Oracle® Communications

Cloud Native Core, Binding Support Function REST Specification Guide

Release 25.1.202
G27768-04
April 2026

Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide, Release 25.1.202

G27768-04

Contents

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support

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

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

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

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

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

Acronyms

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

Table Acronyms

Field	Description
AF	Application Function
BSF	Binding Support Function
FQDN	Fully Qualified Domain Names
GPSI	Generic Public Subscription Identifier
HTTP	Hypertext Transfer Protocol
NEF	Network Exposure Function
NF	Network Function
NRF	NF Repository Function
PCF	Policy Control Function
OCPM	Oracle Communications Policy Management
PDU	Protocol Data Unit
RDBMS	Relational Database Management System
S-NSSAI	Single Network Slice Selection Assistance Information. An S-NSSAI is comprised of: - A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services; - A Slice Differentiator (SD), which is an optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.
SMF	Session Management Function
SUPI	Subscription Permanent Identifier
UDSF	Unstructured Data Storage network function
UE	User Equipment

What's New in This Guide

This section introduces the documentation updates for Release 25.1.2xx in this guide.

Release 25.1.202 - G27768-04, April 2026

There is no change to this document in this release.

Release 25.1.201 - G27768-03, January 2026

There is no change to this document in this release.

Release 25.1.201 - G27768-02, November 2025

There is no change to this document in this release.

Release 25.1.200 - G27768-01, July 2025

- Added the following Pod congestion control settings APIs in Congestion Control Configurations section:
  - `Congestion Control Settings`
  - `Congestion Control Threshold Profile`
  - `Import/Export Congestion Control Settings`
  - `Import/Export Congestion Control Threshold Profiles`
- Added the following Pod congestion control load shedding APIs in Congestion Control Load Shedding Profiles section.
  - `Congestion Control Load Shedding Rules`
  - `Congestion Control Load Shedding Profiles`
  - `Import/Export Congestion Control Load Shedding Rules`
- Added the Diameter Gateway Congestion Migration APIs to support data migration of Diameter Gateway service congestion control configurations..
- Added the following configuration parameters for enhanced logging in General Configurations:
  - enhancedLogging.enableEnhancedLogging
  - enhancedLogging.staleSessionDeletionLogLevel
  - enhancedLogging.enableLogUEIdentifierInfo
  - enhancedLogging.enableLogUeInfoInSessionDeletion

1 Introduction

This document provides information about how to configure the services and manageable objects in Oracle Communications Cloud Native Binding Support Function (BSF) Management Service using Representational State Transfer Application Program Interfaces (REST APIs).

1.1 Overview

BSF provides a Protocol Data Unit (PDU) session binding functionality, which ensures that an Application Function (AF) request for a certain PDU Session reaches the relevant Policy Control Function (PCF) holding the PDU Session information. This Network Function (NF):

- Allows Policy Control Function users to register, update, and remove the binding information
- Allows NF consumers to retrieve the binding information

> **Note**
>
> The performance and capacity of the BSF system may vary based on the call model, Feature/Interface configuration, and underlying CNE and hardware environment.

1.2 References

Refer to the following documents while deploying BSF:

- *Oracle Communications Cloud Native Binding Support Function Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function Network Impact Report Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function Troubleshooting Guide*
- *Oracle Communications Cloud Native Core, Cloud Native Environment Installation and Upgrade Guide*
- *Oracle Communications Cloud Native Core, cnDBTier User Guide*
- *Oracle Communications Cloud Native Core, Data Collector User Guide*
- *Oracle Communications Cloud Native Core Automated Test Suite Guide*
- *Oracle Communications Cloud Native Core Release Notes*
- *Oracle Communications Cloud Native Core Solution Upgrade Guide*

1.3 OpenAPI Specification

BSF supports the OpenAPI version 1.0.0.

2
BSF REST Specifications

This section provides information about REST specifications used in Oracle Communications Cloud Native Core Binding Support Function (BSF).

2.1 Congestion Control Configurations

> **Note**
>
> The default Congestion Control Threshold profile cannot be updated by the User.

Congestion Control Configurations

The Pod Congestion Control BSF services, resource URI parameter `{serviceName}` values can be:

- `oc-diam-gateway`
- `BSF Management`

Table 2-1 Congestion Control Settings APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Get congestion control settings.	GET	{apiRoot}/oc-bsf-configuration/v1/congestionConfigurations/{serviceName}	To get enable, stateChangeSampleCount and stateCalculationInterval	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-1 (Cont.) Congestion Control Settings APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Update congestion control settings.	PUT	{apiRoot}/oc-bsf-configuration/v1/congestionConfigurations/{serviceName}	To update enable, stateChangeSampleCount and stateCalculationInterval	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Update Operations

Table 2-2 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enable	boolean	O	Enable or Disable the Pod Congestion Control feature. **Default value**: false (after upgrade) **Default value**: true (for fresth installation)
stateChangeSampleCount	integer	M	After how many continuous intervals, state can be changed. The count can range from 1 to 2147483647. **Default value**: 5

Table 2-2 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
stateCalculationInterval	integer	M	Number of interval in milliseconds, after which the pod congestion state will be re-verified. **Default value**: 200ms
activeThresholdProfile	String	O	Active threshold profile name. **Default value**: Default
advancedSettings	AdvancedSettings	O	To add additional advanced settings keys to the settings.

Table 2-3 AdvancedSettings

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
key	string	O	Specifies the key name.
value	string	O	Specifies the value of the key.

Sample body request for Put operation for Congestion Control Settings:

```
{
  "activeThresholdProfile": "profileName",
  "stateChangeSampleCount": 5,
  "stateCalculationInterval": 200,
  "enable": true,
  "advancedSettings": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Congestion Control Threshold Profile

Table 2-4 Congestion Control Threshold Profile APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Update congestion control active threshold profile.	PUT	{apiRoot}/oc-bsf-configuration/v1/congestionActiveThresholdProfile/{serviceName}/{activeThresholdProfile}	To update the active threshold profile.	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get active congestion threshold profile.	GET	{apiRoot}/oc-bsf-configuration/v1/congestionActiveThresholdProfile/{serviceName}	To get the CPU and Queue threshold of DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2 and CONGESTED states for all threshold profiles	200: OK General configuration is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-4 (Cont.) Congestion Control Threshold Profile APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Update congestion control threshold profile.	PUT	{apiRoot}/oc-bsf-configuration/v1/congestionThresholdProfiles/{serviceName}/{profileName}	To update the CPU and Queue threshold of DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2 and CONGESTED states of specific threshold profile.	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get congestion control threshold profiles.	GET	{apiRoot}/oc-bsf-configuration/v1/congestionThresholdProfiles/{serviceName}	To get the CPU(%) and Queue(pending counts) of DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2 and CONGESTED states for all threshold profiles.	200: OK General configuration is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-4 (Cont.) Congestion Control Threshold Profile APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Add congestion control threshold profile.	POST	{apiRoot}/oc-bsf-configuration/v1/congestionThresholdProfiles/{serviceName}/{profileName}	To add new congestion threshold profile with specified name	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Delete congestion control threshold profile.	DELETE	{apiRoot}/oc-bsf-configuration/v1/congestionThresholdProfiles/{serviceName}/{profileName}	To delete new congestion threshold profile with specified name	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too many Requests 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get, Put, and Post Operations

Table 2-5 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	String	M	This value should be same as the `profileName` in path variable.

Table 2-5 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
value	CongestionThresholdState	M	Provide the congestion state.
isCustomProfile	Boolean	M	Denotes that this profile is custom created. **Note**: Currently user can create custom profiles only. Hence this value should be set to `true`.

Table 2-6 CongestionThresholdState

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
state	String	M	The value can be following pod Congestion states: • DANGER_OF_CONGESTION • CONGESTION_L1 • CONGESTION_L2 • CONGESTED Bulwark service supports only two states DANGER_OF_CONGESTION and CONGESTED.
resourceUsageLimit	CongestionResourceUsageLimit	M	The Threshold profiles resource usage limits for CPU & Queue.

Table 2-7 CongestionResourceUsageLimit

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
cpu	integer	M	Specifies the Queue percentage for Bulwark and Queue (pending requests) for all other BSF services across all the congestion levels. For Bulwark the range is 1 to 100 and for other services the range is between 1 to 2147483647.

Table 2-7 (Cont.) CongestionResourceUsageLimit

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
queue	integer	M	Specifies the CPU percentage across all the congestion levels. The number can be between 1 to 100.

Sample body request for Put and Post operations for Congestion Threshold Profiles:

```
{
"name": "profileName",
"isCustomProfile": true,
"value": [
        {
        "state": "DANGER_OF_CONGESTION",
        "resourceUsageLimit": {
          "cpu": 40,
          "queue": 32
        }
      },
      {
        "state": "CONGESTION_L1",
        "resourceUsageLimit": {
          "cpu": 50,
          "queue": 34
        }
      },
     {
        "state": "CONGESTION_L2",
        "resourceUsageLimit": {
          "cpu": 60,
          "queue": 36
        }
      },
      {
        "state": "CONGESTED",
        "resourceUsageLimit": {
          "cpu": 70,
          "queue": 38
        }
      }
]}
```

Import or Export the Congestion Control Settings

Table 2-8 Imort/Export Congestion Control Settings

API Name	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Export Congestion Control Settings	GET	{apiRoot}/oc-bsf-configuration/v1/congestionConfigurations/export	To export congestion control settings	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Import Congestion Control Settings	POST	{apiRoot}/oc-bsf-configuration/v1/congestionConfigurations/import?action={action}	To import congestion control settings	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-9 Request/Response Body Parameters

Field Name	Data Type	Mandatory/Optional/ Conditional	Description
topic	String	M	It should be commonconfig.congestionControlSettings
sourceVersion	String	M	Build version
date	String	M	Date in pattern "*yyyy-MM-dd'T'HH:mm:ss'Z'*"
exportData	Congestion Control Settings Data	M	Array for Congestion Control Settings. This array contains JSON objects for each service that supports congestion control feature.

```
{
  "topic": "commonconfig.congestionControlSettings",
  "sourceVersion": "23.4.0-nb-20231118",
  "date": "2023-12-03T10:48:08Z",
  "exportData": [
    {
      "serviceName": "BSF Management",
      "stateChangeSampleCount": 2,
      "stateCalculationInterval": 5000,
      "enable": true
    },
    {
      "serviceName": "bulwark",
      "activeThresholdProfile": "DEFAULT",
      "stateChangeSampleCount": 2,
      "stateCalculationInterval": 5000
    }
  ]
}
```

Import and Export Congestion Control Threshold Profiles

Table 2-10 Import/Export Congestion Control Threshold Profiles

API Name	Request Type	Request Url	Description
Export Congestion Control Threshold Profiles	GET	{apiRoot}/oc-bsf-configuration/v1/congestionThresholdProfiles/export	To export congestion control threshold profiles
Import Congestion Control Threshold Profiles	POST	{apiRoot}//oc-bsf-configuration/v1/congestionThresholdProfiles/import?action={action}	To import congestion control threshold profiles

Table 2-11 Request/Response Body Parameters

Field Name	Data Type	Mandatory/Optional/ Conditional	Description
topic	String	M	It should be commonconfig.congestionThresholdProfiles
sourceVersion	String	M	Build version
date	String	M	Date in pattern "*yyyy-MM-dd'T'HH:mm:ss'Z'*"
exportData	Congestion Threshold Profiles Data	M	Array for Congestion Control Threshold Profiles. This array contains JSON objects of each service that supports congestion control feature.


```
{
    "topic": "commonconfig.congestionThresholdProfiles",
    "sourceVersion": "24.1.0-rc.4",
    "date": "2024-02-29T10:03:44Z",
    "exportData": [
        {
            "activeThresholdProfile": "DEFAULT",
            "congestionThresholdProfiles": [
                {
                    "name": "DEFAULT",
                    "value": [
                        {
                            "state": "DANGER_OF_CONGESTION",
                            "resourceUsageLimit": {
                                "cpu": 55,
                                "queue": 60
                            }
                        },
                        {
                            "state": "CONGESTION_L1",
                            "resourceUsageLimit": {
                                "cpu": 65,
                                "queue": 70
                            }
                        },
                        {
                            "state": "CONGESTION_L2",
                            "resourceUsageLimit": {
                                "cpu": 75,
                                "queue": 80
                            }
                        },
                        {
                            "state": "CONGESTED",
                            "resourceUsageLimit": {
```

```
                                "cpu": 85,
                                "queue": 90
                            }
                        }
                    ],
                    "isCustomProfile": false
                }
            ],
            "serviceName": "BSF Management"
        },
        {
            "activeThresholdProfile": "DEFAULT",
            "congestionThresholdProfiles": [
                {
                    "name": "DEFAULT",
                    "value": [
                        {
                            "state": "DANGER_OF_CONGESTION",
                            "resourceUsageLimit": {
                                "cpu": 80,
                                "queue": 75
                            }
                        },
                        {
                            "state": "CONGESTED",
                            "resourceUsageLimit": {
                                "cpu": 90,
                                "queue": 85
                            }
                        }
                    ],
                    "isCustomProfile": false
                }
            ],
            "serviceName": "bulwark"
        }
    ]
}
```

2.2 Congestion Control Load Shedding Profiles

Congestion Control Load Shedding Rules APIs

Table 2-12 Congestion Control Load Shedding Rules APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Get congestion load shedding profiles.	GET	{apiRoot}/oc-bsf-configuration/v1/congestionLoadSheddingProfile/{serviceName}	To get the name, type and active load shedding rule.	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Update congestion load shedding profile.	PUT	{apiRoot}/oc-bsf-configuration/v1/congestionLoadSheddingProfile/{serviceName}	To update name and loadSheddingRule Name	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-12 (Cont.) Congestion Control Load Shedding Rules APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Get congestion control load shedding rules.	GET	{apiRoot}/oc-bsf-configuration/v1/congestionLoadSheddingRule/{serviceName}	To get the discard priority of DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2 and CONGESTED states for all load shedding rules.	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Update congestion control load shedding rule.	PUT	{apiRoot}/oc-bsf-configuration/v1/congestionLoadSheddingRule/{serviceName}/{ruleName}	To update the discard priority of DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2 and CONGESTED states of specific threshold rule.	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-12 (Cont.) Congestion Control Load Shedding Rules APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Add congestion control load shedding rule.	POST	{apiRoot}/oc-bsf-configuration/v1/congestionLoadSheddingRule/{serviceName}/{ruleName}	To add new congestion load shedding rule with specified name	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Delete congestion control load shedding rule.	DELETE	{apiRoot}/oc-bsf-configuration/v1/congestionLoadSheddingRule/{serviceName}/{ruleName}	To delete congestion load shedding rule with specified name	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too many Requests 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-13 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	String	M	This value should be same as the `ruleName` in path variable.
value	CongestionLoadSheddingState	M	This value should be different congestion states.

Table 2-13 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
isCustomProfile	Boolean	M	Denotes that the rule is custom created by user. **Note**: Currently user can create custom rules only. Hence this value should be set to `true`.

Table 2-14 CongestionLoadSheddingState

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
state	String	M	The value can be following pod Congestion states: • DANGER_OF_CONGESTION • CONGESTION_L1 • CONGESTION_L2 • CONGESTED Bulwark service supports only two states DANGER_OF_CONGESTION and CONGESTED.
discardPriority	integer	M	The discard priority value for the requests. The minimum value is `0` and maximum value is 31. **Default Value**: 5
discardPriorityPercentage	DiscardPriorityPercentage	O	The discard priority range or percentage for the requests. **Note**: This is applicable only to `Diameter Gateway` service.

Table 2-15 DiscardPriorityPercentage

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
range	string	M	The discard priority value or range for the requests. The values allowed is a number such as 1 or a pattern like 11-13. **Note**: This is applicable only to Diameter Gateway service.
percentage	integer	M	The percentage of requests that needs to be discarded. The minimum value is 1 and maximum value is 100. **Example**: 23 **Note**: This is applicable only to Diameter Gateway service.

```
{
  "name": "ruleName",
  "value":
[
    {
      "state": "CONGESTED",
      "discardPriority": 5
    },
    {
      "state": "CONGESTION_L2",
      "discardPriority": 10
    },
    {
      "state": "CONGESTION_L1",
      "discardPriority": 15
    },
    {
      "state": "DANGER_OF_CONGESTION",
      "discardPriority": 20
    }
  ],
  "isCustomProfile": true
}
```

Import or Export Congestion Control Load Shedding Rules

Table 2-16 Import/Export Congestion Control Load Shedding Rules

API Name	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Export Congestion Control Load Shedding Rules	GET	{apiRoot}//oc-bsf-configuration/v1/congestionLoadSheddingRule/export	To export congestion control load shedding rules	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Import Congestion Control Load Shedding rules	POST	{apiRoot}/oc-bsf-configuration/v1/congestionThresholdProfiles/import?action={action}	To import congestion control load shedding rules	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-17 Request/Response Body Parameters

Field Name	Data Type	Mandatory/Optional/ Conditional	Description
topic	String	M	commonconfig.congestionLoadSheddingRules
sourceVersion	String	M	Build version
date	String	M	Date in pattern "*yyyy-MM-dd'T'HH:mm:ss'Z'*"
exportData	Congestion Load Shedding Data	M	Array for Congestion Control Settings. This array contains JSON objects for each service that supports congestion control feature.


