration value	CHF Deployment
REGIONAL	Regional CHF deployment, that is, CHF's, are deployed in primary region and secondary regions. A region may consist of one or more locality.
SITE_WIDE	Site specific CHF deployment, that is, CHF instances, are deployed as per SCP's site deployment.
PRIMARY_SECONDARY_PAIR	Primary and Secondary CHF deployment using ChfServiceInfo. Primary and Secondary CHF instance information is published in ChfServiceInfo while registering with NRF.

Table 2-326 initialServiceRequest

routePolicy	reroutePolicy
Load_Balance	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite and RerouteAcrossMatedSite. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup
Forward_Route	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite and RerouteAcrossMatedSite. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup

Table 2-327 subsequentServiceRequest

routePolicy	reroutePolicy
Load_Balance	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite and RerouteAcrossMatedSite. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup
Forward_Route	Reroute options: • RerouteDisabled • Options in SITE_WIDE deployment: RerouteWithinSite and RerouteAcrossMatedSite. • Options in REGIONAL deployment: RerouteWithinRegion and RerouteAcrossRegion • Options in PRIMARY_SECONDARY_PAIR deployment: RerouteWithinPairGroup

Resource Definition**GET REST API:**

This resource fetches the routing config set configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-config-set/{routingConfigSetName}

The following table describes the URI query parameters supported by the GET method on this resource.

Table 2-328 URI query parameters

Field Name	Data Type	P	Description
routingConfigSetName	String	O	The name of the routing config set used to retrieve the respective configurations.

The following table describes the data structures supported by the GET Response Body on this resource.

Table 2-329 Data structures

Data Type	P	Cardinality	Response Codes	Description
ConfigureRoutingConfigSet	M	1	200 OK	The routing options with the rule name.
ProblemDetails	M	1	404	Problem details

Example

Successful response

```
curl -v -H "Content-Type: application/json" --request GET http://
localhost:8081/ocscp/scpc-configuration/v1/routing-config-set/
defaultRoutingConfigSet
```

```
HTTP/1.1 200 OK
```

```
{
  "routingConfigSetName": "defaultRoutingConfigSet",
  "configureRoutingOptions": {
    "odEnabled": false,
    "cbEnabled": false,
    "odRuleName": "defaultRule",
    "cbRuleName": "defaultRule",
    "pod": {
      "maxRoutingAttempts": 1,
      "alternateRouting": true,
      "loadBalancingAlgorithm": "RoundRobin",
      "alternateNFGroupRoutingOptions": {
        "mode": "NF_SET",
        "srv": {
          "name": "5g-sbi-notification",
          "maxRoutingAttempts": 3,
          "actions": "Forward",
          "loadBalancingAlgorithm": "Priority_only",
          "loadBasedCongestionControlEnabled": true,
          "nfServiceLoadBasedCongestionControlCfg": "defaultRule",
          "defaultPriority": 1,
          "defaultCapacity": 65535,
          "reverseProxySupport": false,
          "initialServiceRequest": {
            "routePolicy": "Forward_Route",
            "reroutePolicy": "RerouteWithinSite",
            "subsequentServiceRequest": {
              "routePolicy": "Forward_Route",
              "reroutePolicy": "RerouteWithinSite"
            }
          },
          "totalTransactionLifetime": "6s",
          "reRouteConditionList": [
            { "statusCode": "307" },
            { "statusCode": "308" },
            { "statusCode": "429" },
            { "statusCode": "5xx" }
          ],
          "responseTimeout": "1s",
          "exceptionErrorResponses": [
            {
              "name": "Resource_Exhausted",
              "action": "Send_Answer",
              "error_code": 503,
              "error_response": "Service Unavailable"
            },
            {
              "name": "No_Response",
              "action": "Send_Answer",
              "error_code": 504,
              "error_response": "Gateway Timeout"
            },
            {
              "name": "Connect_Failure",
              "action": "Send_Answer",
              "error_code": 503,
              "error_response": "Service Unavailable"
            },
            {
              "name": "No_Host",
              "action": "Send_Answer",
              "error_code": 503,
              "error_response": "Service Unavailable"
            },
            {
              "name": "Db_LookUp_Error",
              "action": "Send_Answer",
              "error_code": 500,
              "error_response": "Session/Subscriber binding not found/look-up failure at OCSCP-SDS Service"
            }
          ],
          "deploymentModel": "SITE_WIDE",
          "name": "5g-sbi-notification",
          "assignPreferredLocality": false,
          "overridePreferredLocality": false,
          "forwardRevisedPreferredLocality": false,
          "nextHopSEPP": {
            "totalTransactionLifetime": "7s",
            "responseTimeout": "4s",
            "service": {
              "maxRoutingAttempts": 2,
              "serviceEndpoint": {
                "maxRoutingAttempts": 1,
                "loadBasedCongestionControlEnabled": true,
                "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
                "reRouteConditionList": [
                  { "statusCode": "307" },
                  { "statusCode": "308" },
                  { "statusCode": "429" },
                  { "statusCode": "5xx" }
                ],
                "exceptions": [
                  {
                    "name": "No_Host",
                    "action": "Send_Answer",
                    "error_code": 504,
                    "error_response": "Gateway Timeout"
                  }
                ],
                "nextHopScp": {
                  "totalTransactionLifetime": "7s",
                  "responseTimeout": "4s",
                  "service": {
                    "maxRoutingAttempts": 2,
                    "serviceEndpoint": {
                      "maxRoutingAttempts": 1,
                      "loadBasedCongestionControlEnabled": true,
                      "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
                      "exceptions": [
                        {
                          "name": "No_Host",
                          "action": "Send_Answer",
                          "error_code": 503,
                          "error_response": "Service Unavailable"
                        }
                      ]
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Failure case

```
curl -v -H "Content-Type: application/json" --request GET http://
localhost:8081/ocscp/scpc-configuration/v1/routing-config-set/defaultConfig
```

HTTP/1.1 404 Not Found

```
{"title":"Not Found","status":"404","detail":"RoutingConfigSet data not found
against given RoutingConfigSetName . Please refer to the User
Guide.", "instance":"/ocscp/scpc-configuration/v1/routing-config-set/
defaultConfig", "cause":"DATA_NOT_FOUND"}
```

GET REST API:

This resource fetches all routing configurations rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-config-set

The following table describes the data structures supported by the GET Response Body on this resource.

Table 2-330 Data structures

Data Type	P	Cardinality	Response Codes	Description
ConfigureRoutingConfigSet	M	1..N	200 OK	The routing options with the rule name.

Example of Congestion Control Configuration for GET**Success case**