```
{
  "topic": "commonconfig.congestionLoadSheddingRules",
  "sourceVersion": "23.4.0-nb-20231118",
  "date": "2023-12-03T11:14:26Z",
  "exportData": [
    {
      "congestionLoadSheddingProfiles": [
        {
          "name": "loadSheddingProfile",
          "loadSheddingRuleName": "rule1",
          "type": "congestion"
        }
      ],
      "congestionLoadSheddingRules": [
        {
          "name": "DEFAULT",
          "value": [
            {
              "state": "CONGESTED",
              "discardPriority": 5
            },
            {
              "state": "CONGESTION_L2",
              "discardPriority": 10
            },
            {
              "state": "CONGESTION_L1",
              "discardPriority": 15
            },
            {
              "state": "DANGER_OF_CONGESTION",
              "discardPriority": 20
            }
          ],
          "isCustomProfile": false
        },
        {
```

```
            "name": "rule1",
            "value": [
              {
                "state": "CONGESTED",
                "discardPriority": 5
              },
              {
                "state": "CONGESTION_L2",
                "discardPriority": 10
              },
              {
                "state": "CONGESTION_L1",
                "discardPriority": 15
              },
              {
                "state": "DANGER_OF_CONGESTION",
                "discardPriority": 20
              }
            ],
            "isCustomProfile": true
          }
        ],
        "serviceName": "BSF Management"
      },
      {
        "congestionLoadSheddingProfiles": [
          {
            "name": "loadSheddingProfile",
            "loadSheddingRuleName": "DEFAULT",
            "type": "congestion"
          }
        ],
        "congestionLoadSheddingRules": [
          {
            "name": "DEFAULT",
            "value": [
              {
                "state": "DANGER_OF_CONGESTION",
                "discardPriority": 20
              },
              {
                "state": "CONGESTED",
                "discardPriority": 10
              }
            ],
            "isCustomProfile": false
          }
        ],
        "serviceName": "bulwark"
      }
    ]
  }
```

2.3 Diameter Gateway Congestion Migration

Diameter Gateway Congestion Control Data Migration

Table 2-18 Diameter Gateway Congestion Migration APIs

API Description	HTTP Method or Custom Operation	Resource URI	Description	Possible Result Code
Get Diameter-Gateway Congestion Migration Details	GET	{apiRoot}/oc-bsf-configuration/v1/congestioncontrol/diameter-gateway/migration	To get the status of data migration details when the systems is upgraded from the older version to current version.	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Migrate congestion control previous version configuration data to current version	POST	{apiRoot}/oc-bsf-configuration/v1/congestioncontrol/diameter-gateway/migration	Migrate congestion control previous version configuration data to current version by taking some required inputs from the user and this migration is the one-time activity after version upgrade from old version to current version.	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-19 Request/Response Congestion Migration Data

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enable	boolean	M	This enables the congestion control feature after successful migration.
thresholdsProfileData	ThresholdsProfileData	M	This new thresholds profile will be created with this profile data.
loadSheddingProfileData	LoadSheddingProfileData	M	This load shedding profile will configure as default profile for congestion load shedding rules.
messagePriorityProfileData	MessagePriorityProfileData	M	This message priority profile will configure as default profile for message priority profile, and this will be the common profile for both overload and congestion control feature.

Table 2-20 Request/Response ThresholdsProfileData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
profileName	string	M	A new thresholds profile will be created with this profile name to migrate the old version thresholds data.
queueData	CongestionStateData	M	This queue data will be applied for different congestion states to migrate the old version threshold data.
cpuData	CongestionStateData	M	This CPU data will be applied for congestion states to migrate the old version thresholds data.

Table 2-21 Request/Response LoadSheddingProfileData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
profileName	string	M	The provided load shedding profile will become the default profile for congestion load shedding rules. **Value**: Provide previous version profile name.
ruleDiscardPriorityData	CongestionStateData	M	This Respective Discard Priority data will be applied for congestion states to migrate the old version thresholds data.
loadSheddingResponseCodeData	LoadSheddingResponseCodeData	M	This congestion response result code will configure as common response code for all congestion discards in advance settings configurations.
ruleDiscardPriorityPercentageData	CongestionStatePriorityPercentageData	M	This is to decide the result code is the general result code or experimental result code, so if this value is greater than then the congestionResponseResultCode is consider as experimental result code.

Table 2-22 Request/Response CongestionStateData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
queueData.state	string	M	Specifiy different congestion states. The allowed values are: • DANGER_OF_CONGESTION • CONGESTION_L1 • CONGESTION_L1 • CONGESTED
queueData.value	integer	M	Provide a numerical value in the range of 1-2147483647.

Table 2-22 (Cont.) Request/Response CongestionStateData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
cpuData.state	string	M	Specifiy different congestion states. The allowed values are: • CONGESTION_L1 • CONGESTION_L1
cpuData.value	integer	M	Provide a numerical value in the range of 1-100.
ruleDiscardPriorityData.state	string	M	Specifiy different congestion states. The allowed values are: • CONGESTION_L1 • CONGESTION_L1
ruleDiscardPriorityData.value	integer	M	Provide a numerical value in the range of 1-31.

Table 2-23 Request/Response CongestionStatePriorityPercentageData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
state	string	M	
discardPriorityPercentagesData	DiscardPriorityPercentage	M	

Table 2-24 Request/Response DiscardPriorityPercentage

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
range	string	M	
percentage	integer	M	

Table 2-25 Request/Response LoadSheddingResponseCodeData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
congestionResponseResultCode	integer	M	Provide a numerical value in the range of 1001-5999.
congestionResponseVendorId	integer	O	Provide a numerical value in the range of 0-4294967295

Table 2-26 Request/Response MessagePriorityProfileData

Field Name	Field Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
profileName	string	M	This message priority profile will configure as default profile for message priority profile, and this will be the common profile for both overload and congestion control feature **Value**: Provide previous version profile name.

Sample for GET Congestion migration details:

```
{
  "migrated": true,
  "attempts": 0,
  "cause": "string"
}
```

Sample for add (POST) migration details from previous version configuration data to current version:

```
{
  "enable": true,
  "thresholdsProfileData": {
    "profileName": "string",
    "queueData": [
      {
        "state": "string",
        "value": 0
      }
    ],
    "cpuData": [
      {
        "state": "string",
        "value": 0
      }
    ]
  },
  "loadSheddingProfileData": {
    "profileName": "string",
    "ruleDiscardPriorityData": [
      {
        "state": "string",
        "value": 0
      }
    ],
```

```
    "ruleDiscardPriorityPercentageData": [
      {
        "state": "string",
        "discardPriorityPercentagesData": [
          {
            "range": "1 or 11-13",
            "percentage": 23
          }
        ]
      }
    ],
    "loadSheddingResponseCodeData": {
      "congestionResponseResultCode": 0,
      "congestionResponseVendorId": 0
    }
  },
  "messagePriorityProfileData": {
    "profileName": "string"
  }
}
```

2.4 General Configurations

This section provides information for configuring General Configurations in BSF.

Resource Name: General Configurations

Table 2-27 Supported REST APIs - General Configurations

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
General Configurations	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/general/export	GET	Export General Configuration	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-27 (Cont.) Supported REST APIs - General Configurations

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/general/import -d "{}"	POST	Import General Configuration	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/general	GET	Get Individual General Configuration	200: OK General configuration is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-27 (Cont.) Supported REST APIs - General Configurations

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/general -d " {} "	PUT	Update General Configuration	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Sample cURL Command for GET operation:

```
curl -X 'GET' \
  'http://10.148.210.26:8000/oc-bsf-configuration/v1/general' \
  -H 'accept: application/json'
```

GET and PUT - Get and Update General Configuration

Table 2-28 Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
enableTracing	Boolean	M	Specifies whether to enable tracing. Possible values are: • True (Default) • False
enableMetrics	Boolean	M	Specifies whether to enable system metrics. Possible values are: • True (Default) • False

Table 2-28 (Cont.) Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
enableCollisionDetection	Boolean	M	Specifies whether to enable collision detection for BSF. Possible values are: • True (Default) • False
bindingDiscoveryRequestTimeout	Integer	M	Specifies the request timeout value for the Authentication Request (AAR) message towards the BSF Diameter gateway.
enableSubscriberLog	Boolean	M	-
enableSBICorrelation	Boolean	M	-
enhancedLogging	Array	O	Used to configure the enhanced logging for BSF. For details on the parameters under in section, see Table 2-29.

Table 2-29 Request/Response Parameters for Enhanced Logging

Name	Data Type	Mandatory (M)/ Optional (O)	Description
enhancedLogging.enableEnhancedLogging	Boolean	O	Specifies whether to enable or disable enhanced logging for the BSF deployment. **Default value**: false

Table 2-29 (Cont.) Request/Response Parameters for Enhanced Logging

Name	Data Type	Mandatory (M)/ Optional (O)	Description
enhancedLogging.staleSessionDeletionLogLevel	String	O	Specifies the log level for stale session deletions. The available log levels for stale session deletions are: • TRACE • DEBUG • INFO • WARN • ERROR The logs for BSF stale binding deletion are generated at the specified level. **Note**: The value of this field does not modify in any way the log level that BSF Management service has. The root log level of BSF Management service must be either the same log level defined in the selected or lower for these deletion logs to appear. For example, if the stale session deletions log level is at INFO, then BSF Management service log level must be either TRACE, DEBUG, or INFO. **Default value**: INFO.
enhancedLogging.enableLogUEIdentifierInfo	Boolean	O	Specifies whether to enable or disable UE Identifier information for the BSF deployment. **Default value**: false
enhancedLogging.enableLogUeInfoInSessionDeletion	Boolean	O	Specifies whether to enable or disable UE Identifier information in stale session deletion logging. When this field is disabled, the UE Identifier information in the logs are masked. That is, the identifier information appears like 'xxxx'. **Default value**: false

Sample Request body structure for GET and PUT operations:

```
{
  "enableMetrics": true,
  "enableTracing": true,
  "bindingDiscoveryRequestTimeout": 0,
  "enableCollisionDetection": true,
  "enableSubscriberLog": true,
  "enableSBICorrelation": true,
  "enhancedLogging": {
    "enableEnhancedLogging": true,
    "staleSessionDeletionLogLevel": "string",
    "enableLogUEIdentifierInfo": true,
    "enableLogUeInfoInSessionDeletion": true,
  }
}
```

Sample Response body structure for GET and PUT operations:

```
{
  "enableMetrics": true,
  "enableTracing": true,
  "bindingDiscoveryRequestTimeout": 0,
  "enableCollisionDetection": true,
  "enableSubscriberLog": true,
  "enableSBICorrelation": true,
  "enhancedLogging": {
    "enableEnhancedLogging": true,
    "staleSessionDeletionLogLevel": "string",
    "enableLogUEIdentifierInfo": true,
    "enableLogUeInfoInSessionDeletion": true,
  }
}
```

Export and Import General Configurations

Sample cURL Command for Export Operation:

```
curl -X 'GET' \
  'http://10.148.210.26:8000/oc-bsf-configuration/v1/general/export' \
  -H 'accept: application/json'
```

Table 2-30 Data structures supported by Export and Import Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string	-	Current timestamp
exportData	array	-	Exported list of general configurations. For more information, see Table 2-28

Table 2-30 (Cont.) Data structures supported by Export and Import Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
sourceVersion	string	-	System version of the product from which data is exported
topic	string	-	Topic of each managed object

Sample Request Body structure for Import/Export operations:

```
{
  "topic": "string",
  "sourceVersion": "string",
  "date": "string",
  "exportData": {
    "enableMetrics": true,
    "enableTracing": true,
    "bindingDiscoveryRequestTimeout": 0,
    "enableCollisionDetection": true,
    "enableSubscriberLog": true,
    "enableSBICorrelation": true,
    "enhancedLogging": {
      "enableEnhancedLogging": true,
      "staleSessionDeletionLogLevel": "string",
      "enableLogUEIdentifierInfo": true,
      "enableLogUeInfoInSessionDeletion": true,
    }
  }
}
```

2.5 SBI Error Codes

Table 2-31 Supported REST APIs - SBI Error Codes

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Get SBI Error Codes	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/sbiErrorCodes/{conditionName}	200: OK SBI Error Codes is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-31 (Cont.) Supported REST APIs - SBI Error Codes

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Update SBI Error Codes	PUT	-H "accept: application/json" -H "Content-Type: application/json" -d " {} "{apiRoot}/oc-bsf-configuration/v1/sbiErrorCodes/{conditionName}	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Export SBI Error Codess	GET	-H "accept: application/json"{apiRoot}/oc-bsf-configuration/v1/sbiErrorCodes/export	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-31 (Cont.) Supported REST APIs - SBI Error Codes

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Import SBI Error Codess	POST	-H "accept: application/json"{apiRoot}/oc-bsf-configuration/v1/sbiErrorCodes/import	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Update SBI Error Codes

Table 2-32 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
applicationErrorCode	string	Mandatory	Specifies the application error code for a defined condition.
conditionName	string	Mandatory	Specifies the system defined name for a given condition.
errorDescription	string	Optional	Specifies the description for a defined condition. It is recommended to use descriptions that clearly explain the condition.
httpStatusCode	string	Mandatory	Specifies the HTTP Status code for a defined condition.

Sample Request body for SBI Error Codes PUT operation:

```
{
  "applicationErrorCode": "string",
  "conditionName": "string",
  "errorDescription": "string",
  "httpStatusCode": "string"
}
```

Sample Response body structure for SBI Error Codes GET and PUT operation:

```
{
  "applicationErrorCode": "string",
  "conditionName": "string",
  "errorDescription": "string",
  "httpStatusCode": "string"
}
```

Import and Export SBI Error Codes

Table 2-33 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string		Current timestamp
errors.message			Error message
errors.name			Name of the error
exportData	array		Exported list of SBI Error Codes. For more information, see Get and Update SBI Error Codes.
key	string		Indicates the ID
sourceVersion	string		System version of product from which data is exported
topic	string		Topic of each managed object

Sample Request Body structure for SBI Error Codes Import and Export operations:

```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
  "exportData": [
    {
      "applicationErrorCode": "string",
      "conditionName": "string",
      "errorDescription": "string",
      "httpStatusCode": "string"
    }
  ],
  "key": "string",
  "sourceVersion": "string",
  "topic": "string"
}
```

2.6 Management Service

This section provides information for configuring Management Service in BSF.

Resource Name: Management Service

The following table describes the APIs for Resource - Management Service:

Table 2-34 Supported REST APIs - Management Service

Tasks	Resource URI	HTTP Method or Custom Operation	Possible Result Code
Export Management Service	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/services/managementservice/export	GET	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Import Management Service	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/services/managementservice/import	POST	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get Management Service	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/services/managementservice	GET	200: OK Management Service is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-34 (Cont.) Supported REST APIs - Management Service

Tasks	Resource URI	HTTP Method or Custom Operation	Possible Result Code
Update Management Service	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/services/managementservice	PUT	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Sample Request to Update Management Service

Parameters
The following table describes the parameters:

Table 2-35 Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
apiRoot	String	O	Indicates the URL for server root.
logLevels	BSFSystemConfigurationLogLevels	O	Indicates the different log levels and log name.
audit	BsfAuditConfiguration	O	
bsfNfBindingsSettings	BSFNFBindingsSettings	O	
bsfNfServerSettings	BSFNFServerSettings	O	
activeSessionCounting	BSFActiveSessionCounting	O	
nfCorrelationSettings	NfCorrelationSettings	O	
advancedSettings	AdvancedSettings	M	

Table 2-35 (Cont.) Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
enableBindingRevalidation	boolean	O	When this field is enabled, BSF checks if the binding information for the PDU session is present in BSF. Existence of the binding association for the PDU session in BSF confirms the binding association being valid in BSF. If the binding association is missing in BSF, it is restored by creating the association in BSF. **Default value**: false
rootLogLevel	string	M	Specifies the status of root log level. Possible values are: • TRACE • DEBUG • INFORMATION • WARN (Default) • ERROR • ALWAYS
activeSessionCounting.countRecords	Boolean	O	Enables or disables the active sessions counting. By default, the active sessions counting is disabled. To enable the feature, set the value of this parameter to `true` .
activeSessionCounting.countRecordsInterval	Integer	O	Specifies the time interval (in minutes) for which maximum active sessions are reported as a metric. Default value is 15 minutes. You can set the time interval to any value between 1 to 60 minutes.
audit.enable	Boolean	O	Indicates whether to enable or disable auditing of stale records.

Table 2-35 (Cont.) Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
audit.frequency	Integer	M	Indicates the time when next audit for the BSF management service table will begin after delta time if auditing this table has been finished before the specified minimum audit passes interval.
audit.ansWithResultCodeCfg	Array	O	Indicates the value that is compared with the result code received in the AAA-I answer. If both the values match, a request is sent towards the BSF Management service to initiate stale record notification. For more information, see Table 2-38.
audit.maxTtl	Integer	M	Specifies the maximum binding age for binding records. Once the binding age for a record exceeds the configured value, audit service marks the record as stale and BSF removes the record from its local database. The recommended value is 7200.
audit.notificationRate	Integer	M	Specifies the number of notifications that Audit service sends to the BSF Management service in one second. The recommended value is 50. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)

Table 2-35 (Cont.) Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
audit.queryToPcf	Boolean	O	Indicates whether BSF management service queries PCF to confirm the status of a PcfBinding record, which is suspected as stale by the audit service. **Default value**: false **Note**: When Query to PCF parameter is set to false, the value of "Minimum Audit Attempts" parameter in Service Configurations of Management Service, and "Forced Deletion - Minimum Audit Attempts" parameter in Service configurations of Audit Service should be set to 0.
audit.ttl	Integer	M	Specifies the binding age for binding records. Once the binding age for a record exceeds the configured value, audit service marks the record as suspected stale. The recommended value is 3600.
audit.vendorId	string Example: 000111	O	Specifies the vendor ID that BSF retrieves from the Vendor Specific Attribute to send query requests towards PCF. The vendor ID should be 6-digit long. **Note**: PCF sends the Vendor Specific Attribute in the request body at the time of binding registration.
bsfNfBindingsSettings.bsfBindingLevel	String	O	Indicates the binding level to be included in the 3gpp-sbi-binding header when BSF adds this header in a message to another NF.
bsfNfBindingsSettings.bsfSendBindingHeader	Boolean	O	Indicates if BSF includes the 3gpp-sbi-binding header in SBI messages.

Table 2-35 (Cont.) Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
bsfNfServerSettings.bsfSendServerHeader	Boolean	O	Indicates if BSF management service includes server header while sending an error response.
bsfNfServerSettings.bsfServerHeaderErrorCodes	integer	O	Indicates the error codes for which service header is generated. The error codes can be from 100 to 999.
logLevels:loggerName	String	O	Specifies the name of the logger. For Example, trace
nfCorrelationSettings.sendCorrelationHeader	Boolean	O	
nfCorrelationSettings.allowedCorrelationInfoIdType	array	M	• IMSI

Table 2-36 BSFSystemConfigurationLogLevels

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
level	String:Enum	O	Possible values are: • TRACE (Default) • DEBUG • INFORMATION • WARN • ERROR • ALWAYS
loggername	String	O	Specifies the name of the logger. For Example, trace

Table 2-37 BsfAuditConfiguration

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enable	boolean	O	Possible values are:
enter a range in sec from [20-700]	String	M	Specifies the name of the logger. For Example, trace
enter a range in minutes from [1-10080]	integer	M	
minAuditAttempts	integer	M	

Table 2-37 (Cont.) BsfAuditConfiguration

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enter a range in minutes from [1-1440]	integer	M	
ansWithResultCodeCfg	AnsWithResultCode	O	
queryToPcf	boolean	O	
enter a 6 digit Vendor ID	string	O	

Table 2-38 ansWithResultCodeCfg

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
ansWithResultCode	String:Enum	O	Specifies the result code. Possible values: • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE
resultCode	Integer	O	Specifies the custom result code when `ansWithResultCode` is `EXPERIMENTAL_RESULT_CODE`.
vendorId	Integer	O	Specifies the custom vendor ID when `ansWithResultCode` is `EXPERIMENTAL_RESULT_CODE`.

Sample cURL command for Update Management Service

```
curl -X PUT "http://10.75.206.200:8000/oc-bsf-configuration/v1/services/
managementservice" -H "accept: application/json" -H "Content-Type:
application/json" -d "{ \"activeSessionCounting\": { \"countRecords\": true,
\"countRecordsInterval\": 15 }, \"apiRoot\": \"string\", \"audit\":
{ \"ansWithResultCodeCfg\": [ { \"ansWithResultCode\":
\"DIAMETER_UNABLE_TO_COMPLY\", \"resultCode\": 0, \"vendorId\": 0 } ],
\"enable\": true, \"frequency\": 330, \"maxTtl\": 7200, \"notificationRate\":
50, \"queryToPcf\": true, \"ttl\": 1440, \"vendorId\": \"000111\" },
\"bsfNfBindingsSettings\": { \"bsfBindingLevel\": \"NF_SET\",
\"bsfSendBindingHeader\": true }, \"bsfNfServerSettings\":
{ \"bsfSendServerHeader\": true, \"bsfServerHeaderErrorCodes\": [ 0 ] },
\"logLevels\": [ { \"level\": \"ALWAYS\", \"loggerName\": \"string\" } ],
\"rootLogLevel\": \"ALWAYS\"}"
```

Sample Response for Update Management Service

The following is the schema for adding/updating Management Service:


```
{
  "apiRoot": "string",
  "logLevels": [
    {
      "level": "TRACE",
      "loggerName": "string"
    }
  ],
  "audit": {
    "enable": true,
    "enter a range in sec from [20-700]": 50,
    "enter a range in minutes from [1-10080]": 7200,
    "minAuditAttempts": 5,
    "enter a range in minutes from [1-1440]": 330,
    "ansWithResultCodeCfg": [
      {
        "ansWithResultCode": "DIAMETER_UNABLE_TO_COMPLY",
        "resultCode": 9999,
        "vendorId": 4294967295
      }
    ],
    "queryToPcf": true,
    "enter a 6 digit Vendor ID": "000111"
  },
  "bsfNfBindingsSettings": {
    "bsfBindingLevel": "NF_SET",
    "bsfSendBindingHeader": true
  },
  "bsfNfServerSettings": {
    "bsfSendServerHeader": true,
    "bsfServerHeaderErrorCodes": [
      0
    ]
  },
  "activeSessionCounting": {
    "countRecords": true,
    "enter a range in sec from [1-60]": 15
  },
  "nfCorrelationSettings": {
    "sendCorrelationHeader": true,
    "allowedCorrelationInfoIdType": [
      "imsi"
    ]
  },
  "advancedSettings": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "enableBindingRevalidation": true,
```

```
  "rootLogLevel": "TRACE"
}
```

Export and Import Management Service

Table 2-39 Data structures supported by Export and Import Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)	Description
date	string	Optional	Current timestamp
exportData	array	Mandatory	Exported list of Management Service. For more information, see Table 2-35
sourceVersion	string	Optional	System version of the product from which data is exported
topic	string	Mandatory	Topic of each managed object

Sample Request Body structure for Import operation:

```
{
  "date": "string",
  "exportData": {
    "apiRoot": "string",
    "audit": {
      "ansWithResultCodeCfg": [
        {
          "ansWithResultCode": "DIAMETER_UNABLE_TO_COMPLY",
          "resultCode": 0,
          "vendorId": 0
        }
      ],
      "enable": true,
      "frequency": 330,
      "maxTtl": 7200,
      "notificationRate": 50,
      "queryToPcf": true,
      "ttl": 1440,
      "vendorId": "000111"
    },
    "bsfNfBindingsSettings": {
      "bsfBindingLevel": "NF_SET",
      "bsfSendBindingHeader": true
    },
    "bsfNfServerSettings": {
      "bsfSendServerHeader": true,
      "bsfServerHeaderErrorCodes": [
        0
      ]
    },
    "nfCorrelationSettings": {
    "sendCorrelationHeader": true,
    "allowedCorrelationInfoIdType": [
```

```
      "imsi"
    ]
    },
    "logLevels": [
      {
        "level": "ALWAYS",
        "loggerName": "string"
      }
    ],
    "rootLogLevel": "ALWAYS"
    "enableBindingRevalidation": true
  },
  "sourceVersion": "string",
  "topic": "string"
}
```

2.7 Diameter Settings

This section provides information for configuring diameter gateway in BSF.

Diameter Settings

Table 2-40 Supported REST APIs - Diameter Settings

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
Diameter Settings	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/settings/export	GET	Export Diameter Settings	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-40 (Cont.) Supported REST APIs - Diameter Settings

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
Diameter Settings	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/settings/import -d "{}"	POST	Import Diameter Settings	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Diameter Settings	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/settings	GET	Get Diameter Settings	200: OK Diameter Settings are returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-40 (Cont.) Supported REST APIs - Diameter Settings

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
Diameter Settings	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot} /oc-bsf-configuration/v1/diameter/settings -d " {} "	PUT	Update Diameter Settings	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Update Diameter Settings

Table 2-41 Data structures supported by GET and PUT response body

Name	Data Type	Mandatory (M)/ Optional (O)	Description
timer:connectionTimeout	Number	O	Specifies the connection timeout interval in seconds. The default is 3 seconds.
timer:reconnectDelay	Number	O	Specifies the time frame to delay before attempting to reconnect after a connection failure in seconds. The default is 3 seconds.
timer:responseTimeout	Number	O	Specifies the response timeout interval in seconds. The default is 5 seconds.
timer:watchdog interval	Number	O	Specifies the watchdog interval in seconds. The default is 6 seconds.
transport:protocol	String	O	TCP/SCTP

Table 2-42 congestionControl

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
congestionLoadSheddingProfile	string	O	Specifies the load shedding profile name.
congestionMessagePriorityProfile	string	O	Specifies the message priority profile name.

Table 2-43 DiamSettingsOverloadControl

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
overloadLoadSheddingProfile	string	O	Specifies the load shedding profile name for overload control.
overloadMessagePriorityProfile	string	O	Specifies the message priority profile name for overload control.

Table 2-44 Enhanced Timer Configuration

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
appId	Integer	M	Specifies the application name.
appResponseTimeoutValue	Integer	M	Specifies the application response timeout in milliseconds.
cmdCodeResponseTimeoutValueMap	Map <Integer, Integer>	O	Specifies the command code response timeout for the AAR, RAR, STR, and ASR message types in milliseconds.

Sample Request body structure for PUT operations:

```
{
  "advancedSettings": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "congestionControl": {
    "congestionLoadSheddingProfile": "string",
    "congestionMessagePriorityProfile": "string"
  },
  "messageTimers": [
    {
```

```
      "appId": 0,
      "appResponseTimeoutValue": 0,
      "cmdCodeResponseTimeoutValueMap": {
        "258": 0,
        "265": 0,
        "274": 0,
        "275": 0
      }
    }
  ],
  "overloadControl": {
    "overloadLoadSheddingProfile": "string",
    "overloadMessagePriorityProfile": "string"
  },
  "timer": {
    "connectionTimeout": 3,
    "reconnectDelay": 3,
    "responseTimeout": 5,
    "watchdogInterval": 6
  },
  "topologyhiding": {
    "AppsToHide": [
      "All"
    ],
    "EnableTopologyHiding": true
  },
  "transport": {
    "protocol": "SCTP"
  }
}
```

Sample Response body structure for GET and PUT operations:

```
{
  "advancedSettings": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "congestionControl": {
    "congestionLoadSheddingProfile": "string",
    "congestionMessagePriorityProfile": "string"
  },
  "messageTimers": [
    {
      "appId": 0,
      "appResponseTimeoutValue": 0,
      "cmdCodeResponseTimeoutValueMap": {
        "258": 0,
        "265": 0,
        "274": 0,
        "275": 0
      }
    }
```

```
  ],
  "overloadControl": {
    "overloadLoadSheddingProfile": "string",
    "overloadMessagePriorityProfile": "string"
  },
  "timer": {
    "connectionTimeout": 3,
    "reconnectDelay": 3,
    "responseTimeout": 5,
    "watchdogInterval": 6
  },
  "topologyhiding": {
    "AppsToHide": [
      "All"
    ],
    "EnableTopologyHiding": true
  },
  "transport": {
    "protocol": "SCTP"
  }
}
```

Export and Import Diameter Settings

Table 2-45 Data structures supported by Export and Import Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string	-	Current timestamp
exportData	array	-	Exported list of Diameter Settings. For more information, see Table 2-41
sourceVersion	string	-	System version of the product from which data is exported
topic	string	-	Topic of each managed object

Sample Request Body structure for Import/Export operations:

```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
  "exportData": {
    "advancedSettings": [
      {
        "key": "string",
        "value": "string"
```

```
      }
    ],
    "congestionControl": {
      "congestionLoadSheddingProfile": "string",
      "congestionMessagePriorityProfile": "string"
    },
    "messageTimers": [
      {
        "appId": 0,
        "appResponseTimeoutValue": 0,
        "cmdCodeResponseTimeoutValueMap": {
          "258": 0,
          "265": 0,
          "274": 0,
          "275": 0
        }
      }
    ],
    "overloadControl": {
      "overloadLoadSheddingProfile": "string",
      "overloadMessagePriorityProfile": "string"
    },
    "timer": {
      "connectionTimeout": 3,
      "reconnectDelay": 3,
      "responseTimeout": 5,
      "watchdogInterval": 6
    },
    "topologyhiding": {
      "AppsToHide": [
        "All"
      ],
      "EnableTopologyHiding": true
    },
    "transport": {
      "protocol": "SCTP"
    }
  },
  "sourceVersion": "string",
  "topic": "string"
}
```

2.8 Diameter Routing Table

Table 2-46 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Export Diameter Routing Table	GET	{apiRoot}/oc-bsf-configuration/v1/diameter/routingTable/export	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Import Diameter Routing Table	POST	{apiRoot}/oc-bsf-configuration/v1/diameter/routingTable/import	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get Diameter Routing Table	GET	{apiRoot}/oc-bsf-configuration/v1/diameter/routingTable	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-46 (Cont.) Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Update Diameter Routing Table	PUT	{apiRoot}/oc-bsf-configuration/v1/diameter/routingTable	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Update Operations

Table 2-47 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
defaultRoute	string	M	Provide the default route.
routeTable	string	M	The route table information.

Table 2-48 defaultRoute

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
serverID	string	O	The serverID details.

Table 2-49 routeTable

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
appIDs	integer	M	
hosts	string	M	
name	string	O	
priority	string	O	
realms	string	O	
type	Realm	O	

Sample Request body structure for PUT operations:

```
"defaultRoute": {
    "serverId": "string"
  },
  "routeTable": [
    {
      "appIds": [
        "All"
      ],
      "hosts": [
        "string"
      ],
      "name": "string",
      "priority": "string",
      "realms": [
        "string"
      ],
      "serverIds": [
        "string"
      ],
      "type": "Host"
    }
  ]
}
```

Sample Response body structure for GET and PUT operations:

```
{
  "defaultRoute": {
    "serverId": "string"
  },
  "routeTable": [
    {
      "appIds": [
        "All"
      ],
      "hosts": [
        "string"
      ],
      "name": "string",
      "priority": "string",
      "realms": [
        "string"
      ],
      "serverIds": [
        "string"
      ],
      "type": "Host"
    }
  ]
}
```

Export/Import Diameter Routing Table

Table 2-50 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string		Current timestamp
exportData	array		Exported list of diamteter routing table.
sourceVersion	string		System version of product from which data is exported
topic	string		Topic of each managed object

Sample Request Body structure for Import/Export operations:

```
{
  "date": "string",
  "exportData": {
    "defaultRoute": {
      "serverId": "string"
    },
    "routeTable": [
      {
        "appIds": [
          "All"
        ],
        "hosts": [
          "string"
        ],
        "name": "string",
        "priority": "string",
        "realms": [
          "string"
        ],
        "serverIds": [
          "string"
        ],
        "type": "Host"
      }
    ]
  },
  "sourceVersion": "string",
  "topic": "string"
}
```

2.9 Load Shedding Profile

Table 2-51 Supported REST APIs - Load Shedding Profile

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Create Load Shedding Profile	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get Load Shedding Profile	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles/{loadsheddingName}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Update Load Shedding Profile	PUT	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles/{loadsheddingName}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-51 (Cont.) Supported REST APIs - Load Shedding Profile

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Export Load Shedding Profiles	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles/export	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Import Load Shedding Profiles	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles/import	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Delete Load Shedding Profile	DELETE	-H "accept: */*" {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles/{loadsheddingName}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too many Requests 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Create and Update Load Shedding Profile

Table 2-52 PUT and POST Request Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
loadSheddingRules	CongestionLoadSheddingRules	Optional	Specifies the list of configured Congestion Load Shedding Rules.
name	string	Mandatory	Specifies the unqiue name of the load shedding profile.
overloadLoadSheddingRules	OverloadLoadSheddingRules	Optional	Specifies the list of configured Overload Load Shedding Rules.
type	Enum The supported values are: • Overload Control • congestion	Optional	Specifies the type of load shedding profile. The load shedding profile can be one of the following types: • Congestion Control • Overload Control

Table 2-53 CongestionLoadSheddingRules

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
ansWithResultCode	Enum The supported values are: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE	Optional	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control.
discardPriority	integer	Mandatory	Specifies the discard priority for the congestion load shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or lower priority is rejected.

Table 2-53 (Cont.) CongestionLoadSheddingRules

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
resultCode	integer	Conditional	**Note**: Specify a value for this parameter when you choose `EXPERIMENTAL_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the custom result code, which is returned in the answer response when service request is rejected due to congestion control. .
state	Enum The supported values are: • CONGESTED • DANGER_OF_CONGESTION	Optional	Specifies the type of state for which you are defining the rule.
vendorId	integer	Conditional	**Note**: Specify a value for this parameter when you choose `EXPERIMENTAL_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the vendor ID, which is returned in the answer response when service request is rejected due to congestion control. .

Table 2-54 OverloadLoadSheddingRules

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
ansWithResultCode	Enum The supported values are: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE	Optional	Specifies the result code, returned in the answer response, when request message is rejected as part of overload control.

Table 2-54 (Cont.) OverloadLoadSheddingRules

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
discardPriority	integer	Mandatory	Specifies the discard priority for the overload shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or lower priority is rejected.
level	Enum The supported values are: • L1 • L2 • L3 • L4	Mandatory	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies.
resultCode	integer	Conditional	**Note**: Specify a value for this parameter when you choose `EXPERIMENTAL_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the custom result code, which is returned in the answer response when service request is rejected due to overload control. .
vendorId	integer	Conditional	**Note**: Specify a value for this parameter when you choose `EXPERIMENTAL_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the vendor ID, which is returned in the answer response when service request is rejected due to overload control. .

Sample Request body for Load Shedding Profile (PUT and POST operations):

```
{
  "loadSheddingRules": [
    {
      "ansWithResultCode": "DIAMETER_TOO_BUSY",
      "discardPriority": 0,
      "resultCode": 0,
      "state": "CONGESTED",
      "vendorId": 0
    }
  ],
  "name": "string",
  "overloadLoadSheddingRules": [
    {
      "ansWithResultCode": "DIAMETER_TOO_BUSY",
```

```
      "discardPriority": 0,
      "level": "L1",
      "resultCode": 0,
      "vendorId": 0
    }
  ],
  "type": "DIAMETER_TOO_BUSY"
}
```

Sample Response body structure for GET, PUT, and POST operation:

```
{
  "loadSheddingRules": [
    {
      "ansWithResultCode": "DIAMETER_TOO_BUSY",
      "discardPriority": 0,
      "resultCode": 0,
      "state": "CONGESTED",
      "vendorId": 0
    }
  ],
  "name": "string",
  "overloadLoadSheddingRules": [
    {
      "ansWithResultCode": "DIAMETER_TOO_BUSY",
      "discardPriority": 0,
      "level": "L1",
      "resultCode": 0,
      "vendorId": 0
    }
  ],
  "type": "DIAMETER_TOO_BUSY"
}
```

Import and Export Load Shedding Profile

Table 2-55 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string	M	Current timestamp
exportData	array	M	Exported list of Load Shedding Profile. For more information, see Create and Update Load Shedding Profile.
key	string	M	Indicates the ID
sourceVersion	string	M	System version of product from which data is exported
topic	string	M	Topic of each managed object

Sample Request Body structure for Load Shedding Profile Import and Export operations:


```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
  "exportData": [
    {
      "loadSheddingRules": [
        {
          "ansWithResultCode": "DIAMETER_TOO_BUSY",
          "discardPriority": 0,
          "resultCode": 0,
          "state": "CONGESTED",
          "vendorId": 0
        }
      ],
      "name": "string",
      "overloadLoadSheddingRules": [
        {
          "ansWithResultCode": "DIAMETER_TOO_BUSY",
          "discardPriority": 0,
          "level": "L1",
          "resultCode": 0,
          "vendorId": 0
        }
      ],
      "type": "DIAMETER_TOO_BUSY"
    }
  ],
  "key": "string",
  "sourceVersion": "string",
  "topic": "string"
}
```

2.10 Congestion Threshold

Table 2-56 Supported REST APIs - Congestion Threshold

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Get Congestion Threshold	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/threshold/{serviceType}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 429: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Update Congestion Threshold	PUT	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/threshold/{serviceType}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Export Congestion Thresholds	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/threshold/export/{serviceType}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-56 (Cont.) Supported REST APIs - Congestion Threshold

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Import Congestion Thresholds	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/threshold/import/{serviceType}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Update Congestion Threshold

Table 2-57 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
stateCalculationInterval	integer	Mandatory	Specifies the interval at which congestion state is calculated.
stateChangeSampleCount	integer	Mandatory	Specifies the continuous sample counts for which calculated state remains the same.
thresholds[]	array		An array to define threshold values for each resource for a given state,
thresholds[].state	string		Specifies the congestion state.
thresholds[].resourceUsageLimit			Specifies the resource usage limit for a defined state.
thresholds[].resourceUsageLimit.cpu	integer		Specifies the threshold value for CPU message.
thresholds[].resourceUsageLimit.memory	integer		Specifies the threshold value for memory message.
thresholds[].resourceUsageLimit.queue	integer		Specifies the threshold value for number of messages in the queue.

Sample Request body for Congestion Threshold PUT operation:

```
    {
"stateCalculationInterval": 100,
"stateChangeSampleCount": 10,
"thresholds": [
```

```
    {
      "state": "CONGESTED",
      "resourceUsageLimit": {
        "cpu": 80,
        "memory": 80,
        "queue": 50
      }
    },
    {
      "state": "DANGER_OF_CONGESTION",
      "resourceUsageLimit": {
        "cpu": 60,
        "memory": 60,
        "queue": 30
      }
    }
  ]
}
```

Sample Response body structure for Congestion Threshold GET and PUT operation:

```
{
  "stateCalculationInterval": 100,
  "stateChangeSampleCount": 10,
  "thresholds": [
    {
      "state": "CONGESTED",
      "resourceUsageLimit": {
        "cpu": 80,
        "memory": 80,
        "queue": 50
      }
    },
    {
      "state": "DANGER_OF_CONGESTION",
      "resourceUsageLimit": {
        "cpu": 60,
        "memory": 60,
        "queue": 30
      }
    }
  ]
}
```

Import and Export Congestion Threshold

Table 2-58 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string		Current timestamp

Table 2-58 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
exportData	array		Exported list of Congestion Threshold. For more information, see Get and Update Congestion Threshold.
key	string		Indicates the ID
sourceVersion	string		System version of product from which data is exported
topic	string		Topic of each managed object

Sample Request Body structure for Congestion Threshold Import and Export operations:

```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
  "exportData": {
    "stateCalculationInterval": 100,
    "stateChangeSampleCount": 10,
    "thresholds": [
      {
        "state": "CONGESTED",
        "resourceUsageLimit": {
          "cpu": 80,
          "memory": 80,
          "queue": 50
        }
      },
      {
        "state": "DANGER_OF_CONGESTION",
        "resourceUsageLimit": {
          "cpu": 60,
          "memory": 60,
          "queue": 30
        }
      }
    ]
  },
  "sourceVersion": "string",
  "topic": "string"
}
```

2.11 Peer Node

This section provides information for configuring Peer Node in BSF.

Resource Name: Peer Node

Table 2-59 Supported REST APIs - Peer Node

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
Peer Node	-H "accept: application/json" -H "Content-Type: application/json" /oc-bsf-configuration/v1/diameter/peernodes	POST	Create Peer Node	200: OK 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
	-H "accept: application/json" /oc-bsf-configuration/v1/diameter/peernodes/export	GET	Get All (Export) Peer Nodes	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-59 (Cont.) Supported REST APIs - Peer Node

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
	-H "accept: application/json" -H "Content-Type: application/json" /oc-bsf-configuration/v1/diameter/peernodes/import	POST	Import Peer Nodes	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
	-H "accept: application/json" /oc-bsf-configuration/v1/diameter/peernodes/{peernodeName}	GET	Get Peer Node	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-59 (Cont.) Supported REST APIs - Peer Node

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
	-H "accept: application/json" -H "Content-Type: application/json" /oc-bsf-configuration/v1/diameter/peernodes/{peernodeName}	PUT	Update Peer Node	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
	-H "accept: */*" /oc-bsf-configuration/v1/diameter/peernodes/{peernodeName}	DELETE	Delete Peer Node	200: OK 204: Peer Node was succesfully deleted 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

GET and PUT - Get, Create, and Update Peer Node

Table 2-60 Data structures supported by the GET and PUT Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
diamName	String	O	Unique Name of the Peer Node

Table 2-60 (Cont.) Data structures supported by the GET and PUT Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
dtype	String	O	Defines which type of Diameter Service it should take up. The value can be Application function (af), backend, diameter routing agent(dra), ocs, tdf, or udr.
host	String	O	The host name. Enter a FQDN, ipv4 or ipv6 address available for establishing diameter transport connections to the peer node.
identity	String	O	An identity to define a node in a realm.
initiateConnection	boolean	O	Set it to True to initiate a connection for this peer node. **Default Value**: FALSE
port	Number	O	The port number. Enter a number from 0 to 65535.
realm	String	O	The realm name, that is, FQDNs to all of that computers that transact diameter traffic.
reconnectLimit	Number		

Sample Request body structure for PUT operations:

```
{
  "diamName": "string",
  "dtype": "af",
  "host": "string",
  "identity": "string",
  "initiateConnection": true,
  "port": "3868",
  "realm": "string",
  "reconnectLimit": "3"
}
```

Sample Response body structure for GET and PUT operations:

```
{
  "diamName": "string",
  "dtype": "af",
  "host": "string",
  "identity": "string",
  "initiateConnection": true,
  "port": "3868",
  "realm": "string",
  "reconnectLimit": "3"
}
```

DELETE - delete peer node

Table 2-61 Data structures supported by the DELETE Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
Peer Node Name	string	M	Peer Node Name

Get All (Export) and Import Peer Node

Table 2-62 Data structures supported by Export and Import Response Body

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string		Current timestamp
exportData	array		Exported list of peer nodes.
key	string		Indicates the ID
sourceVersion	string		System version of product from which data is exported
topic	string		Topic of each managed object

Sample Request Body structure for Import/Export operations:

```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
  "exportData": [
    {
      "diamName": "string",
      "dtype": "af",
      "host": "string",
      "identity": "string",
      "initiateConnection": true,
      "port": "3868",
      "realm": "string",
      "reconnectLimit": "3"
    }
  ],
  "key": "string",
  "sourceVersion": "string",
  "topic": "string"
}
```

2.12 Message Priority Profile

Table 2-63 Supported REST APIs - Message Priority Profile

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Create Message Priority Profile	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get Message Priority Profile	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files/{messagepriorityName}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Update Message Priority Profile	PUT	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files/{messagepriorityName}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-63 (Cont.) Supported REST APIs - Message Priority Profile

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Export Message Priority Profiles	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files/export	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Import Message Priority Profiles	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files/import	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Delete Message Priority Profile	DELETE	-H "accept: */*" {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files/{messageprioritypro fileName}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too many Requests 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Create and Update Message Priority Profile

Table 2-64 PUT and POST Request Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	Mandatory	Unique name of the message priority profile.
priorityRules []	array	Optional	Specifies configured message priority rules.
priorityRules []conditions	conditions	Optional	Specifies the conditions for message priority rule.
priorityRules []conditions.application	string	Mandatory	Specifies the type of application.
priorityRules []conditions.message	string	Mandatory	Specifies the type of message for the selected application.
priorityRules []conditions.preDefinedAVPConditions	array	Optional	Specifies the pre-defined AVP conditons.
enableDRMPPriority	boolean	Optional	When this switch is enabled, the priority for the message rule is assigned from DRMP AVP.
messagePriority	integer	Mandatory	Specifies the priority assigned to the message. It can be a number from 0 to 15.
ruleName	string	Mandatory	Specifies the unique name of the message priority rule.
rulePriority	integer	Mandatory	Specifies the priority assigned to the message priority rule.

Sample Request body for PUT and POST operations:

```
{
  "name": "string",
  "priorityRules": [
    {
      "conditions": {
        "application": "Gx",
        "message": "CCR",
        "preDefinedAVPConditions": [
          {
            "conditionCCRTValue": "UPDATE_REQUEST",
            "conditionCSIDValue": [
              "string"
            ],
            "conditionMCPTTIdValue": [
              "string"
            ],
            "conditionMCVideoIdValue": [
              "string"
            ],
            "conditionMPSIdValue": [
```

```
              "string"
            ],
            "conditionName": "CC-Request-Type",
            "conditionReservPriorityValue": [
              "string"
            ],
            "conditionRxRTValue": [
              "INITIAL_REQUEST"
            ],
            "conditionSNRTypeValue": [
              "ABORT_SESSION_REQUEST"
            ],
            "conditionServiceURNIDValue": [
              "string"
            ]
          }
        ]
      },
      "enableDRMPPriority": true,
      "messagePriority": 8,
      "ruleName": "string",
      "rulePriority": 3
    }
  ]
}
```

Sample Response body structure for GET, PUT, and POST operations:

```
{
  "name": "string",
  "priorityRules": [
    {
      "conditions": {
        "application": "Gx",
        "message": "CCR",
        "preDefinedAVPConditions": [
          {
            "conditionCCRTValue": "UPDATE_REQUEST",
            "conditionCSIDValue": [
              "string"
            ],
            "conditionMCPTTIdValue": [
              "string"
            ],
            "conditionMCVideoIdValue": [
              "string"
            ],
            "conditionMPSIdValue": [
              "string"
            ],
            "conditionName": "CC-Request-Type",
            "conditionReservPriorityValue": [
              "string"
            ],
            "conditionRxRTValue": [
```

```
            "INITIAL_REQUEST"
          ],
          "conditionSNRTypeValue": [
            "ABORT_SESSION_REQUEST"
          ],
          "conditionServiceURNIDValue": [
            "string"
          ]
        }
      ]
    },
    "enableDRMPPriority": true,
    "messagePriority": 8,
    "ruleName": "string",
    "rulePriority": 3
  }
 ]
}
```

Import and Export Message Priority Profile

Table 2-65 Request and Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string		Current timestamp
exportData	array		Exported list of Message Priority Profile. For more information, see Create and Update Message Priority Profile.
key	string		Indicates the ID
sourceVersion	string		System version of product from which data is exported
topic	string		Topic of each managed object

Sample Request Body structure for Message Priority Profile Import operation:

```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
  "exportData": [
    {
      "name": "string",
      "priorityRules": [
        {
          "conditions": {
```

```
                "application": "Gx",
                "message": "CCR",
                "preDefinedAVPConditions": [
                  {
                    "conditionCCRTValue": "UPDATE_REQUEST",
                    "conditionCSIDValue": [
                      "string"
                    ],
                    "conditionMCPTTIdValue": [
                      "string"
                    ],
                    "conditionMCVideoIdValue": [
                      "string"
                    ],
                    "conditionMPSIdValue": [
                      "string"
                    ],
                    "conditionName": "CC-Request-Type",
                    "conditionReservPriorityValue": [
                      "string"
                    ],
                    "conditionRxRTValue": [
                      "INITIAL_REQUEST"
                    ],
                    "conditionSNRTypeValue": [
                      "ABORT_SESSION_REQUEST"
                    ],
                    "conditionServiceURNIDValue": [
                      "string"
                    ]
                  }
                ]
              },
              "enableDRMPPriority": true,
              "messagePriority": 8,
              "ruleName": "string",
              "rulePriority": 3
            }
          ]
        }
      ],
      "key": "string",
      "sourceVersion": "string",
      "topic": "string"
    }
```

2.13 Diameter Error Codes

Table 2-66 Supported REST APIs - Diameter Error Codes

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Get Diameter Error Codes	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/diameterErrorCodes/{conditionName}	200: OK SBI Error Codes is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable
Update Diameter Error Codes	PUT	{apiRoot}/oc-bsf-configuration/v1/diameter/diameterErrorCodes/{conditionName}	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Export Diameter Error Codes	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/diameterErrorCodes/export	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-66 (Cont.) Supported REST APIs - Diameter Error Codes

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Import Diameter Error Codes	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/diameter/diameterErrorCodes/import -d " {} "	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Update Diameter Error Codes

Table 2-67 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
conditionName	string	Mandatory	Specifies the system defined name for a given condition.
diameterResultCode	string	Conditional	Specifies the Diameter result code for a defined condition.
errorMessage	string	Optional	Specifies the description for a defined condition. It is recommended to use descriptions that clearly explain the condition.
experimentalResultCode	string	Conditional	Specifies the custom Diameter result code for a defined condition.
useExperimentalResultCode	boolean	Optional	Indicates whether to use the Result Code AVP (268) or Experimental Result AVP (297) when an error result is generated by BSF.
vendorId	string	Conditional	Specifies the Vendor ID of the operator or governing body that manages the code entered by the user in the `experimentalResultCode` field.

Sample Request body for Diameter Error Codes PUT operation:

```
{
  "conditionName": "string",
  "diameterResultCode": "string",
  "errorMessage": "string",
  "experimentalResultCode": "string",
  "useExperimentalResultCode": true,
  "vendorId": "string"
}
```

Sample Response body structure for Diameter Error Codes GET and PUT operation:

```
{
  "conditionName": "string",
  "diameterResultCode": "string",
  "errorMessage": "string",
  "experimentalResultCode": "string",
  "useExperimentalResultCode": true,
  "vendorId": "string"
}
```

Import and Export Diameter Error Codes

Table 2-68 Request or Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
date	string	Optional	Current timestamp
errors.message	string	Optional	Error message
errors.name	string	Optional	Name of the error
exportData	array	Mandatory	Exported list of SBI Error Codes. For more information, see Table 2-67.
key	string	Optional	Indicates the ID
sourceVersion	string	Optional	System version of product from which data is exported
topic	string	Mandatory	Topic of each managed object

Sample Request Body structure for Diameter Error Codes Import and Export operations:

```
{
  "date": "string",
  "errors": [
    {
      "message": "string",
      "name": "string"
    }
  ],
```