```
curl -v -H "Content-Type: application/json" --request GET http://
localhost:8081/ocscp/scpc-configuration/v1/routing-config-set
```

HTTP/1.1 200 OK

```
[{"routingConfigSetName":"defaultRoutingConfigSet","configureRoutingOptions":
{"odEnabled":false,"cbEnabled":false,"odRuleName":"defaultRule","cbRuleName":
"defaultRule","pod":
{"maxRoutingAttempts":1,"alternateRouting":true,"loadBalancingAlgorithm":"Roun
d_Robin"},"alternateNFGroupRoutingOptions":{"mode":"NF_SET"},"srv":
{"name":"5g-sbi-
notification","maxRoutingAttempts":3,"actions":"Forward","loadBalancingAlgorit
hm":"Priority_only","loadBasedCongestionControlEnabled":true,"nfServiceLoadBas
edCongestionControlCfg":"defaultRule","defaultPriority":1,"defaultCapacity":65
535,"reverseProxySupport":false,"initialServiceRequest":
{"routePolicy":"Forward_Route","reroutePolicy":"RerouteWithinSite"},"subsequen
tServiceRequest":
{"routePolicy":"Forward_Route","reroutePolicy":"RerouteWithinSite"},"totalTra
nsactionLifetime":"6s","reRouteConditionList":[{"statusCode":"307"},
{"statusCode":"308"}, {"statusCode":"429"},
{"statusCode":"5xx"}],"responseTimeout":"1s","exceptionErrorResponses":
[{"name":"Resource_Exhausted","action":"Send_Answer","error_code":503,"error_r
esponse":"Service Unavailable"},
{"name":"No_Response","action":"Send_Answer","error_code":504,"error_response"
:"Gateway Timeout"}],
```

```
{
  "name": "Connect_Failure", "action": "Send_Answer", "error_code": 503, "error_response": "Service Unavailable"},
  {"name": "No_Host", "action": "Send_Answer", "error_code": 503, "error_response": "Service Unavailable"},
  {"name": "Db_LookUp_Error", "action": "Send_Answer", "error_code": 500, "error_response": "Session/Subscriber binding not found/look-up failure at OCSCP-SDS Service"}], "deploymentModel": "SITE_WIDE", "name": "5g-sbi-notification", "assignPreferredLocality": false, "overridePreferredLocality": false, "forwardRevisedPreferredLocality": false, "nextHopSEPP": {
  "totalTransactionLifetime": "7s", "responseTimeout": "4s", "service": {
  "maxRoutingAttempts": 2}, "serviceEndpoint": {
  "maxRoutingAttempts": 1}, "loadBasedCongestionControlEnabled": true, "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp", "reRouteConditionList": [{"statusCode": "307"}, {"statusCode": "308"}, {"statusCode": "429"}, {"statusCode": "5xx"}], "exceptions": [{"name": "No_Host", "action": "Send_Answer", "error_code": 504, "error_response": "Gateway Timeout"}]}, "nextHopScp": {
  "totalTransactionLifetime": "7s", "responseTimeout": "4s", "service": {
  "maxRoutingAttempts": 2}, "serviceEndpoint": {
  "maxRoutingAttempts": 1}, "loadBasedCongestionControlEnabled": true, "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp", "exceptions": [{"name": "No_Host", "action": "Send_Answer", "error_code": 503, "error_response": "Service Unavailable"}]}]]}]
```

PUT REST API:

This resource creates or updates the routing config set configurations for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-config-set/{routingConfigSetName}

Table 2-331 URI query parameters

Field Name	Data Type	P	Description
routingConfigSetName	String	O	The name of the routing config set rule used to create the respective routing options.

Table 2-332 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response codes	Description
ConfigureRoutingConfigSet	M	1	200 OK	This response is generated when an existing record is updated.
ConfigureRoutingConfigSet	M	1	201	This response is generated when a new record is created.
ProblemDetails	M	1	400	Returns problem details.

Example

Successful response

```
curl -v -H "Content-Type: application/json" --request PUT http://
localhost:8081/ocscp/scpc-configuration/v1/routing-config-set/defaultConfig -
d '{
  "routingConfigSetName": "defaultConfig",
  "configureRoutingOptions": {
    "odEnabled": false,
    "cbEnabled": false,
    "ociEnabled": false,
    "odRuleName": "defaultRule",
    "cbRuleName": "defaultRule",
    "ociRuleName": "defaultOciConfigRule",
    "pod": {
      "maxRoutingAttempts": 1,
      "alternateRouting": true,
      "loadBalancingAlgorithm": "Round_Robin"
    },
    "alternateNFGroupRoutingOptions": {
      "mode": "NF_SET"
    },
    "srv": {
      "name": "5g-sbi-notification",
      "maxRoutingAttempts": 3,
      "actions": "Forward",
      "loadBalancingAlgorithm": "Priority_only",
      "loadBasedCongestionControlEnabled": true,
      "nfServiceLoadBasedCongestionControlCfg": "defaultRule",
      "defaultPriority": 1,
      "defaultCapacity": 65535,
      "reverseProxySupport": false,
      "initialServiceRequest": {
        "routePolicy": "Forward_Route",
        "reroutePolicy": "RerouteWithinSite"
      },
      "subsequentServiceRequest": {
        "routePolicy": "Forward_Route",
        "reroutePolicy": "RerouteWithinSite"
      }
    },
    "totalTransactionLifetime": "6s",
    "reRouteConditionList": [
      {
        "statusCode": "307"
      },
      {
        "statusCode": "308"
      },
      {
        "statusCode": "429"
      },
      {
        "statusCode": "5xx"
      }
    ],
    "responseTimeout": "1s",
```

```

"exceptionErrorResponses": [
  {
    "name": "Resource_Exhausted",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "No_Response",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "Connect_Failure",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "No_Host",
    "action": "Send_Answer",
    "error_code": 504,
    "error_response": "Gateway Timeout"
  },
  {
    "name": "Db_LookUp_Error",
    "action": "Send_Answer",
    "error_code": 500,
    "error_response": "Session/Subscriber binding not found/look-up
failure at OCSCP-SDS Service"
  }
],
"deploymentModel": "SITE_WIDE",
"name": "5g-sbi-notification",
"assignPreferredLocality": false,
"overridePreferredLocality": false,
"forwardRevisedPreferredLocality": false,
"nextHopSEPP": {
  "totalTransactionLifetime": "7s",
  "responseTimeout": "4s",
  "service": {
    "maxRoutingAttempts": 2
  },
  "serviceEndpoint": {
    "maxRoutingAttempts": 1
  },
  "loadBasedCongestionControlEnabled": true,
  "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
  "reRouteConditionList": [
    {
      "statusCode": "307"
    },
    {
      "statusCode": "308"
    }
  ],

```