```
  "exportData": [
    {
      "conditionName": "string",
      "diameterResultCode": "string",
      "errorMessage": "string",
      "experimentalResultCode": "string",
      "useExperimentalResultCode": true,
      "vendorId": "string"
    }
  ],
  "key": "string",
  "sourceVersion": "string",
  "topic": "string"
}
```

2.14 Session Viewer

Table 2-69 Supported REST APIs - Session Viewer

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Get PCF Bindings	GET	-H "accept: application/json" {apiRoot}/oc-bsf-query/v1/pcfBindings	200: OK. PCF bindings is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable
Delete Binding IDs	POST	{apiRoot}/oc-bsf-query/v1/pcfBindings/cleanup	200: OK. 201: Created 204: No content 401: Unauthorized 403: Forbidden 404: Not Found 500: Internal Server Error
Get Active Session Counter	GET	/v1/activeSessionCount/pcfBindings	200 : OK 401: Unauthorized 403: Forbidden 404: Not Found

Get PCF Bindings

To fetch PCF bindings, it is required to use any one of the following query parameters:

- SUPI
- GPSI
- UE Address

Table 2-70 Query Parameters

Parameter Name	Data Type	Mandatory(M)/ Optional(O)	Description
dnn	string	Optional	Specifies the Data Network Name.
gpsi	string	Optional	Specifies the Generic Public Subscription Identifier. For example - `msisdn-9192503899`.
ipDomain	string	Optional	Specifies the IPv4 address domain identifier
ipv4Addr	string	Optional	Specifies the IP addresses in IPv4 format
ipv6Prefix	string	Optional	Specifies the IPv6 Address Prefix. Note: When you use IPv6 prefix to query a session, ensure that you provide the full notation value. **Example**: `2011:db8:3c4d:0:0:0:0:0/48`
mac	string	Optional	Specifies the MAC address, which is formatted as six groups of two hexadecimal digits separated by colons (:) or hyphens (-). For example, in the format hh:hh:hh:hh:hh:hh.
sNssaiSd	string	Optional	Specifies the Slice Differentiator (SD) for a given S-NSSAI (Single Network Slice Selection Assistance Information). This optional information is used to differentiate slice or service type across multiple network slices.
sNssaiSst	integer	Optional	Specifies the Slice or Service type for a given S-NSSAI (Single Network Slice Selection Assistance Information).
supi	string	Optional	Specifies the Subscription Permanent Identifier. For example - `imsi-450081100100001`.

Sample cURL command

```
curl -X GET "http://10.75.168.25:32202/api-docs/oc-bsf-query/v1/pcfBindings?
supi=imsi-450080000000001" -H "accept: application/json"
```

Sample Response body structure for Pcf Bindings GET operation:

In the response, PCF bindings is returned as a string.

Delete PCF Bindings

Table 2-71 Request Body Parameters

Parameter Name	Data Type	Mandatory(M)/ Optional(O)	Description
bindingIds	string	Mandatory	Specifies the binding IDs to be deleted manually by the user.

Sample request body structure for Pcf Bindings delete operation:

```
{
  "bindingIds": [
    "string"
  ]
}
```

Sample cURL command

```
curl -X POST "http://10.75.168.25:32202/api-docs/oc-bsf-query/v1/pcfBindings/
cleanup" -H "accept: application/json" -H "Content-Type: application/json" -d
"{ \"bindingIds\": [ \"string\" ]}"
```

Get Active Session Counter

Get Active Session Counter is used to get an active session counter for a service.

There are no input parameters for this API.

Table 2-72 Response paramters

Parameter Name	Data Type	Mandatory(M)/Optional (O)	Description
dateTime	string	NA	Time stamp of the query
count	string	NA	Active sessions count
errorMsg	integer	NA	Error message to include in the response in case the request fails.

Sample success response:

```
{
  "dateTime": "Tue, 02 Jan 2018 18:07:59",
  "count": 2211
}
```

Sample failure response:

```
{
  "dateTime": "Tue, 02 Jan 2018 18:07:59"
```

```
  "errMsg": "Active Session Counting is not enabled"
}
```

Sample cURL command

```
curl -X GET "http://10.75.206.200:8000/oc-bsf-query/v1/activeSessionCount/
pcfBindings" -H "accept: */*"
```

2.15 Bulk Import/Export Controller

This section provides information for configuring bulk import/export in BSF.

Resource Name: Bulk Import Export Controller

Table 2-73 Supported REST APIs - Bulk Import Export Controller

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
Bulk Import Export Controller	-H "accept: */*" -H "ConttedFiles.zip;type=application/x-zip-compressed" /oc-bsf-configuration/v1/administration/import	POST	Bulk Import	200: OK 201: Created 401: Unauthorized 403: Forbidden 404: Not Found
	-H 'accept: application/json' -H 'Content-Type: application/json' -d @sampleput.json /oc-bsf-configuration/v1/administration/import/{importResourceId}/status	GET	Import Status	200: OK 401: Unauthorized 403: Forbidden 404: Not Found
	-H 'accept: application/json' -H 'Content-Type: application/json' -d @sampleput.json /oc-bsf-configuration/v1/administration/import/{importResourceId}/report	GET	Import Report	200: OK 401: Unauthorized 403: Forbidden 404: Not Found
	-H "accept: */*" /oc-bsf-configuration/v1/administration/import	GET	Import Resource Ids	200: OK 401: Unauthorized 403: Forbidden 404: Not Found

Table 2-73 (Cont.) Supported REST APIs - Bulk Import Export Controller

Resource Name	Resource URI	HTTP Method or Custom Operation	Description	Possible Result Code
	-H "accept: */*" -d "" /oc-bsf-configuration/v1/administration/export	POST	Bulk Export	200: OK 201: Created 401: Unauthorized 403: Forbidden 404: Not Found
	-H "accept: application/json" /oc-bsf-configuration/v1/administration/export/{exportResourceId}/status	GET	Export Status for BSF	200: OK 401: Unauthorized 403: Forbidden 404: Not Found
	-H "accept: application/octet-stream" /oc-bsf-configuration/v1/administration/export/{exportResourceId}/report	GET	Export Report for BSF	200: OK 401: Unauthorized 403: Forbidden 404: Not Found
	-H "accept: application/octet-stream" /oc-bsf-configuration/v1/administration/export/{exportResourceId}/download	GET	Download Exported File	200: OK 401: Unauthorized 403: Forbidden 404: Not Found
	-H "accept: */*" /oc-bsf-configuration/v1/administration/export	GET	Export Resource IDs	200: OK 401: Unauthorized 403: Forbidden 404: Not Found

Note

The Bulk Import/Export APIs return a ResourceId in response to the POST request. The ResourceId is the background task id for the POST operations. This id can be used to track the import or export requests, and download the export data.

For example, the POST API for bulk export operation takes Managed Object (MO) name as input. The response of this API contains the resource id of the file created for export. You can use this resource Id to download the export data at any point of time.

Below are the status displayed by Bulk import/export:

- **IN_PROGRESS**: If the import/export is running.

- **DONE**: If the import/export is finished. Following are the possible status if the import/export is in DONE status:
  - **SUCCESS** : If the import/export is successful
  - **FAILED** : If the import/export is failed
  - **PARTIAL_SUCCESS** : If the import/export is partially successful

2.16 Subscriber Activity Logging

Table 2-74 Supported REST APIs for Subscriber Activity Logging

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Create Subscriber Logging	POST	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/subscriberActivityLogging -d "{}"	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get Subscriber Logs	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/subscriberActivityLogging/{identifierValue}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-74 (Cont.) Supported REST APIs for Subscriber Activity Logging

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Update Subscriber Logging	PUT	-H "accept: application/json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/subscriberActivityLogging/{identifierValue} -d " {} "	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Delete Subscriber Logging	DELETE	-H "accept: */*" {apiRoot}/oc-bsf-configuration/v1/subscriberActivityLogging/{identifierValue}	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too many Requests 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Export Subscriber Logs	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/subscriberActivityLogging/export	200: OK General configuration is returned 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 429: Too Many Requests 500: Internal Server Error 503: Service Unavailable

Table 2-74 (Cont.) Supported REST APIs for Subscriber Activity Logging

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Import Subscriber Logs	POST	-H "accept: application/problem+json" -H "Content-Type: application/json" {apiRoot}/oc-bsf-configuration/v1/subscriberActivityLogging/import -d "{ }"	200: OK 201: Imported 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Get and Create Subscriber Logging

Table 2-75 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enable	boolean	O	Enable the subscriber logging.
type	string	O	Identifier type
value	string	M	Provide the value.

Sample Request body structure for POST operation:

```
{
  "enable": true,
  "type": "gpsi",
  "value": "string"
}
```

Sample Response body structure for GET, POST, and PUT operations:

```
[
  {
    "date": "string",
    "errors": [
      {
        "message": "string",
        "name": "string"
```

```
      }
    ],
    "exportData": [
      {
        "enable": true,
        "type": "gpsi",
        "value": "string"
      }
    ],
    "sourceVersion": "string",
    "topic": "string"
  }
]
```

Delete Subscriber Logging

Table 2-76 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
identifierValue	string	M	Subscriber Identifier

2.17 NRF Status

Table 2-77 BSF NRF Status Supported APIs

Description	HTTP Method or Custom Operation	Resource URI	Possible Result Code
Get NRF Status	GET	-H "accept: application/json" {apiRoot}/oc-bsf-configuration/v1/nrfStatus	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 2-78 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
nfStatus	String	M	It shows whether the BSF instance is registered, suspended, or deregistered with NRF.
nfType	String	M	The type of Network Function. Example: "BSF".
nfInstanceId	String	M	It shows the unique Instance ID of BSF registered with NRF.
nfFqdn	String	O	It shows the FQDN of the BSF registered with NRF.
nfRegistrationTime	String	O	It shows the time at which PCF registered with NRF
nfRegisteredWith	String	O	It shows the FQDN of the NRF with which BSF is registered.
nrfData	Object	M	It shows the details about the NRF.

Table 2-79 nrfData

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
priority	Integer	M	It shows the priority of the NRF instances. An NRF instance with priority 1 is treated as primary NRF.
apiRoot	String	M	
status	String	M	It shows the health status of the NRF instance. It could be in either healthy or unhealthy state.
statusChangeTime	String	M	It shows the time when the NRF status changed.
errorReason	Array	M	It shows the HTTP status codes or exceptions for which retry is attempted.
connectedTime	String	O	It shows the time when PCF last connected with primary NRF.
isPrimary	Boolean	M	It shows if this primary NRF or not.
isAttachedWithBsf	Boolean	M	It shows if this NRF instance is attached with BSF or not.

Sample Response body structure for GET operations:


```
{
    "nfStatus":"REGISTERED",
    "nfType":"BSF",
    "nfInstanceId":"fe7d992b-0541-4c7d-ab84-c6d70b1b0123",
    "nfFqdn":"ocbsf1-2-api-gateway.bsf1-2.svc.atlantic.morrisville.us.lab.oracle.com",
    "nfRegistrationTime":"2022-54-22 08:50:24",
    "nfRegisteredWith": "nf1stub.pdprodigiespolicy.svc:8080",
    "nrfData":[
      {
            "priority":1,
            "apiRoot":"nf2stub.pdprodigiespolicy.svc:8080",
            "status":"HEALTHY",
            "statusChangeTime": "2022-54-22 08:53:24",
            "errorReason": null,
            "connectedTime": "2022-54-22 08:54:24",
            "isPrimary": true,
            "isAttachedWithBsf": true
      },
      {     "priority":2,
            "apiRoot":"nf1stub.pdprodigiespolicy.svc:8080",
            "status":"UNHEALTHY",
            "statusChangeTime": "2022-54-22 08:51:24",
            "errorReason": "SocketTimeoutException",
            "connectedTime": "2022-54-22 08:54:22",
            "isPrimary": false,
            "isAttachedWithBsf": false
      }
]}
```


2.18 Error Configurations

API support is available for EXPORT/IMPORT of error handler configurations.

Table 2-80 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI	Media Type	Possible Result Code
Export Error Configuration	GET	{/oc-bsf-configuration/v1/services/errorHandler/errorConfiguration/export	application/json	200: OK 400: Bad Request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout default: default Response
Import Error Configuration	POST	/oc-bsf-configuration/v1/services/errorHandler/errorConfiguration/import	application/json	201: Imported 400: Bad Request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Preconditon Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout detault: default Response

This section describes the request/response body parameters for APIs for Error Import or Export Configurations.

Table 2-81 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
topic	string	M	Topic of each managed object
sourceVersion	string	O	System version of product from which data is exported
date	string	O	Current Timestamp
exportData	array	O	Exported list of error rules configurations

Sample Request Body structure for Import/Export operations:

```
{
  "topic": "string",
  "sourceVersion": "string",
  "date": "string",
  "exportData": [
    {
      "ruleMapperConfigs": [
        {
          "templateId": "string",
          "action": "string",
          "ruleName": "string",
          "isDefault": true,
          "context": {
            "context": "string",
            "errorInfo": {
              "errorDetails": {
                "status": "string",
                "instance": "string",
                "cause": "string",
                "message": "string",
                "resource": "string",
                "sourceService": "PDS",
                "targetService": "PDS"
              },
              "resourceErrorMap": {
                "additionalProp1": {
                  "status": "string",
                  "instance": "string",
                  "cause": "string",
                  "message": "string",
                  "resource": "string",
                  "sourceService": "PDS",
                  "targetService": "PDS"
                },
                "additionalProp2": {
                  "status": "string",
```

```
      "instance": "string",
      "cause": "string",
      "message": "string",
      "resource": "string",
      "sourceService": "PDS",
      "targetService": "PDS"
    },
    "additionalProp3": {
      "status": "string",
      "instance": "string",
      "cause": "string",
      "message": "string",
      "resource": "string",
      "sourceService": "PDS",
      "targetService": "PDS"
    }
  },
  "trace": {
    "additionalProp1": [
      {
        "errorState": "string",
        "errorDetails": {
          "status": "string",
          "instance": "string",
          "cause": "string",
          "message": "string",
          "resource": "string",
          "sourceService": "PDS",
          "targetService": "PDS"
        }
      }
    ],
    "additionalProp2": [
      {
        "errorState": "string",
        "errorDetails": {
          "status": "string",
          "instance": "string",
          "cause": "string",
          "message": "string",
          "resource": "string",
          "sourceService": "PDS",
          "targetService": "PDS"
        }
      }
    ],
    "additionalProp3": [
      {
        "errorState": "string",
        "errorDetails": {
          "status": "string",
          "instance": "string",
          "cause": "string",
          "message": "string",
          "resource": "string",
          "sourceService": "PDS",
```

```
            "targetService": "PDS"
          }
        }
      ]
    }
  },
  "type": "string"
},
"errorMatcher": {
  "errorStateDisp": {
    "errorType": {
      "label": "string",
      "value": "string"
    },
    "origin": {
      "label": "string",
      "value": "string"
    },
    "operation": {
      "label": "string",
      "value": "string"
    },
    "errorStatus": {
      "label": "string",
      "value": "string"
    },
    "sourceInterface": {
      "label": "string",
      "value": "string"
    }
  },
  "errorCauseDisp": {
    "status": {
      "label": "string",
      "value": "string"
    },
    "instance": {
      "label": "string",
      "value": "string"
    },
    "message": {
      "label": "string",
      "value": "string"
    },
    "cause": {
      "label": "string",
      "value": "string"
    },
    "resource": {
      "label": "string",
      "value": "string"
    }
  },
  "errorCause": {
    "field": "string",
    "match": "string",
```

```
                "value": {
                  "status": "string",
                  "instance": "string",
                  "message": "string",
                  "resource": "string",
                  "cause": "string"
                }
              },
              "errorState": "string"
            },
            "priority": 0,
            "key": "string",
            "errorRuleEnabled": true
          }
        ],
        "enableErrorHandler": true,
        "serviceName": "string"
      }
    ]
}
```

3
Common Services REST Specifications

This section provides information about the REST specifications for Common Services used in Oracle Communications Cloud Native Core Binding Support Function (BSF). You can use the following APIs to update configurations related to the Overload Control feature.

3.1 Egress Gateway for SCP Health

Peer Configuration

Table 3-1 Peer Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Get Peer Configuration	GET	/{nfType}/nf-common-component/v1/{serviceName}/peerconfiguration	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-1 (Cont.) Peer Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Update Peer Configuration	PUT	/{nfType}/nf-common-component/v1/{serviceName}/peerconfiguration	application/json	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Partially Update Peer Configuration	PATCH	/{nfType}/nf-common-component/v1/{serviceName}/peerconfiguration	application/json	200: OK 204: No Content 304: Not Modified 400: Bad Request 422: Unprocessable Entity

Table 3-1 (Cont.) Peer Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Get All Peer Configuration	GET	/{nfType}/nf-common-component/v1/{serviceName}/{instanceId}/peerconfiguration	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Update All Peer Configurations	PUT	/{nfType}/nf-common-component/v1/{serviceName}/{instanceId}/peerconfiguration	application/json	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-1 (Cont.) Peer Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Partially Update Peer Configurations in the list	PATCH	/{nfType}/nf-common-component/v1/{serviceName}/{instanceId}/peerconfiguration	application/json	200: OK 204: No Content 304: Not Modified 400: Bad Request 422: Unprocessable Entity

Table 3-2 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
id	string	O	Peer identifier **Note**: Unique value in peerconfiguration
host	string	O	Host details of a peer.It can be IPv4, IPv6 and FQDN details.
virtualHost	string	O	Host details of a remote peer. For SLF feature, the virtualHost is SCP peer details. It must be a valid FQDN.This FQDN is sent to Alternate Route Service for DNS SRV resolution.
port	string	O	Port details of a peer.
apiPrefix	string	O	API prefix details of a peer. **Note**: Keep the value as '/' only
healthApiPath	string	O	Path of health API `/scp-api-root/v1/status`. This attribute is added to maintain the health status of the API. This attribute is added as part of monitoring the availability of SCP health status.

Sample Body:

```
[
   {
      "id":"peer1",
      "host":"10.75.225.67",
```

```
      "port":"31235",
      "apiPrefix":"/",
      "healthApiPath":"/health/v1"
   },
   {
      "id":"peer2",
      "host":"10.75.214.18",
      "port":"31236",
      "apiPrefix":"/",
      "healthApiPath":"/health/v2"
   }
]
```

Peer Monitor Configuration

Table 3-3 Peer Monitor Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Get Peer Monitor Configuration	GET	/{nfType}/nf-common-component/v1/{serviceName}/peermonitoringconfiguration	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-3 (Cont.) Peer Monitor Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Add or Update Peer Monitor Configuration	PUT, PATCH	/{nfType}/nf-common-component/v1/{serviceName}/peermonitoringconfiguration	application/json	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Get Peer Monitor Configuration(array)	GET	/{nfType}/nf-common-component/v1/{serviceName}/{instanceId}/peermonitoringconfiguration	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-3 (Cont.) Peer Monitor Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Add or update Peer Monitor Configuration(array)	PUT, PATCH	/{nfType}/nf-common-component/v1/{serviceName}/{instanceId}/peermonitoringconfiguration	application/json	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-4 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enabled	Boolean	O	Attribute to enable or disable monitoring at a global level. **Default value**: false
timeout	Long	O	Flag to configure the duration after which calls to the SCP health API is timed out. This is provided in milliseconds. The allowed value ranges from 300 milliseconds to 10000 milliseconds. **Default value**: 1000

Table 3-4 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
frequency	Long	O	Indicates the frequency or interval at which Egress Gateway microservice initiates health check calls toward SCP. This is provided in milliseconds. The allowed value ranges from 300 milliseconds to 10000 milliseconds. **Default value**: 2000
failureThreshold	Integer	O	Indicates the number of consecutive failure responses after which a healthy SCP can be marked as unhealthy. The allowed value ranges 1 to 10. The maximum number of attempts to mark SCP unhealthy is 10. **Default value**: 3
successThreshold	Integer	O	Indicates the number of successful responses after which an unhealthy SCP can be marked as healthy. Health API call to given SCP shall succeed consecutively to these many attempts before it is marked as Available from UNAVAILABLE. The allowed value ranges 1 to 10. **Default value**: 3

Sample body:

```
{
    "enabled":true,
    "timeout":1000,
    "frequency":2000,
    "failureThreshold":3,
    "successThreshold":3
}
```

Peer Set Configuration

Table 3-5 Peerset Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Get Peerset Configuration	GET	{apiRoot}/egw/healthStatus/peerSet/{peerSetId}	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
List of Peerset Configuration(array)	GET	{apiRoot}/egw/healthStatus/peerSet	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-5 (Cont.) Peerset Configuration supported REST APIs details

Description	HTTP Method or Custom Operation	Resource URI	Content Type	Possible Result Codes
Get the list of peer sets where in each peer set consists of ID and list of http or https instances.	GET	/{nfType}/nf-common-component/v1/{serviceName}/peersetconfiguration	application/json	200: OK 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout
Add or update the list of peer sets where in each peer set consists of ID and list of http or https instances.	PUT, PATCH	/{nfType}/nf-common-component/v1/{serviceName}/peersetconfiguration	application/json	200: OK Specifies that the update is successful and provides the values in database. 201: Created 400: Bad request 401: Unauthorized 403: Forbidden 404: Not Found 405: Method Not Allowed 406: Not Acceptable 408: Request Timeout 409: Conflict 412: Precondition Failed 500: Internal Server Error 503: Service Unavailable 504: Gateway Timeout

Table 3-6 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
id	string	O	Identifier for Peer Set.
httpConfiguration	array(PeerIdentiferConfiguration)	O	Configuration for HTTP based Peers. This value will be selected, if 3GPPAPIRootScheme value is http.
httpsConfiguration	array(PeerIdentifierConfiguration)	O	Configuration for HTTPs based Peers. This value will be selected, if 3GPPAPIRootScheme value is https.

Table 3-7 PeerIdentifierConfiguration

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
priority	integer	O	Priority of peer to be used in a peer set.
peerIdentifier	string	O	Peer identifier is the value of peer configured during PeerConfiguration.

Sample body:

```
peerSetConfiguration[
   {
       "id":"set0",
       "httpConfiguration":[
       {
       "priority": 1,
              "peerIdentifier": "peer1"
       }],
       "httpsConfiguration":[
       {
       "priority": 1,
              "peerIdentifier": "peer1"
       }]
```

3.2 OC Policy Mapping

This URI can be used to update service names and corresponding policy name for the service which is mapped to "ocDiscardPolicies" based on "policyName" and also to enable/disable the Overload Control feature and the sampling period in overload control. By default, the Overload

Control feature is disabled and the sampling period is the 60s. To enable the feature, REST API needs to be invoked and update the enabled flag to true.

Table 3-8 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get OC Policy Mapping	GET	BSF/nf-common-component/v1/{serviceName}/ocpolicymapping
Update OC Policy Mapping	PUT	BSF/nf-common-component/v1/{serviceName}/{instanceId}/ocpolicymapping
Partially OC Policy Mapping	PATCH	BSF/nf-common-component/v1/{serviceName}/{instanceId}/ocpolicymapping

Get, Update, and Patch OCPolicyMapping

Table 3-9 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
enabled	boolean	M	To enable or disable Overload Control feature. Set values to: • true: To enable • false: To disable
mappings.svcName	string	M	The SVC entry to determine a mapping between service and discard policy name per service.
mappings.policyName	string	M	The discard policy entry to determine a mapping between service and discard policy name per service.
samplingPeriod	integer	M	Time frame for each cycle of Overload Control per service. Its value is in milliseconds.

Sample Request/Response body structure for GET, PUT, and PATCH operations:

```
{
   "enabled": true,
   "mappings": [
   {
     "svcName": "sm.bsf.com",
     "policyName": "OCDP1"
   },
   {
     "svcName": "cm.bsf.com",
     "policyName": "OCDP2"
   },
```

```
    {
      "svcName": "localhost",
      "policyName": "OCDP3"
    }],
    "samplingPeriod": 200
}
```

3.3 Error Code Profiles

This URI can be used to update the errorCodeProfiles that are used in Overload Control feature for populating details in error responses when a request is discarded.

By default, the errorCodeProfiles remains null.

Table 3-10 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get error code profiles	GET	BSF/nf-common-component/v1/{serviceName}/errorcodeprofiles
Update error code profiles	PUT	BSF/nf-common-component/v1/{serviceName}/{instanceId}/errorcodeprofiles
Partially update the error code profiles	PATCH	BSF/nf-common-component/v1/{serviceName}/{instanceId}/errorcodeprofiles

Get, Update, and Patch errorCodeProfile

Table 3-11 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
name	string	M	Error name.
errorCode	integer	M	errorCode field in an errorScenario determines the HttpStatusCode that needs to be populated in **ProblemDetails (HttpStatus field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType field.
errorCause	string	O	errorCause field in an errorScenario determines the error cause that needs to be populated in **ProblemDetails (Cause field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter.
errorTitle	string	O	errorTitle field in an errorScenario determines the title that needs to be populated in **ProblemDetails (Title field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter.

Table 3-11 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
redirectURL	string	O	redirectUrl field in an errorScenario determines the redirection URL, this value is populated in **LOCATION** header while sending response from IGW. The header is populated only when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter, the errorCode configured for the particular errorScenario lies in 3xx error series and the redirectUrl field for the particular errorScenario is configured appropriately.
retry-after	string	O	retryAfter field in an errorScenario determines the value in seconds/ particular date after which the service should be retried, this value is populated in **Retry-After** header while sending response from IGW. The header is populated only when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter, the errorCode configured for the particular errorScenario lies in 3xx error series and the retryAfter field for the particular errorScenario is configured appropriately in seconds.
errorDescription	string	O	errorDescription field in an errorScenario determines the description that needs to be populated in **ProblemDetails (Detail field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType field.

Sample Request/Response body structure for GET, PUT, and PATCH operations:

```
[
 {
   "name": "error300",
   "errorCode": 300,
   "errorCause": "",
   "errorTitle": "",
   "redirectURL": "",
   "retry-after": "",
   "errorDescription": ""
 },
 {
   "name": "error500",
   "errorCode": 500,
   "errorCause": "",
   "errorTitle": "",
   "redirectURL": "",
   "retry-after": "",
   "errorDescription": ""
 },
 {
```

```
   "name": "error429",
   "errorCode": 429,
   "errorCause": "",
   "errorTitle": "",
   "redirectURL": "",
   "retry-after": "",
   "errorDescription": ""
 }
]
```

3.4 OC Discard Policies

This URI can be used to update discard policies that will be used in overload control to select the appropriate policy from the configured list based on the load level of a particular service. By default, ocDicardPolicies will be null.

Table 3-12 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get Discard Policies	GET	BSF/nf-common-component/v1/{serviceName}/ocdiscardpolicies
Update Discard Policy	PUT	BSF/nf-common-component/v1/{serviceName}/{instanceId}/ocdiscardpolicies
Partially update the Discard Policy	PATCH	BSF/nf-common-component/v1/{serviceName}/{instanceId}/ocdiscardpolicies

Get, Update, and Patch OCDiscardData

Table 3-13 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
name	string	M	Name of the discarded policy.
scheme	string The value can be: • PriorityBased • Percentage Based	M	Discarded policy scheme.
policies.value	integer	M	Value of priority above which requests are considered as potential candidates for drop. Percentage of requests to drop in the current sampling period over the calculated rate in the previous sampling period.

Table 3-13 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
policies.action	string The vaue can be: RejectWithErrorCode	O	Defines the action to be taken on selected requests rejection based on error code.
policies.level	string	O	Defines the overload level.
policies.errorCodeProfile	string	O	The error code profiles.

Sample Request/Response body structure for GET, PUT, and PATCH operations:

```
[
 {
   "name": "OCDP2",
   "scheme": "PercentageBased",
   "policies": [
   {
     "value": 20,
     "action": "RejectWithErrorCode",
     "level": "L1",
     "errorCodeProfile": "error411"
   },
   {
     "value": 40,
     "action": "RejectWithErrorCode",
     "level": "L2",
     "errorCodeProfile": "error412"
   },
   {
      "value": 60,
      "action": "RejectWithErrorCode",
      "level": "L3",
      "errorCodeProfile": "error413"
   },
   {
     "value": 80,
     "action": "RejectWithErrorCode",
     "level": "L4",
     "errorCodeProfile": "error414"
   },
   {
     "value": 95,
     "action": "RejectWithErrorCode",
     "level": "L5",
     "errorCodeProfile": "error415"
   }]
```

```
 },
 {
   "name": "OCDP1",
   "scheme": "PriorityBased",
   "policies": [
   {
     "value": 30,
     "action": "RejectWithErrorCode",
     "level": "Minor",
     "errorCodeProfile": "error300"
   },
   {
     "value": 20,
     "action": "RejectWithErrorCode",
     "level": "Critical",
     "errorCodeProfile": "error500"
   }]
 }
]
```

3.5 Overload Level Threshold

This URI can be used to configure the Overload Threshold Level. The data is saved in a line with service_name perf-info and used by the overload manager.

Table 3-14 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get Overload Threshold Value of the required SVC (Backend service).	GET	/BSF/nf-common-component/v1/perf-info/overloadLevelThreshold
Update the Overload Threshold Value of the required SVC (Backend service).	PUT	/BSF/nf-common-component/v1/perf-info/overloadLevelThreshold

Update overloadLevelThreshold

Table 3-15 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
svcName	string	M	Name of the backend service (svcName).
metricsThresholdList	array	M	List of criteria used to calculate the load level.
metricsThresholdList.metricsName	string	M	Name of criteria

Table 3-15 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)aints	Description
metricsThresholdList.levelThresholdList	array	M	List of threshold values
metricsThresholdList.levelThresholdList.level	string	M	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's `ocdiscardpolicies`.
metricsThresholdList.levelThresholdList.abatementValue	integer	M	If the metric level goes below this value, load level goes to a lower value. **Note**: The abatement value must always be greater than zero. Also, it must be greater than onset value.
metricsThresholdList.levelThresholdList.onsetValue	integer	M	If the metric level goes above this value, load level is set.

Sample Request/Response body structure for GET/PUT operation:

```
[
       {
       "svcName": "bsf.management",
       "metricsThresholdList": [
           {
               "metricsName": "svc_pending_count",
               "levelThresholdList": [
                   {
                       "level": "L1",
                       "onsetValue": 50,
                       "abatementValue": 40
                   },
                   {
                       "level": "L2",
                       "onsetValue": 200,
                       "abatementValue": 180
                   },
                   {
                       "level": "L3",
                       "onsetValue": 400,
                       "abatementValue": 360
                   },
                   {
                       "level": "L4",
                       "onsetValue": 600,
                       "abatementValue": 540
                   },
                   {
                       "level": "L5",
                       "onsetValue": 800,
```

```
                    "abatementValue": 720
                }
            ]
        }
    ]
    }
]
```

3.5.1 Overload Level Threshold Profiles

This URI can be used to configure the Overload Threshold Level Profiles. The data is saved in a line with service_name perf-info and used by the overload manager.

Table 3-16 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get the Overload Threshold Profile of the required SVC (Backend service).	GET	/oc-bsf-configuration/v1/overloadlevelThreshold/activeProfile For details on Request/Response parameters for GET activeProfile, see Table 3-17
Activate the Overload Threshold Profile	PUT	/oc-bsf-configuration/v1/overloadlevelThreshold/activeProfile For details on Request/Response parameters for PUT activeProfile, see Table 3-17
Get all the overload threshold profiles names which includes default and custom profiles	GET	/oc-bsf-configuration/v1/overloadlevelThreshold/profiles For details on Request/Response parameters for GET profiles, see Table 3-18
Get Overload Threshold Value for particular profile.	GET	/oc-bsf-configuration/v1/overloadlevelThreshold/profiles/{name} For details on Request/Response parameters for GET profiles/{name}, see Table 3-19
Adds a new Overload Threshold Profile	POST	/oc-bsf-configuration/v1/overloadlevelThreshold/profiles/{name} For details on Request/Response parameters for POST profiles/{name}, see Table 3-19
Update the profile.	PUT	/oc-bsf-configuration/v1/overloadlevelThreshold/profiles/{name} For details on Request/Response parameters for PUT profiles/{name}, see Table 3-19

Table 3-16 (Cont.) Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Delete the Overload Threshold Profile of the required SVC (Backend service).	DELETE	/oc-bsf-configuration/v1/overloadlevelThreshold/profiles/{name}
Migrate the data from standalone to profile i.e if any overloadlevelThreshold data is already configured then it will migrate that data to profile name - Name of the profile activate - if after migration , profile should be activated	POST	//oc-bsf-configuration/v1/overloadlevelThreshold/migrate For details on Request/Response parameters for POST migrate, see Table 3-20
Exports the Overload Threshold Profile.	GET	/oc-bsf-configuration/v1/overloadlevelThreshold/export
Imports the Overload Threshold Profile.	POST	/oc-bsf-configuration/v1/overloadlevelThreshold/import For details on Request/Response Body Parameters for POST (import), see Table 3-21.

Table 3-17 Request/Response Body Parameters for GET/PUT activeProfile

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	M	Name of the active profile.

Sample Request/Response for GET/PUT activeProfile

```
{
    "name":"custom"
}
```

Table 3-18 Request/Response Body Parameters for GET profiles

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	M	Name of the profile.
isCustomProfile	string	M	To specify the type of profile: default or custom

Sample Request/Response for GET profiles

```
[
{
    "name":"default",
    "isCustomProfile":false
},{
    "name":"custom",
    "isCustomProfile":true
}
]
```

Table 3-19 Request/Response Body Parameters for GET/PUT/POST profiles/{name}

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	M	Name of the profile.
value.svcName	string	M	Name of the backend service (svcName).
value.metricsThresholdList	array	M	List of criteria used to calculate the load level.
value.metricsThresholdList.metricsName	string	M	Name of criteria
value.metricsThresholdList.levelThresholdList	array	M	List of threshold values
value.metricsThresholdList.levelThresholdList.level	string	M	Specifies the name of the level: L1/L2/L3.
value.metricsThresholdList.levelThresholdList.abatementValue	integer	M	If the metric level goes below this value, load level goes to a lower value. **Note**: • This value should be greater than 0. • This value should be greater than onset value.
value.metricsThresholdList.levelThresholdList.onsetValue	integer	M	If the metric level goes above this value, load level is set.

Sample Request/Response for GET/PUT/POST profiles/{name}