```

        {
          "statusCode": "429"
        },
        {
          "statusCode": "5xx"
        }
      ],
      "exceptions": [
        {
          "name": "No_Host",
          "action": "Send_Answer",
          "error_code": 504,
          "error_response": "Gateway Timeout"
        }
      ]
    },
    "nextHopScp": {
      "totalTransactionLifetime": "7s",
      "responseTimeout": "4s",
      "service": {
        "maxRoutingAttempts": 2
      },
      "serviceEndpoint": {
        "maxRoutingAttempts": 1
      },
      "loadBasedCongestionControlEnabled": true,
      "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
      "exceptions": [
        {
          "name": "No_Host",
          "action": "Send_Answer",
          "error_code": 504,
          "error_response": "Gateway Timeout"
        }
      ]
    }
  }
}

```

HTTP/1.1 201 Created

```

{"routingConfigSetName":"defaultConfig","configureRoutingOptions":
{"odEnabled":false,"cbEnabled":false,"odRuleName":"defaultRule","cbRuleName":
"defaultRule","pod":
{"maxRoutingAttempts":1,"alternateRouting":true,"loadBalancingAlgorithm":"Roun
d_Robin"},"alternateNFGroupRoutingOptions":{"mode":"NF_SET"},"srv":
{"name":"5g-sbi-
notification","maxRoutingAttempts":3,"actions":"Forward","loadBalancingAlgorit
hm":"Priority_only","loadBasedCongestionControlEnabled":true,"nfServiceLoadBas
edCongestionControlCfg":"defaultRule","defaultPriority":1,"defaultCapacity":65
535,"reverseProxySupport":false,"initialServiceRequest":
{"routePolicy":"Forward_Route","reroutePolicy":"RerouteWithinSite"},"subsequen
tServiceRequest":
{"routePolicy":"Forward_Route","reroutePolicy":"RerouteWithinSite"}},{"totalTra
nsactionLifetime":"6s","reRouteConditionList":[{"statusCode":"5xx"},
{"statusCode":"307"}, {"statusCode":"429"}],

```

```
{
  "statusCode": "308",
  "responseTimeout": "1s",
  "exceptionErrorResponses": [
    {
      "name": "Resource_Exhausted",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Response",
      "action": "Send_Answer",
      "error_code": 504,
      "error_response": "Gateway Timeout"
    },
    {
      "name": "Connect_Failure",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Host",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "Db_LookUp_Error",
      "action": "Send_Answer",
      "error_code": 500,
      "error_response": "Session/Subscriber binding not found/look-up failure at OCSCP-SDS Service"
    }
  ],
  "deploymentModel": "SITE_WIDE",
  "name": "5g-sbi-notification",
  "assignPreferredLocality": false,
  "overridePreferredLocality": false,
  "forwardRevisedPreferredLocality": false,
  "nextHopSEPP": {
    "totalTransactionLifetime": "7s",
    "responseTimeout": "4s",
    "service": {
      "maxRoutingAttempts": 2,
      "serviceEndpoint": {
        "maxRoutingAttempts": 1,
        "loadBasedCongestionControlEnabled": true,
        "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
        "reRouteConditionList": [
          {
            "statusCode": "5xx"
          },
          {
            "statusCode": "307"
          },
          {
            "statusCode": "429"
          }
        ],
        "connection": "#0 to host localhost left intact"
      },
      "exceptions": [
        {
          "name": "No_Host",
          "action": "Send_Answer",
          "error_code": 504,
          "error_response": "Gateway Timeout"
        }
      ]
    },
    "nextHopScp": {
      "totalTransactionLifetime": "7s",
      "responseTimeout": "4s",
      "service": {
        "maxRoutingAttempts": 2,
        "serviceEndpoint": {
          "maxRoutingAttempts": 1,
          "loadBasedCongestionControlEnabled": true,
          "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
          "exceptions": [
            {
              "name": "No_Host",
              "action": "Send_Answer",
              "error_code": 503,
              "error_response": "Service Unavailable"
            }
          ]
        }
      }
    }
  }
}
```

Failure Case

```
1.
curl -v -H "Content-Type: application/json" --request PUT http://localhost:8081/ocscp/scpc-configuration/v1/routing-config-set/defaultConfig -d '{
  "routingConfigSetName": "defaultRoutingConfigSet",
  "configureRoutingOptions": {
    "odEnabled": false,
    "cbEnabled": false,
    "ociEnabled": false,
    "odRuleName": "defaultRule",
    "cbRuleName": "defaultRule",
    "ociRuleName": "defaultOciConfigRule",
    "pod": {
      "maxRoutingAttempts": 1,
      "alternateRouting": true,
      "loadBalancingAlgorithm": "Round_Robin"
    },
    "alternateNFGroupRoutingOptions": {
      "mode": "NF_SET"
    },
    "srv": {
      "name": "5g-sbi-notification",
      "maxRoutingAttempts": 3,

```

```

    "actions": "Forward",
    "loadBalancingAlgorithm": "Priority_only",
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRule",
    "defaultPriority": 1,
    "defaultCapacity": 65535,
    "reverseProxySupport": false,
    "initialServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    },
    "subsequentServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    }
  },
  "totalTransactionLifetime": "6s",
  "reRouteConditionList": [
    {
      "statusCode": "307"
    },
    {
      "statusCode": "308"
    },
    {
      "statusCode": "429"
    },
    {
      "statusCode": "5xx"
    }
  ],
  "responseTimeout": "1s",
  "exceptionErrorResponses": [
    {
      "name": "Resource_Exhausted",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Response",
      "action": "Send_Answer",
      "error_code": 504,
      "error_response": "Gateway Timeout"
    },
    {
      "name": "Connect_Failure",
      "action": "Send_Answer",
      "error_code": 504,
      "error_response": "Gateway Timeout"
    },
    {
      "name": "No_Host",
      "action": "Send_Answer",
      "error_code": 504,
      "error_response": "Gateway Timeout"
    }
  ]

```

```

    },
    {
      "name": "Db_LookUp_Error",
      "action": "Send_Answer",
      "error_code": 500,
      "error_response": "Session/Subscriber binding not found/look-up
failure at OCSCP-SDS Service"
    }
  ],
  "deploymentModel": "SITE_WIDE",
  "name": "5g-sbi-notification",
  "assignPreferredLocality": false,
  "overridePreferredLocality": false,
  "forwardRevisedPreferredLocality": false,
  "nextHopSEPP": {
    "totalTransactionLifetime": "7s",
    "responseTimeout": "4s",
    "service": {
      "maxRoutingAttempts": 2
    },
    "serviceEndpoint": {
      "maxRoutingAttempts": 1
    },
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopSepp",
    "reRouteConditionList": [
      {
        "statusCode": "307"
      },
      {
        "statusCode": "308"
      },
      {
        "statusCode": "429"
      },
      {
        "statusCode": "5xx"
      }
    ],
    "exceptions": [
      {
        "name": "No_Host",
        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
      }
    ]
  },
  "nextHopScp": {
    "totalTransactionLifetime": "7s",
    "responseTimeout": "4s",
    "service": {
      "maxRoutingAttempts": 2
    },
    "serviceEndpoint": {
      "maxRoutingAttempts": 1
    }
  }
}

```