```
{
    "name": "custom",
        "value": [
        {
            "svcName": "bsf.management",
            "metricsThresholdList": [
                {
                    "metricsName": "cpu",
                    "levelThresholdList": [
```

```
                        {
                            "level": "L1",
                            "onsetValue": 49,
                            "abatementValue": 46
                        },
                        {
                            "level": "L2",
                            "onsetValue": 55,
                            "abatementValue": 52
                        },
                        {
                            "level": "L3",
                            "onsetValue": 58,
                            "abatementValue": 56
                        }
                    ]
                }
            ]
        }
    ]
}
```

Table 3-20 Request/Response Body Parameters for POST migrate

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	M	Name of the profile to migrate.
activate	string	M	To activate the profile. Set value to: • true: To activate • false: Not to activate

Sample Request/Response for GET profiles list

```
{
     "name":"migrate_profile",
     "activate":true/false
}
```

Table 3-21 Request/Response Body Parameters for POST (import)

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
exportData.name	string	M	Name of the profile.

Table 3-21 (Cont.) Request/Response Body Parameters for POST (import)

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
exportData.value.svcName	string	M	Name of the backend service (svcName).
exportData.value.metricsThresholdList	array	M	List of criteria used to calculate the load level.
exportData.value.metricsThresholdList.metricsName	string	M	Name of criteria: • `cpu` • `svc_pending_count` • `svc_failure_count` • `memory`
exportData.value.metricsThresholdList.levelThresholdList	array	M	List of threshold values
exportData.value.metricsThresholdList.levelThresholdList.level	string	M	Specifies the name of the level: L1/L2/L3.
exportData.value.metricsThresholdList.levelThresholdList.abatementValue	integer	M	If the metric level goes below this value, load level goes to a lower value. The abatement values for each of the metrics are as follows: • `cpu` (Calucalted in percentage (%)) and ranges between 1-100 • `svc_pending_count` (Accepts an integer value) and ranges between 1 to 1000000 • `svc_failure_count` (Accepts an integer value) and ranges between 1 to 1000000 • `memory` (Calucalted in percentage (%)) and ranges between 1-100
exportData.value.metricsThresholdList.levelThresholdList.onsetValue	integer	M	If the metric level goes above this value, load level is set. The onset value of L1 is less than the abatement value of L2 and the onset value of L2 is less than the abatement value of L3. The onset values for each of the metrics are as follows: • `cpu` (Calucalted in percentage (%)) and ranges between 1-100 • `svc_pending_count` (Accepts an integer value) and ranges between 1 to 1000000 • `svc_failure_count` (Accepts an integer value) and ranges between 1 to 1000000 • `memory` (Calucalted in percentage (%)) and ranges between 1-100

Sample Request/Response Body Parameters for POST (import)

```
"exportData": [
    {
      "name": "TestProfile",
      "value": [
        {
          "svcName": "bsf.management",
          "metricsThresholdList": [
            {
              "metricsName": "cpu",
              "levelThresholdList": [
                {
                  "level": "L1",
                  "abatementValue": 41,
                  "onsetValue": 44
                },
                {
                  "level": "L2",
                  "abatementValue": 47,
                  "onsetValue": 49
                },
                {
                  "level": "L3",
                  "abatementValue": 50,
                  "onsetValue": 52
                }
              ]
            },
        }
```

3.6 NF profile registration with NRF

These URIs can be used to update or retrieve Binding Support Function (BSF) profile to be registered with Network Repository Function (NRF).

Table 3-22 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get BSF NfProfile	GET	BSF/nf-common-component/v1/nrf-client-nfmanagement/nfProfileList
Update BSF NfProfile	PUT	BSF/nf-common-component/v1/nrf-client-nfmanagement/nfProfileList

The sample request body structure for GET and PUT operation is as follows:

```
[
   {
      "nfInstanceId":"fe7d992b-0541-4c7d-ab84-c6d70b1b0666",
      "nfType":"BSF",
      "nfStatus":"REGISTERED",
```

```
      "fqdn":"ocbsf1-2-api-
gateway.bsf1-2.svc.atlantic.morrisville.us.lab.oracle.com",
      "priority":1,
      "capacity":1,
      "load":2,
      "bsfInfo":{
         "ipv4AddressRanges":[
            {
               "start":"10.0.0.1",
               "end":"10.113.255.255"
            }
         ],
         "ipv6PrefixRanges":[
            {
               "start":"2800:a00:cc03::/64",
               "end":"2800:a00:cc04::/64"
            }
         ]
      },
      "nfServices":[
         {
            "serviceInstanceId":"03063893-cf9e-4f7a-9827-111111111111",
            "serviceName":"nbsf-management",
            "versions":[
               {
                  "apiVersionInUri":"v1",
                  "apiFullVersion":"1.0.0",
                  "expiry":"2019-08-03T18:66:08.871+0000"
               }
            ],
            "scheme":"http",
            "nfServiceStatus":"REGISTERED",
            "fqdn":"ocbsf1-2-api-
gateway.bsf1-2.svc.atlantic.morrisville.us.lab.oracle.com",
            "interPlmnFqdn":null,
            "ipEndPoints":[
               {
                  "ipv4Address":"10.233.22.149",
                  "transport":"TCP",
                  "port":80
               }
            ],
            "apiPrefix":null,
            "allowedNfTypes":[
               "PCF",
               "AF",
               "NEF"
            ],
            "priority":1,
            "capacity":1,
            "load":2
         }
      ]
   }
]
```

BSF NRF Status

Table 3-23 BSF NRF Status supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get BSF instance details	GET	BSF/v1/nrf-client/{**nfInstanceId**}/nf-status

The sample request body structure for GET operation is as follows:

```
{
 "nfStatus": "REGISTERED",
 "currentNrfConnection": {
   "apiRoot": "nf1stub.pdprodigiespolicy.svc:8080",
   "connectionTime": "2022-54-22 08:54:24"
 },
 "registeredWithNrf": {
   "apiRoot":null,
   "connectionTime": "2022-54-22 08:54:24"
 }
}
```

NRF Health Status

Table 3-24 NRF Health Status supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get NRF instance details	GET	BSF/v1/nrf-client/nrf-health-status

The sample request body structure for GET operation is as follows:

```
[{
  "priority": 1,
  "nrfApiRoot": "http://notify-stub-service.default:8080",
  "status": "HEALTHY",
  "statusChangeTime": "yyyy-MM-dd HH:mm:ss",
  "errorReason": "SocketTimeoutException"
}]
```

3.7 Server Header at Ingress Gateway

This section describes the Common Config Server URIs that you can use to enable and configure server header at Ingress Gateway. The server header is included in the error responses sent by Ingress Gateway for the errors generated at Ingress Gateway as well as backend microservices.

> **Note**
>
> You can configure server header at both global and route level. However, if you define server header configuration at both global and route level, the route level configuration (irrespective of being enabled or disabled) takes precendence over the global level configuration.

Error Code Series List

The following table describes the URIs available to define and retrieve error code series list:

Table 3-25 Supported REST APIs for Error Code Series List

Description	HTTP Method or Custom Operation	Resource URI
Get Error Code Series List	GET	{apiRoot}/BSF/nf-common-component/v1/igw/errorcodeserieslist
Define Error Code Series List	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/errorcodeserieslist
Delete Error Code Series List	PUT To delete the configurations, put an empty json in the request. `[]`	{apiRoot}/BSF/nf-common-component/v1/igw/errorcodeserieslist

The sample request body structure for PUT operation is as follows:

```
errorcodeserieslist:
[
    {
        "id": "E1",
        "errorCodeSeries":
        [
            {
                "errorSet": "4xx",
                "errorCodes": [400, 408]
            },
            {
                "errorSet": "5xx",
                "errorCodes": [500, 503]
            }
        ]
    },
    {
        "name": "E2",
        "errorCodeSeries":
        [
            {
                "errorSet": "4xx",
```

```
                "errorCodes": [-1]
            }
        ]
    }
]
```

Table 3-26 Request and Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
id	string	M	Specifies the unique ID that is used in the `errorCodeSeriesId` while configuring server header at global or route level.
errorCodeSeries.errorSet	string	M	Specifies an errorSet (4XX, 5XX) in errorCodeSeries for matching server response.
errorCodeSeries.errorCodes	array	M	Specifies the error codes in a specific error set against which the server response is validated for populating server header.

Configuring Server header (global level)

The following table describes the URIs available to enable and configure server header at global level:

Table 3-27 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get Server Header	GET	{apiRoot}/BSF/nf-common-component/v1/igw/serverheaderdetails
Define Server Header	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/serverheaderdetails

The sample request body structure for PUT operation is as follows:

```
serverheaderdetails:
{
   "enabled": true,
   "errorCodeSeriesId": "E1", # See "errorcodeserieslist" resource below for
more details.
   "configuration": {
     "nfType": "BSF",
     "nfInstanceId": "123456"
   }
}
```

Table 3-28 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enabled	boolean	M	When the value for this parameter is set to true, server headers are generated at a global level. To generate server headers at route level, set the value to false.
errorCodeSeriesId	string	M	Specifies the error list IDs.
configuration.nfType	string	M	Specifies the type of network function. **Default value**: BSF
configuration.nfInstanceId	string	M	Specifies the NF Instance ID of the BSF.

Configuring Server header (route level)

The following table describes the URIs available to enable and configure server header at route level:

Table 3-29 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get Route Level Configuration	GET	{apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration
Define Server Header at Route Level	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration

The sample request body structure for PUT operation is as follows:

```
[{
        "id": "reverse_bsf_service",
        "serverHeaderDetails": {
        "enabled": true,
        "errorCodeSeriesId": "E1"
        }
    }]
```

The sample request body structure to clear route using PUT operation is as follows:

```
[]
```

Table 3-30 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
id	string	M	Specifies the route IDs for which you need to define server header. You can define the server header at route level for any of the following supported route IDs: • reverse_bsf_service • reverse_nrf_notify_service
serverHeaderDetails.enabled	boolean	M	Set the value for this parameter to true if you want to define server header at the route level.
serverHeaderDetails.errorCodeSeriesId	string	M	Specifies the error list IDs.

The sample request body structure for GET operation is as follows:

```
[{
    "id":"reverse_bsf_service"
}]
```

3.8 Rate Limiting at Ingress Gateway

This section describes the URIs that you can use to configure route level rate limiting in persistent configuration at Ingress Gateway.

Error Code Profiles

The following table describes the URIs available to define and retrieve error code profiles in persistent configuration:

Table 3-31 Supported REST APIs for Error Code Profiles

Description	HTTP Method or Custom Operation	Resource URI
Get Error Code Profiles	GET	{apiRoot}/BSF/nf-common-component/v1/igw/errorcodeprofiles
Define Error Code Profiles	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/errorcodeprofiles

The sample request body structure for PUT operation is as follows:

```
[
        {
            "name": "error453",
            "errorCode": 453,
```

```
            "errorDescription": "",
            "errorCause": "",
            "errorTitle": "",
            "redirectURL": "",
            "retry-after": ""
        },
        {
            "name": "error500",
            "errorCode": 500,
            "errorDescription": "",
            "errorCause": "",
            "errorTitle": "",
            "redirectURL": "",
            "retry-after": ""
        },
        {
            "name": "error429",
            "errorCode": 429,
            "errorDescription": "",
            "errorCause": "",
            "errorTitle": "",
            "redirectURL": "",
            "retry-after": ""
        }
    ]
```

Table 3-32 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	M	Specifies the unique name for the error profile.
errorCode	string	M	errorCode field in an errorScenario determines the HttpStatusCode that needs to be populated in **ProblemDetails (HttpStatus field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType field.
errorCause	string	M	errorCause field in an errorScenario determines the error cause that needs to be populated in **ProblemDetails (Cause field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter.
errorTitle	string	O	errorTitle field in an errorScenario determines the title that needs to be populated in **ProblemDetails (Title field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter.

Table 3-32 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
redirectURL	string	O	redirectUrl field in an errorScenario determines the redirection URL, this value is populated in **LOCATION** header while sending response from IGW. The header is populated only when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter, the errorCode configured for the particular errorScenario lies in 3xx error series and the redirectUrl field for the particular errorScenario is configured appropriately.
retry-after	string	O	retryAfter field in an errorScenario determines the value in seconds/ particular date after which the service should be retried, this value is populated in **Retry-After** header while sending response from IGW. The header is populated only when the exception occurred at IGW matches the configured errorScenario's exceptionType parameter, the errorCode configured for the particular errorScenario lies in 3xx error series and the retryAfter field for the particular errorScenario is configured appropriately in seconds.
errorDescription	string	O	errorDescription field in an errorScenario determines the description that needs to be populated in **ProblemDetails (Detail field)** response from IGW when the exception occurred at IGW matches the configured errorScenario's exceptionType field.

Configuring Rate Limit for BSF

The following table describes the URIs available to enable and configure ratelimit:

Table 3-33 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get Rate Limit	GET	{apiRoot}/BSF/nf-common-component/v1/igw/routelevelratelimiting
Define Rate Limit	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/routelevelratelimiting

The sample request body structure for PUT operation is as follows:

```
{
   "enabled": true,
   "samplingPeriod": 2000,
   "rateLimitPolicies": [
```

```
    {
      "name": "R1",
      "value": 5,
      "action": "RejectWithErrorCode",
      "scheme": "PriorityBased",
      "errorCodeProfile": "error429"
    }
    ]
}
```

Table 3-34 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enabled	boolean	M	Specifies whether to enable or disable rate limiting feature.
samplingPeriod		M	Specifies the duration for each cycle of route rate limit. The value of sampling period is defined in milliseconds.
rateLimitPolicies.name	string	M	Specifies the unique name of the discard policy.
rateLimitPolicies.value	integer	M	Specifies the value of priority above which requests are considered as potential candidates for drop.
rateLimitPolicies.action	string	M	Specifies the action such as silent drop or rejection for the selected requests.
rateLimitPolicies.scheme	string	M	Specifies the scheme on the basis of which requests are selected to be dropped. The only supported value for this parameter is `PriorityBased`.
rateLimitPolicies.errorCodeProfile	string	M	Specifies the error code profile.

Configuring Rate Limit for BSF at route level

The following table describes the URIs available to enable and configure rate-limit at route level:

Table 3-35 Supported REST APIs

Description	HTTP Method or Custom Operation	Resource URI
Get Rate Limit at route level Configuration	GET	{apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration
Define Rate Limit at route level Configuration	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration

The sample request body structure for PUT operation is as follows:

```
[
    {
        "id": "reverse_bsf_service",
        "rateLimiting": {
            "methods": [
                {
                    "name": "POST",
                    "rate": 3,
                    "rateLimitPolicy": "R1"
                }
            ]
        }
    }
]
```

Table 3-36 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
id	string	M	Specifies the route IDs for which you need to define the rate limit. You can define the rate limit at route level for any of the following supported route IDs: • bsf_management_register • bsf_management_deregister • bsf_management_discovery
rateLimiting.methods.name	string	M	Specifies the name of the HTTP method such as GET, PUT, POST, DELETE, or PATCH. The rate limit is calculated by considering the method along with the route ID.
rateLimiting.methods.rate	integer	M	Specifies the rate for route level rate limit. Any requests with sbi-priority header with a value greater than the configured number are discarded.
rateLimiting.methods.rateLimitPolicy	string	M	Specifies the unique rate limit policy name.

3.9 Pod Protection Mechanism at Ingress Gateway

This section describes the URIs that you can configure to apply congestion control on Ingress Gateway when the pod is overloaded.

Pod Protection

The following table describes the URIs available to retrieve and update pod protection configurations:

Table 3-37 Supported REST APIs for Pod Protection

Description	HTTP Method or Custom Operation	Resource URI
Get Pod Protection	GET	{apiRoot}/BSF/nf-common-component/v1/igw/podprotection
Update subset of Pod Protection	PATCH	{apiRoot}/BSF/nf-common-component/v1/igw/podprotection
Update Pod Protection	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/podprotection

The sample request body structure for PUT operation is as follows:

```
{
        "enabled": false,
        "monitoringInterval": 100,
        "congestionControl": {
            "enabled": false,
            "stateChangeSampleCount": 10,
            "actionSamplingPeriod": 3,
            "states": [
                {
                    "name": "Normal",
                    "weight": 0,
                    "entryAction": [
                        {
                            "action": "MaxConcurrentStreamsUpdate",
                            "args": {
                                "incrementBy": 30,
                                "incrementByActionSamplingPeriod": 3,
                                "maxConcurrentStreamsPerCon": 100
                            }
                        },
                        {
                            "action": "AcceptIncomingConnections",
                            "args": {
                                "accept": true
                            }
                        }
                    ]
                },
                {
                    "name": "DoC",
                    "weight": 1,
                    "resourceThreshold": {
                        "cpu": 60,
                        "memory": 60,
                        "pendingMessage": 5000
                    },
                    "entryAction": [
                        {
                            "action": "AcceptIncomingConnections",
                            "args": {
                                "accept": false
```