```

    },
    "loadBasedCongestionControlEnabled": true,
    "nfServiceLoadBasedCongestionControlCfg": "defaultRuleForNextHopScp",
    "exceptions": [
      {
        "name": "No_Host",
        "action": "Send_Answer",
        "error_code": 504,
        "error_response": "Gateway Timeout"
      }
    ]
  }
}
}'

```

HTTP/1.1 400 Bad Request

```

{"title":"Bad Request","status":"400","detail":"RoutingConfigSet Name in
request Body does not match with RoutingConfigSet provided with API .Please
refer to the User Guide","instance":"/ocscp/scpc-configuration/v1/routing-
config-set/defaultConfig","cause":"INVALID_KEY_COMBINATION"}

```

DELETE REST API:

This resource deletes the routing config sets for the specified rules.

Resource URI: /ocscp/scpc-configuration/{version}/routing-config-set/
{routingConfigSetName}

Table 2-333 URI query parameters supported by the DELETE method on this resource

Field Name	Data Type	P	Description
routingOptionsConfigName	String	O	The name of the routing options configuration which needs to be deleted.

Table 2-334 Data structures supported by the Delete Response Body on this resource

Data Type	P	Cardinality	Response codes	Description
Default	M	1	200 OK	-
ProblemDetails	M	1	400/404	Problem details.

Example

Successful response

```

curl -v -H "Content-Type: application/json" --request DELETE http://
localhost:8081/ocscp/scpc-configuration/v1/routing-config-set/defaultConfig

```

HTTP/1.1 204 No Content

Failure case 1

```
curl -v -H "Content-Type: application/json" -X DELETE http://localhost:8081/
ocscp/scpc-configuration/v1/routing-config-set/defaultRule
HTTP/1.1 403 Forbidden
{"title":"Forbidden","status":"403","detail":"Default rule cannot be deleted.
Please refer to the User Guide.","instance":"/ocscp/scpc-configuration/v1/
routing-config-set/defaultRule","cause":"OPERATION_NOT_ALLOWED"}
```

Failure case 2

```
curl -v -H "Content-Type: application/json" --request DELETE http://
localhost:8081/ocscp/scpc-configuration/v1/routing-config-set/
defaultRoutingConfigSet
```

```
HTTP/1.1 403 Forbidden
```

```
{"title":"Forbidden","status":"403","detail":"Default Configuration present
for Routing Config set cannot be deleted","instance":"/ocscp/scpc-
configuration/v1/routing-config-set/
defaultRoutingConfigSet","cause":"OPERATION_NOT_ALLOWED"}
```

2.37 NRF SRV Configuration

This section provides the following NRF SRV Configuration Rest API:

- Resource URIs for the nrfsrvconfig resource type.
- Types of data model.
- URI query parameters supported by GET, PUT, and DELETE methods.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the nrfsrvconfig resource type.

Table 2-335 nrfsrvconfig Resource Type

Resource Name	Resource URI	HTTP Method	Description
nrfsrvconfig	/ocscp/scpc-configuration/ {version}/nrfsrvconfig/ {nrfSrvFqdn}	PUT	Creates the new NRF SRV configuration for the given nrfSrvFqdn or updates the existing NRF SRV configuration.
nrfsrvconfig	/ocscp/scpc-configuration/ {version}/nrfsrvconfig/ {nrfSrvFqdn}	GET	Get the NRF SRV configuration for the given NRF SRV FQDN.
nrfsrvconfig	/ocscp/scpc-configuration/ {version}/nrfsrvconfig	GET	Get all the NRF SRV configuration available in the database.
nrfsrvconfig	/ocscp/scpc-configuration/ {version}/nrfsrvconfig/ {nrfSrvFqdn}	DELETE	Removes the NRF SRV configuration for the given NRF SRV FQDN.

Note

- Use the Configure Alternate NF Group section to refresh the NRF SRV FQDN.
- Set "spnlist" with NRF SRV in SPN format, and set refreshAll to false.

Resource Definition

This section describes GET, PUT, and DELETE resource types supported by NRF SRV configuration.

PUT API

This resource creates the new NRF SRV configuration or updates the existing NRF SRV configuration by taking NRFSRVConfigData as the request body.

Resource URI: /ocscp/scpc-configuration/{version}/nrfsrvconfig/{nrfSrvFqdn}

Request Body**Table 2-336 Data Structures Supported by the PUT Request Body**

Data Type	Description
NRFSRVConfigData	Indicates the data type of the NRF SRV configuration. For more information, see Table 2-340 .

Table 2-337 Data Structures Supported by the PUT Response Body

Data Type	P	Cardinality	Response Codes	Description
NRFSRVConfigData	M	1	200 OK	This response is used when an existing record is updated.
NRFSRVConfigData	M	1	201 CREATED	This response is used when a new entry is created.
ProblemDetails	M	1	400 BAD REQUEST	This response is used when request body validation fails.

The following example is of NRF SRV Configuration REST API for PUT method.

Response:

```
curl -X 'PUT' \
  'http://10.75.226.46:30590/ocscp/scpc-configuration/v1/nrfsrvconfig/nrf2svc.scpsvc.svc.cluster.local' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "nrfSrvFqdn": "nrf2svc.scpsvc.svc.cluster.local",
    "nrfSrvConfig": {
      "nfSetIdList": [
        "setnrfk2.nrfset.5gc.mnc012.mcc345"
```

```

    ],
    "performSubscription": true,
    "performAudit": true,
    "registerScp": true,
    "apiPrefix": "USEast",
    "scheme": "http",
    "versions": [
      {
        "apiVersionInUri": "v1",
        "apiFullVersion": "1.0.0"
      }
    ],
    "serviceNames": [
      "nnrf-nfm",
      "nnrf-disc",
      "nnrf-oauth2"
    ],
    "isInterPlmnFqdn": true
  }
}'

```

Example of NRF SRV Configuration REST API for PUT Method Bad Request

Use case: A configuration where no entry contains 'v1' in apiVersionInUri.