```
                        }
                    },
                    {
                        "action": "MaxConcurrentStreamsUpdate",
                        "args": {
                            "incrementBy": 30,
                            "incrementByActionSamplingPeriod": 3,
                            "decrementBy": 30,
                            "decrementByActionSamplingPeriod": 1,
                            "maxConcurrentStreamsPerCon": 50
                        }
                    }
                ]
            },
            {
                "name": "Congested",
                "weight": 2,
                "resourceThreshold": {
                    "cpu": 75,
                    "memory": 75,
                    "pendingMessage": 7000
                },
                "entryAction": [
                    {
                        "action": "AcceptIncomingConnections",
                        "args": {
                            "accept": false
                        }
                    },
                    {
                        "action": "MaxConcurrentStreamsUpdate",
                        "args": {
                            "decrementBy": 30,
                            "decrementByActionSamplingPeriod": 1,
                            "maxConcurrentStreamsPerCon": 10
                        }
                    }
                ]
            }
        ]
    }
}
```

Table 3-38 Request and Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
enabled	boolean	M	Specifies whether to enable or disable pod protection at Ingress Gateway.
monitoringInterval	integer	M	Specifies the interval (in ms) in which the state of the resource is checked and then updated.

Table 3-38 (Cont.) Request and Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
congestionControl.enabled	boolean	M	Specifies whether to enable or disable congestion control at Ingress Gateway.
congestionControl.stateChangeSampleCount	integer	M	Specifies the number of times the pod must remain in the same state in order to transition to a different state. For instance, if a given pod is in the normal state (weight 0) and the value for this parameter is configured as 10, then the pod must remain in DOC state for 10 consecutive counts before it can transition to the DOC state.
congestionControl.actionSamplingPeriod	integer	M	Specifies the time at which action is performed.
congestionControl.states		M	Specifies the pre-defined congestion states for a pod. The supported values for the state are as follow • Normal • DOC • Congested

Table 3-39 states

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
name	string	M	Specifies the name of the state.
weight	integer	M	Specifies the weight for a state. The criticality of a state is directly proportional to its weight. For example, the resource threshold for weight 0 (Normal) must be less than the resource threshold of weight 1 (DOC). Similarly, the maxConcurrentStreamsPerCon of weight 0 (Normal) must be greater than weight 1 (DOC).
resourceThreshold	integer	O	Specifies the threshold values for CPU, memory, and pending requests at Ingress Gateway for each state.
entryAction.action	string	M	Specifies the action associated with each state. The supported values for this parameter are as follow: • MaxConcurrentStreamsUpdate • AcceptIncomingConnections

Table 3-39 (Cont.) states

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
entryAction.args	array	O	Specifies the args associated with each action type. For the action `AcceptIncomingConnections`, the arg `accept` can be either true or false. For the action `MaxConcurrentStreamsUpdate`, the supported args are as follow: 1. `incrementBy`: possible values (positive integer) 2. `decrementBy`: possible values (positive integer) 3. `maxConcurrentStreamsPerCon`: possible values (positive integer) 4. `decrementByActionSamplingPeriod`: possible values (positive integer) 5. `incrementByActionSamplingPeriod`: possible values (positive integer)

3.10 User-Agent Header

3.10.1 Configuration for User-Agent Header Generation at Egress Gateway

This section describes the URIs that you can configure for user-agent header generation at Egress Gateway.

The configuration to enable and disable the generation of the user-agent header can be done using REST API exposed by the config-service when sending the following JSON body.

Table 3-40 Supported REST APIs for User-Agent Generation

Description	HTTP Method or Custom Operation	Resource URI
PUT User-Agent Generation	PUT	http://<config-service IP>:<config-service PORT>/bsf/nf-common-component/v1/egw/useragentheader

CURL command for PUT Operation: `curl -X PUT http://10.75.232.35:8000/bsf/nf-common-component/v1/egw/useragentheader -H "Content-Type: application/json" -d`

The sample request body structure for PUT operation is as follows:

```
{
     "enabled": true,
```

```
    "nfType": "BSF",
    "nfInstanceId": "fe7d992b-0541-4c7d-ab84-c6d70b1b0555",
    "nfFqdn": "pcf.oracle.org",
    "addFqdnToHeader": true,
    "overwriteHeader": false
}
```

Table 3-41 Request Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
egress-gateway.userAgentHeaderConfigMode	String	M	This parameter is used to accept the user-agent configurations from Helm or REST.
egress-gateway.userAgentHeader.enabled	Boolean	M	Specifies whether the feature is enabled or disabled. By default, the value is set to false.
egress-gateway.userAgentHeader.nfType	String	M	This parameter holds the nfType that will be used to generate the user agent header.
egress-gateway.userAgentHeader.nfInstanceId	String	M	This parameter represents the UUID of the CNPCF deployment that will be used to generate the user agent header.
egress-gateway.userAgentHeader.addFqdnToHeader	Boolean	M	This parameter specifies if the user agent will use the FQDN information under the module to append it when generating the user agent header.The default value is set to 'false' meaning that the FQDN information will not be encoded into the user agent header during its generation. By default, the value is set to false.
egress-gateway.userAgentHeader.nfFqdn	String	O	This is an optional parameter and can be present or not, if operators want to include the FQDN string configured under this section then the parameter userAgentHeader.addFqdnToHeader needs to be enabled.
egress-gateway.userAgentHeader.overwriteHeader	Boolean	M	This parameter specifies if the the user agent header is sent or not.

3.10.2 Configuration for User-Agent Header Validation at Ingress Gateway

This section describes the URIs that you can configure for user-agent header Validation at Ingress Gateway.

The configuration to enable and disable the validation of the user-agent header can be done using REST API exposed by the config-service when sending the following JSON body.

Table 3-42 Supported REST APIs for User-Agent Validation

Description	HTTP Method or Custom Operation	Resource URI
PUT User-Agent Validation	PUT	http://<config-service IP>:<config-service PORT>/bsf/nf-common-component/v1/igw/useragentheadervalidation

CURL command for PUT Operation: `curl -X PUT http://10.75.192.253:8000/bsf/nf-common-component/v1/igw/useragentheadervalidation -H "Content-Type: application/json"`

The sample request body structure for PUT operation is as follows:

```
{
   "enabled": true,
   "validationType": "relaxed",
   "consumerNfTypes": [
      "PCF","AF","NEF"
   ]
}
```

Table 3-43 Request Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
ingress-gateway.userAgentHeaderValidationConfigMode	String	M	This flag is used to accept the user-agent configurations from Helm or REST.
ingress-gateway.userAgentHeaderValidation.enabled	Boolean	M	Specifies the type of validation that will be taken into consideration when processing the values born on the user agent header.
ingress-gateway.userAgentHeaderValidation.validationType	String	M	Specifies the type of validation that will be taken into consideration when processing the values on the user agent header.
ingress-gateway.userAgentHeaderValidation.consumerNfTypes	String	M	Compares the NF Type born in the user agent header present in the incoming requests towards BSF's Ingress Gateway.

3.11 Controlled Shutdown at Ingress and Diameter Gateway

This section describes the URIs that you can use to enable and configure Controlled Shutdown at Ingress and Diameter Gateway.

Operational State

The following table describes the URIs available to define and retrieve operational state:

Table 3-44 Supported REST APIs for Operational State

Description	HTTP Method or Custom Operation	Resource URI
GET Operational State	GET	{apiRoot}/oc-bsf-configuration/v1/controlledshutdown/operationalState
PUT Operational State	PUT	{apiRoot}/oc-bsf-configuration/v1/controlledshutdown/operationalState

The sample request body structure for PUT operation is as follows:

```
{
  "operationalState": "NORMAL"
}
```

Table 3-45 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
Operational State	Enum • NORMAL • PARTIAL_SHUTDOWN • COMPLETE_SHUTDOWN	M	Specifies the operational state

Operational State History

The following table describes the URIs available to retrieve operational state history:

Table 3-46 Supported REST APIs for Operational State History

Description	HTTP Method or Custom Operation	Resource URI
GET Operational State History	GET	{apiRoot}/oc-bsf-configuration/v1/controlledshutdown/operationalStateHistory

The sample request body structure for GET operation is as follows:

```
[
  {
    "id": "ea01053b-5a3b-4de2-850b-7210bf2a04d5",
    "type": "operationalState",
    "value": "{\"state\":\"NORMAL\"}",
    "timeStamp": "2022-08-30T08:12:45.88519",
    "status": "SUCCESS"
  }
]
```

Table 3-47 Request/Response Body Parameters

Field Name	Data Type	Description
id	UUID	Auto-generated ID
type	String	Type of historical data
value	String	Operational state value
timeStamp	Date	Logs the timestamp when the operational state event took place
status	String	• Success: Successful in switching of operational state • Failure: Fail in switching of operational state

Table 3-48 Request Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
Offset	Integer	O	Offset is a position in the set of records.
Limit	Integer	O	Limit as an option allows to limit the number of rows returned from a query.
Page	Integer	O	Page shows the set of records based on the limit. If the limit is not provided the page will fetch all the records.

> **Note**
>
> If offset and Limit are not provided in the API, then the query fetches all the records from the database.

Controlled Shutdown Error Mapping

The following table describes the URIs available to define and retrieve Controlled Shutdown Error Mapping:

Table 3-49 Supported REST APIs for Controlled Shutdown Error Mapping

Description	HTTP Method or Custom Operation	Resource URI
PUT Controlled Shutdown Error Mapping	PUT	{apiRoot}/BSF/nf-common-component/v1/igw/controlledshutdownerrormapping

The sample request body structure for PUT operation is as follows:

```
{
    "routeErrorProfileList": [
        {
            "errorProfileName": "ERR_100",
            "routeIds": [
                "reverse_nrf_notify_service",
"bsf_management_register"
            ]
        }
    ]
}
```

> **Note**
>
> Here, the routeId attribute must be the first field.

Table 3-50 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
routeErrorProfileList	Array	M	Specifies the route error profile list.

Table 3-50 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
routeErrorProfileList.routeIDs	Array	M	Specifies the route ID. You can define the server header at route level for any of the following supported route IDs: • bsf_management_register • bsf_management_deregister • bsf_management_discovery • reverse_nrf_notify_service
routeErrorProfileList.errorProfileName	String	M	Specifies the error code profile.

Message Type

The following table describes the URIs available to define and retrieve Message Type:

Table 3-51 Supported REST APIs for Message Type

Description	HTTP Method or Custom Operation	Resource URI
GET Message Type	GET	{apiRoot}/oc-bsf-configuration/v1/diameter/controlledshutdown/errormappings/{messageType}
PUT Message Type	PUT	{apiRoot}/oc-bsf-configuration/v1/diameter/controlledshutdown/errormappings/{messageType}

The sample request body structure for PUT operation is as follows:

```
{
  "messageType": "CER",
  "ansWithResultCode": "CUSTOM_RESULT_CODE",
  "resultCode": "7899",
  "useExperimentalResultCode": true,
  "vendorId": "2"
}
```

Table 3-52 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
messageType	String	M	Rx _AAR_I and Rx_AAR_U, STR, RAR, ASR, and CER.
ansWithResultCode	Enum The supported values are: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • CUSTOM_RESULT_CODE	M	Specifies the result code, returned in the answer response.
resultCode	Integer	M	Specify a value for this parameter when you choose `CUSTOM_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the custom result code, which is returned in the answer response. .
useExperimentalResultCode	Boolean	O	Specify a value for this parameter when you choose `CUSTOM_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the value of result code by user according to their requirement. Result code associates with the vendor ID, when the useExperimentalResultCode is true.
vendorId	Integer	O	Specify a value for this parameter when you choose `CUSTOM_RESULT_CODE` value for the `ansWithResultCode` parameter and `useExperimentalResultCode` is true.

Export/Import

The following table describes the URIs available to define and retrieve Export/Import:

Table 3-53 Supported REST APIs for Export/Import

Description	HTTP Method or Custom Operation	Resource URI
GET Export	GET	{apiRoot}/oc-bsf-configuration/v1/diameter/controlledshutdown/errormappings/export
Put Import	PUT	{apiRoot}/oc-bsf-configuration/v1/diameter/controlledshutdown/errormappings/import

The sample response body structure for PUT operation is as follows:

```
"exportData": [
    {
      "messageType": "Rx_AAR_I",
      "ansWithResultCode": "CUSTOM_RESULT_CODE",
      "useExperimentalResultCode": false,
      "resultCode": "1300"
    },
    {
      "messageType": "Rx_AAR_U",
      "ansWithResultCode": "DIAMETER_TOO_BUSY",
      "useExperimentalResultCode": false
    },
    {
      "messageType": "STR",
      "ansWithResultCode": "CUSTOM_RESULT_CODE",
      "useExperimentalResultCode": true,
      "resultCode": "2109",
      "vendorId": "1"
    }
```

Table 3-54 Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
messageType	String	M	Type of the request

Table 3-54 (Cont.) Request/Response Body Parameters

Field Name	Data Type	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
ansWithResultCode	Enum The supported values are: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • CUSTOM_RESULT_CODE	M	Specifies the result code, returned in the answer response.
resultCode	Integer	M	Specify a value for this parameter when you choose `CUSTOM_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the custom result code, which is returned in the answer response. .
useExperimentalResultCode	Boolean	O	Specify a value for this parameter when you choose `CUSTOM_RESULT_CODE` value for the `ansWithResultCode` parameter. Specifies the value of result code by user according to their requirement. Result code associates with the vendor ID, when the useExperimentalResultCode is true.
vendorId	Integer	O	Specify a value for this parameter when you choose `CUSTOM_RESULT_CODE` value for the `ansWithResultCode` parameter and `useExperimentalResultCode` is true.

3.12 NF Scoring for a Site

The following table describes the URI available to define NF Scoring:

Table 3-55 NF Scoring

Description	HTTP Method or Custom Operations	Resource API
GET for NF Score	GET	*/oc-bsf-configuration/v1/nfscore*

Table 3-56 Fields

Field Name	Mandatory (M)/ Optional(O)/ Conditional(C)	Datatype	Description
NF Score	M	Float	The score of a site based on NF-specific factors (metrics, alerts, and so on).
detailedReport	M	NA	Detailed report of NFScore calculation.
scoringFactors	M	NA	Comprises the factors that contributed to the NFScore
criteria	C	NA	Factors involved in NFScore calculation Criteria are present for a specific factor If it is enabled for NF-Scoring.
maxScore	C	Integer	Max score of that factor maxScore is present for a specific factor If it is enabled for NF-Scoring.
calculatedScore	C	Float	calculated score of that factor calculatedScore are present for a specific factor If it is enabled for NF-Scoring.
additionalInfo	O	NA	additional info related to factor's score calculation.
configuredValue	C	Integer	An expected value configured for a factor configuredValue is present for a specific factor If it is enabled for NF-Scoring.
actualValue	C	Float	An actual value for a particular factor after doing factor-specific configuration. actualValue is present for a specific factor If it is enabled for NF-Scoring.
totalSvcs	C	Integer	Total configured services. totalSvcs is present when the factor SVC-Health is enabled

Table 3-56 (Cont.) Fields

Field Name	Mandatory (M)/ Optional(O)/ Conditional(C)	Datatype	Description
upSvcs	C	Integer	Total running services. upSvcs is present when the factor SVC-Health is enabled
totalSites	C	Integer	Total configured sites totalSites is present when the factor replicationHealth is enabled.
availableLinks	C	Integer	Total healthy sites availableLinks is present when the factor replicationHealth is enabled.
critical	C	Integer	Critical alert's contribution to alert's calculated score This attribute is present when ActiveAlerts are enabled as NF-Scoring factor
major	C	Float	Major alert's contribution to alert's calculated score This attribute is present when ActiveAlerts are enabled as NF-Scoring factor
minor	C	Float	Minor alert's contribution to alert's calculated score This attribute is present when ActiveAlerts are enabled as NF-Scoring factor
failedFactors	C	Float	Enabled factors that failed to contribute to NFScore This attribute is present when an application fails to calculate the score for 1 or more factors.
detail	C	NA	Factor's failure reason This attribute is present when there are 1 or more failed factors.

Note: When the 'Enable' flag is true for any criteria, then its related fields will be shown.

Sample Response Body for GET for NF Score:

```
{
  "NFScore": 129,
  "detailedReport": {
    "scoringFactors": [
      {
        "criteria": "tps",
        "maxScore": 100,
        "calculatedScore": 75,
        "additionalInfo": {
          "configuredValue": 4000,
          "actualValue": 3000
        }
      },
      {
        "criteria": "serviceHealth",
        "maxScore": 100,
        "calculatedScore": 70,
        "additionalInfo": {
          "totalSvcs": 10,
          "upSvcs": 7
        }
      },
      {
        "criteria": "signallingConnections",
        "maxScore": 100,
        "calculatedScore": 50,
        "additionalInfo": {
          "configuredValue": 50,
          "actualValue": 25
        }
      },
      {
        "criteria": "replicationHealth",
        "maxScore": 100,
        "calculatedScore": 50,
        "additionalInfo": {
          "totalSites": 3,
          "availableLinks": 1
        }
      },
      {
        "criteria": "localityPreference",
        "maxScore": 100, #remove
        "calculatedScore": 100
      },
      {
        "criteria": "activeAlert",
        "score": -30,#rename to "calculatedScore"
        "additionalInfo": {
          "critical": -10,
          "major": -20,
          "minor": 0
        }
      }
```

```
      ]
    },
    "failedFactors": [
      {
        "criteria": "replicationHealth",
        "detail": "failed to calculate replicationHealth score"
      }
    ]
}
```