```

curl -X 'PUT' \
  'http://10.75.226.46:30590/ocscp/scpc-configuration/v1/nrfsrvconfig/
nrf2svc.scpsvc.svc.cluster.local' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "nrfSrvConfig":{
      "apiPrefix":"USEast",
      "isInterPlmnFqdn":"false",
      "nfSetIdList":[
        "setnrf11.nrfset.5gc.mnc012.mcc346"
      ],
      "performAudit":"false",
      "performSubscription":"false",
      "plmnList":[
        {
          "mcc":"410",
          "mnc":"213"
        }
      ],
      "registerScp":"false",
      "scheme":"http",
      "serviceNames":[
        "nnrf-nfm",
        "nnrf-disc",
        "nnrf-oauth2"
      ],
      "versions":[
        {
          "apiFullVersion":"1.0.0",
          "apiVersionInUri":"v2"
        }
      ]
    }
  }'

```

```

    }
  ]
},
"nrfSrvFqdn":"nrf1svc.scpsvc.svc.cluster.local"
}
}'

```

Response

```

{
  "title":"Bad Request",
  "status":400,
  "detail":"Atleast one entry in the version list must have its apiVersion
set as v1. Please refer to the User Guide.",
  "instance":"/ocscp/scpc-configuration/v1/nrfsrvconfig/
nrf1svc.scpsvc.svc.cluster.local",
  "cause":"MANDATORY_IE_INCORRECT"
}

```

GET API

This resource fetches the NRF SRV configuration based on the supplied nrfSrvFqdn or fetches all the records.

Resource URI: /ocscp/scpc-configuration/{version}/nrfsrvconfig/{nrfSrvFqdn}

Table 2-338 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
NRFSRVConfigData	M	1..N	200 OK	This response is used when a record is fetched.
ProblemDetails	M	1	404 NOT FOUND	This response is used when no matching entry is found.
ProblemDetails	M	1	400 BAD REQUEST	This response is used when query parameter validation fails.

The following example is of NRF SRV Configuration REST API for GET method.

Response:

```

curl -X 'GET' \
  'http://10.75.226.46:30590/ocscp/scpc-configuration/v1/nrfsrvconfig/
nrf2svc.scpsvc.svc.cluster.local' \
  -H 'accept: application/json'

```

DELETE API

This resource removes the NRF SRV configuration for the given nrfSrvFqdn.

Resource URI: /ocscp/scpc-configuration/{version}/nrfsrvconfig/{nrfSrvFqdn}

Table 2-339 Data Structures Supported by the DELETE Response Body

Data Type	P	Cardinality	Response Codes	Description
None	-	-	204 NO CONTENT	This response is used when the query is successful.
Problem Details	M	1	404 NOT FOUND	This response is used when no matching entry is found.
Problem Details	M	1	400 BAD REQUEST	This response is used when query parameter validation fails.

The following example is of NRF SRV Configuration REST API for DELETE method.

Response:

```
curl -X 'DELETE' \
      'http://10.75.226.46:30590/ocscp/scpc-configuration/v1/nrfsrvconfig/
nrf2svc.scpsvc.svc.cluster.local' \
      -H 'accept: application/json'
```

Data Model

The following tables describe different data models required for configuring NRF SRV data.

Table 2-340 NRFSRVConfigData

Name	Data Type	P	Default Value	Description
nrfSrvFqdn	String	M	NA	The data type of NRF SRV FQDN for the corresponding NRF SRV configuration.
nrfSrvConfig	NRFSRVConfig	M	NA	This is the NRF SRV configuration data.

Table 2-341 NRFSRVConfig

Name	Data Type	P	Default Value	Description
plmnList	List	O	NA	List of the NRF serving PLMN.
nfSetIdList	List	M	NA	This is the SetId list for this NRF SRV configuration. You can configure multiple nfSetIds, but the NRF profile and rule creation will only take into account the nfSetId from the 0th index. This setId must be unique for each NRF SRV configuration; that is, this setId must not be present in any other NRF SRV configuration.

Table 2-341 (Cont.) NRFSRVConfig

Name	Data Type	P	Default Value	Description
performSubscription	boolean	O	true	This field allows to decide whether NRF from this NRF SRV should be used for a subscription or not. The possible values are true or false.
performAudit	boolean	O	true	This field allows to decide whether NRF from this NRF SRV should be used for a audit or not. The possible values are true or false.
registerScp	boolean	O	false	This field allows to decide whether to register SCP with the NRF from the NRF Set. The possible values are true or false.
scheme	UriScheme	M	NA	This field is used for the URI Scheme. The supported value is http/https.
versions	array(NFServiceVersion)	M	NA	This field lists the NFServiceVersion. Configuring multiple API versions is permissible, but at least one entry in the version list must have its apiVersionInUri set to "v1." This is because SCP currently utilizes "v1" for its self-generated requests towards NRF.
apiPrefix	String	O	NA	This field is used in the URI while communicating with NRF.
serviceNames	array(ServiceName)	M	"nnrf-nfm", "nnrf-disc", "nnrf-oauth2"	Indicates the service name of the NRF SRV configuration. The nnrf-nfm and nnrf-disc are mandatory for NRF SRV configurations. The supported value is nnrf-nfm/nnrf-disc/nnrf-oauth2.
isInterPlmnFqdn	boolean	O	false	This field allows you to choose whether or not to map the NRF from this NRF SRV resolution to the InterPlmn Fqdn.

Table 2-342 NFServiceVersion

Name	Data Type	P	Default Value	Description
apiVersionInUri	String	M	NA	The apiVersionInUri is used in the URI while communicating with NRF. The supported value is v1/v2.
apiFullVersion	String	M	NA	The apiFullVersion should be in format x.y.z.

Allowed or Not Allowed API operations

Table 2-343 Different Types of Scenarios

Scenario	Allowed or Not Allowed	Notes
If performAudit is true, and the nnrf-nfm service is configured as a service for audit (global helm configuration), user can remove its entry from the NRF SRV configuration.	Not Allowed	nnrf-nfm service is mandatory
If inserting or updating nfSetId with a value that already exists in another nfSetId configuration.	Not Allowed	-
If performAudit is true, and the nnrf-disc service is configured as a service for audit (global helm configuration), user can remove its entry from the NRF SRV configuration.	Not Allowed	nnrf-disc service is mandatory
If nrfServiceForAudit is nnrf-disc and supported NRF services should have disc and user can change performAudit to true	Allowed	-
If nrfServiceForAudit is nnrf-nfm and supported NRF services should have mgmt and user can change performAudit to true	Allowed	-
If model-D is enabled and nrfSetID (or nrInstanceId) is present in the NRF_CONFIG table for nnrf-disc, and user can remove the nnrf-disc service from the NRF SRV configuration.	Not Allowed	nnrf-disc service is mandatory
If OAuth2 is enabled and nrfSetID (or nrInstanceId) is present in the NRF_CONFIG table for nnrf-oauth2, and user can remove the nnrf-oauth2 service from the NRF SRV configuration.	Not Allowed	-
The registerScp can be set from false to true when nrfset has mgmt service configured in the supported NRF service list.	Allowed	-
The performSubscription can be set from false to true when nrfset has mgmt service configured in the supported NRF service list.	Allowed	-
Configuring the version with the "apiVersionInUri" value as v2 only.	Not Allowed	Configuring multiple API versions is permissible, but at least one entry in the version list must have its apiVersionInUri set to "v1". This is because SCP currently utilizes "v1" for its self-generated requests towards NRF.

Note

Service types nnrf-nfm and nnrf-disc are mandatory for [Table 2-341](#) table configurations. Deletion of nnrf-nfm and nnrf-disc service types from the NRF SRV profile is not supported.

2.38 NRF FQDN InstanceId Mapping

This section describes REST API configurations required for the mapping the NRF FQDN InstanceId.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the nrffqdninstanceidmapping resource type.

Table 2-344 nrffqdninstanceidmapping Resource Type

Resource Name	Resource URI	HTTP Method	Description
nrffqdninstanceidmapping	/ocscp/scpc-configuration/{version}/nrffqdninstanceidmapping	GET	Fetches the NRF FQDN and corresponding instanceid mapping details.

Resource Definition

This section describes GET resource types supported by NRF FQDN InstanceId Mapping.

GET API

This resource fetches the NRF FQDN and corresponding instanceid mapping details.

Resource URI: /ocscp/scpc-configuration/{version}/nrffqdninstanceidmapping

Table 2-345 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
NRFFQDNInstanceIdMappingData	M	1..N	200 OK	This response is used when a record is fetched.

The following example is of NRF FQDN InstanceId Mapping REST API for GET method.

Response:

```
curl -X 'GET'
      'http://10.75.226.46:31527/ocscp/scpc-configuration/v1/
nrffqdninstanceidmapping'
      -H 'accept: application/json'

[
  {
    "nrfFqdn": "nrf2svc.scpsvc.svc.cluster.local",
```

```

    "data": {
      "v1": {
        "nfInstanceId": "e12013b2-590d-39ab-9aba-dac025f69a65",
        "nrfRegionOrSetId": "setnrfl1.nrfset.5gc.mnc012.mcc345",
        "svcNameSvcNfInstanceId": {
          "nnrf-nfm": "fe137ab7-740a-46ee-aa5c-951806d77b01",
          "nnrf-disc": "fe137ab7-740a-46ee-aa5c-951806d77b02",
          "nnrf-oauth2": "fe137ab7-740a-46ee-aa5c-951806d77b03"
        }
      }
    }
  },
  {
    "nrfFqdn": "nrf3svc.scpsvc.svc.cluster.local",
    "data": {
      "v1": {
        "nfInstanceId": "4ca42748-72e2-3dd7-b4a0-4e664b021312",
        "nrfRegionOrSetId": "setnrfl1.nrfset.5gc.mnc012.mcc345",
        "svcNameSvcNfInstanceId": {
          "nnrf-nfm": "fe137ab7-740a-46ee-aa5c-951806d77b01",
          "nnrf-disc": "fe137ab7-740a-46ee-aa5c-951806d77b02",
          "nnrf-oauth2": "fe137ab7-740a-46ee-aa5c-951806d77b03"
        }
      }
    }
  },
  {
    "nrfFqdn": "nrf4svc.scpsvc.svc.cluster.local",
    "data": {
      "v1": {
        "nfInstanceId": "91b26862-b80f-3607-a8ef-43b429cf3b30",
        "nrfRegionOrSetId": "setnrfl1.nrfset.5gc.mnc012.mcc345",
        "svcNameSvcNfInstanceId": {
          "nnrf-nfm": "fe137ab7-740a-46ee-aa5c-951806d77b01",
          "nnrf-disc": "fe137ab7-740a-46ee-aa5c-951806d77b02",
          "nnrf-oauth2": "fe137ab7-740a-46ee-aa5c-951806d77b03"
        }
      }
    }
  },
  {
    "nrfFqdn": "ocnrf-ingressgateway.ocnrf.svc.cluster.local",
    "data": {
      "v1": {
        "nfInstanceId": "85e3cce9-d6f1-3af6-abbb-1419cfb38e1d",
        "nrfRegionOrSetId": "setnrfl1.nrfset.5gc.mnc012.mcc345",
        "svcNameSvcNfInstanceId": {
          "nnrf-nfm": "fe137ab7-740a-46ee-aa5c-951806d77b01",
          "nnrf-disc": "fe137ab7-740a-46ee-aa5c-951806d77b02",
          "nnrf-oauth2": "fe137ab7-740a-46ee-aa5c-951806d77b03"
        }
      }
    }
  }
]

```


Data Model

The following tables describe different data models required for mapping NRF FQDN InstanceId data.

Table 2-346 NRFFQDNInstanceIdMappingData

Name	Data Type	P	Default Value	Description
nrfFqdn	String	M	NA	This is the NRF FQDN received from DNS server.
data	JSON	M	NA	This is the mapping detail of instanceid corresponding to the NRF FQDN.

2.39 Viewing SCP Feature Status

This section describes REST API configurations required for knowing the status of SCP features.

Resources

The following table describes the resource URIs and the corresponding HTTP methods for the scpfeaturestatus resource type.

Table 2-347 scpfeaturestatus Resource Type

Resource Name	Resource URI	HTTP Method	Description
scpfeaturestatus	/ocscp/scpc-configuration/{version}/scpfeaturestatus	GET	Fetches the runtime status of NRF migration task.

Resource Definition

This section describes GET resource types to fetch the runtime status of the NRF migration task.

Resource URI: /ocscp/scpc-configuration/{version}/scpfeaturestatus

Table 2-348 Data Structures Supported by the GET Response Body

Data Type	P	Cardinality	Response Codes	Description
SCPFeatureStatusData	M	1	200 OK	This response is used when a record is fetched.

The following example is of SCP Feature Status REST API for GET method.

Response:

```
curl -X 'GET'
      'http://10.75.226.46:31527/ocscp/scpc-configuration/v1/scpfeaturestatus'
      -H 'accept: application/json'
```

```
[
  {
    "feature": "nrf_bootstrap_info",
    "admin": "ENABLED",
    "status": "ENABLED"
  }
]
```

Data Model

The following tables describe different data models required for SCP Feature Status REST API.

Table 2-349 SCPFeatureStatusData

Name	Data Type	P	Default Value	Description
feature	String	M	nrf_bootstrap_info	Indicates the names of the services, such as nrf_bootstrap_info. Note: Currently, this API is only supported for nrf_bootstrap_info feature.
admin	String	M	Disabled	Indicates the admin status for performing the migration.
status	String	M	Disabled	Indicates the runtime status of the feature.
creationtimestamp	Integer	M	NA	Indicates the time of creation of the event, for example, creationTimestamp": "2021-05-26T01:17:15.000+00:00
updatetimestamp	Integer	M	NA	Indicates the time of updation of the event, for example, updateTimestamp": "2021-05-26T06:24:15.000+00:00

A

HTTP Status Code and Applicability for Rerouting

This section describes the HTTP status codes usage on SBI. HTTP status codes are carried in the ":status" pseudo header field in HTTP/2, as defined in subclause 8.1.2.4 in IETF RFC 7540.

The following table specifies HTTP status codes per HTTP method which is supported on SBI. Support of the HTTP status code is:

- Mandatory, which is marked in table as "**M**". This signifies that all 3GPP NFs support the processing of the specific HTTP status code for the specific HTTP method, when received in a HTTP response message. In such cases the 3GPP NF also supports the handling of the "ProblemDetails" JSON object with the Content-Type header field set to the value "application/problem+json" for HTTP status codes 4xx and 5xx, if the corresponding API definition in the related technical specification does not specify another response body for the corresponding status code;
- Service specific, which is marked in table as "**SS**" and means that the requirement to process the HTTP status code depends on the definition of the specific API; or
- Not applicable, which is marked in table as "**N/A**". This means that the specific HTTP status code shall not be used for the specific HTTP method within the 3GPP NFs.
- Applicable for Rerouting column describes if the status code is applicable for rerouting at SCP. These Status codes can be configured in Routing options for each NF services.

NOTE 1: "200 OK" response used on SBI shall contain body.

NOTE 2: If the NF acting as an HTTP Client receives 2xx response code not appearing in table, the NF shall treat the received 2xx response: - as "204 No Content" if 2xx response does not contain body; and - as "200 OK" if 2xx response contains body.

HTTP status code supported on SBI

Table A-1 HTTP status code supported on SBI

HTTP Status Code						Applicable for Rerouting	HTTP Method
	DELETE	GET	PATCH	POST	PUT		
100 Continue	N/A	N/A	N/A	N/A	N/A	No	
200 OK (NOTE 1)	SS	M	SS	SS	SS	No	
201 Created	N/A	N/A	N/A	SS	SS	No	
202 Accepted	SS	N/A	SS	SS	SS	No	
204 No Content (NOTE 2)	M	N/A	SS	SS	SS	No	
300 Multiple Choices	N/A	N/A	N/A	N/A	N/A	No	
303 See Other	SS	SS	N/A	SS	SS	No	

Table A-1 (Cont.) HTTP status code supported on SBI

307 Temporary Redirect	SS	SS	SS	SS	SS	Yes	307 (Should be included as part of 3xx)
308 Permanent Redirect	SS	SS	SS	SS	SS	Yes	308 (Should be included as part of 3xx)
400 Bad Request	M	M	M	M	M	No	
401 Unauthorized	M	M	M	M	M	No	
403 Forbidden	SS	SS	SS	SS	SS	No	
404 Not Found	SS	SS	SS	SS	SS	Yes	404
405 Method Not Allowed	SS	SS	SS	SS	SS	No	
406 Not Acceptable	N/A	N/A	N/A	N/A	N/A	No	
408 Request Timeout	SS	SS	SS	SS	SS	Yes	408
409 Conflict	N/A	N/A	SS	SS	SS	Yes	409 (should be included as part of "retriable-4xx")
410 Gone	SS	SS	SS	SS	SS	Yes	410
411 Length Required	N/A	N/A	M	M	M	No	
412 Precondition Failed	SS	SS	SS	SS	SS	No	
413 Payload Too Large	N/A	N/A	M	M	M	No	
414 URI Too Long	N/A	M	N/A	N/A	N/A	No	
415 Unsupported Media Type	N/A	N/A	M	M	M	No	
429 Too Many Requests	N/A	N/A	N/A	N/A	N/A	Yes	
500 Internal Server Error	M	M	M	M	M	Yes	500
501 Not Implemented	SS	SS	SS	SS	SS	Yes	501
502 Bad Gateway	SS	SS	SS	SS	SS	Yes	502 (Should be included as part of gateway error and "5xx")
503 Service Unavailable	M	M	M	M	M	Yes	503 (Should be included as part of "5xx")
504 Gateway Timeout	SS	SS	SS	SS	SS	Yes	504 (Should be included as part of "5xx")

NF as HTTP Client

Besides the HTTP Status Codes defined in the API specification, a NF as HTTP client should support handling of 1xx, 3xx, 4xx and 5xx HTTP Status Codes specified in above table,

following the client behavior in corresponding IETF RFC where the received HTTP Status Code is defined.

When receiving a not recommended or not recognized 1xx, 3xx, 4xx or 5xx HTTP Status Code, a NF as HTTP client should treat it as x00 status code of the class, as described in clause 6 of IETF RFC 7231.

If 100, 200/204, 300, 400 or 500 response code is not defined by the API specification, the client may follow guidelines below:

- For 1xx (Informational):
 - Discard the response and wait for final response.
- For 2xx (Successful):
 - Consider the service operation is successful if no mandatory information is expected from the response payload in subsequent procedure.
 - If mandatory information is expected from response payload in subsequent procedure, parse the payload following description in subclause 6.2.1 of IETF RFC 7231 [11]. If parse is successful and mandatory information is extracted, continue with subsequent procedure.
 - Otherwise, consider service operation has failure and start failure handling.
- For 3xx (Redirection):
 - Retry the request towards the directed resource referred in the Location header, using same request method.
- For 4xx (Client Error):
 - Validate the request message and make correction before resending. Otherwise, stop process and go to error handling procedure.
- For 5xx (Server Error):
 - Stop process and go to error handling process.

NF as HTTP Server

A NF acting as an HTTP server is able to generate HTTP status codes specified in above table per indicated HTTP method.

An HTTP method which is not supported by 5GC SBI API specification is rejected with the HTTP status code "501 Not Implemented".

NOTE 1: In this case, the NF does not need to include in the HTTP response the "cause" attribute indicating corresponding error since the HTTP status code "501 Not Implemented" itself provides enough information of the error, that is, the NF does not recognize the HTTP method.

If the specified target resource does not exist, the NF rejects the HTTP method with the HTTP status code "404 Not Found".

If the NF supports the HTTP method but not by a target resource, the NF rejects the HTTP method with the HTTP status code "405 Method Not Allowed" and includes in the response an Allow header field containing the supported method(s) for that resource.

NOTE 2: In this case, the NF does not need to include in the HTTP response the "cause" attribute indicating corresponding error since the HTTP status code "405 Method Not Allowed" itself provides enough information of the error and hence the Allow header field lists HTTP method(s) supported by the target resource.

If the received HTTP request contains incorrect optional IE, the NF discards the incorrect IE.

If the NF supports the HTTP method by a target resource but the NF cannot successfully fulfill the received request, the following requirements apply.

A NF as HTTP Server should map application errors to the most similar 3xx/4xx/5xx HTTP status code specified in table 5.2.7.1-1. If no such code is applicable, it should use "400 Bad Request" status code for errors caused by client side or "500 Server Internal Error" status code for errors caused on server side.

If the received HTTP request contains unsupported payload format, the NF rejects the HTTP request with the HTTP status code "415 Unsupported Media Type". If the HTTP PATCH method is rejected, the NF includes the Accept-Patch header field set to the value of supported patch document media types for a target resource i.e. to "application/merge-patch+json" if the NF supports "JSON Merge Patch" and to "application/json-patch+json" if the NF supports "JSON Patch". If the received HTTP PATCH request contains both "JSON Merge Patch" and "JSON Patch" documents and the NF supports only one of them, the NF ignores unsupported patch document.

NOTE 3: The format problem might be due to the request's indicated Content-Type or Content-Encoding header fields, or as a result of inspecting the payload body directly.

If the received HTTP request contains payload body larger than the NF is able to process, the NF rejects the HTTP request with the HTTP status code "413 Payload Too Large".

If the result of the received HTTP POST request used for a resource creation is equivalent to the existing resource, the NF rejects the HTTP request with the HTTP status code "303 See Other" and includes in the HTTP response a Location header field set to the URI of the existing resource.

Protocol and application errors common to several 5GC SBI API specifications for which the NF includes in the HTTP response a payload body ("ProblemDetails" data structure or application specific error data structure) with the "cause" attribute indicating corresponding error are listed in below table.

Table A-2 Protocol and Application Errors

Parameters	HTTP status code	Description
INVALID_API	400 Bad Request	The HTTP request contains an unsupported API name or API version in the URI.
INVALID_MSG_FORMAT	400 Bad Request	The HTTP request has an invalid format.
INVALID_QUERY_PARAM	400 Bad Request	The HTTP request contains an unsupported query parameter in the URI.
MANDATORY_IE_INCORRECT	400 Bad Request	A mandatory IE or conditional IE in data structure, but mandatory required, for an HTTP method was received with a semantically incorrect value. (NOTE 1)
MANDATORY_IE_MISSING	400 Bad Request	IE which is defined as mandatory or as conditional in data structure, but mandatory required, for an HTTP method is not included in the payload body of the request. (NOTE 1)

Table A-2 (Cont.) Protocol and Application Errors

Parameters	HTTP status code	Description
UNSPECIFIED_MSG_FAILURE	400 Bad Request	The request is rejected due to unspecified client error. (NOTE 2)
MODIFICATION_NOT_ALLOWED	403 Forbidden	The request is rejected because the contained modification instructions attempt to modify IE which is not allowed to be modified.
SUBSCRIPTION_NOT_FOUND	404 Not Found	The request for modification or deletion of subscription is rejected because the subscription is not found in the NF.
RESOURCE_URI_STRUCTURE_NOT_FOUND	404 Not Found	The request is rejected because a fixed part after the first variable part of an "apiSpecificResourceUriPart" (as defined in subclause 4.4.1 of 3GPP TS 29.501) is not found in the NF. This fixed part of the URI may represent a sub-resource collection (e.g. contexts, subscriptions, policies) or a custom operation. (NOTE 5)
INCORRECT_LENGTH	411 Length Required	The request is rejected due to incorrect value of a Content-length header field.
NF_CONGESTION_RISK	429 Too Many Requests	The request is rejected due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation.
INSUFFICIENT_RESOURCES	500 Internal Server Error	The request is rejected due to insufficient resources.
UNSPECIFIED_NF_FAILURE	500 Internal Server Error	The request is rejected due to unspecified reason at the NF. (NOTE 3)
SYSTEM_FAILURE	500 Internal Server Error	The request is rejected due to generic error condition in the NF.
NF_CONGESTION	503 Service Unavailable	The NF experiences congestion and performs overload control, which does not allow the request to be processed. (NOTE 4)

NOTE 1: "invalidParams" attribute is included in the "ProblemDetails" data structure indicating missing or incorrect IE.

NOTE 2: This application error indicates error in the HTTP request and there is no other application error value that can be used instead.

NOTE 3: This application error indicates error condition in the NF and there is no other application error value that can be used instead.

NOTE 4: If the reason for rejection is a temporary overload, the NF may include in the response a Retry-After header field to indicate how long the service is expected to be unavailable.

NOTE 5: If the request is rejected because of an error in the URI before the first variable part of "apiSpecificResourceUriPart", then the "404 Not Found" HTTP status code may be sent without the "ProblemDetails" data structure indicating protocol or application error.

B

Error Code Generated by SCP

This section describes HTTP error responses generated by SCP:

Table B-1 SCP Generated Error Responses

HTTP Status Code	Sample Error Scenarios at SCP
400	When SCP receives a request with malformed URL (For example, % is added URL after apiRoot).
400 Not Found	When SCP receives request with the 3gpp-sbi-routing-binding header and an invalid version.
400 Bad Request	When SCP receives a request with the malformed 3GPP-SBI-routing-binding header.
411 Length Required	Not Applicable
413 Payload Too Large	Not Applicable
429 Too Many Requests	When the ingress rate exceeds the configured limit for a given consumer, SCP rejects the additional messages with the error code.
431 Request Header Fields Too Large	When SCP receives a request with the total length of the headers are larger than 8k.
500 Internal Error	- Sample 1: When payload size content length exceeds the 256 KB threshold limit. - Sample 2: When the response is bigger than configured. <code>maxPayloadSizeInKb</code>. - Sample 3: When SCP receives a request with incorrect content-length header field.
503 NF_CONGESTION	- Sample 1: When the producer is overloaded and no alternates are available. - Sample 2: When the SCP is overloaded based on configured thresholds.
503 Service Unavailable	When SCP receives a request with the 3gpp-sbi-routing-binding header and an invalid API name.
504 Gateway Timeout	When no response is received from a producer for the configured response timeout value.
508 Loop Detected	When SCP receives a via header with its own FQDN or IP.