

Contrail Service Orchestration (CSO) HTTP API Reference and Developer Guide

Version 6.1.0, API Documentation, Modified Jul 28, 2021.

Table of Contents

CSO HTTP API Reference and Developer Guide

Copyright

1. Introduction

1.1. Before You Begin

1.2. Related Information

1.3. Understanding REST and RPC for HTTP APIs

1.4. Microservice APIs

1.4.1. YANG Components

1.4.2. Microservice YANG Example

1.4.3. Obtaining Component Information

1.4.4. Obtaining Item Information

2. CSO and NSC

2.1. API Basics

2.1.1. CSO Services REST Interface Architecture

2.1.2. API Considerations for Performing RPC Operations

2.1.3. Authentication Using Keystone

2.1.4. Monitoring Long-Running Jobs

2.1.5. API Categories

2.2. CSO and NSC API Background Information

2.2.1. Enterprise Networking Model

2.2.2. Site Property Hierarchy

2.3. Enterprise Object Relationship

2.4. Role-Based Access Control

2.4.1. Creating a User with One Custom Service Provider Role

2.4.2. Creating a User with Two Custom Service Provider Roles

2.4.3. Creating a User with One Tenant Role and One Service Provider Role at the Service Provider Level

2.4.4. Creating a User with One Tenant Role at the Tenant Level

2.4.5. Creating a User with Two Tenant Roles at the Tenant Level

2.4.6. Editing a User at the Tenant Level

2.4.7. Deleting a User at the Tenant Level

2.4.8. Deleting a User at the Service Provider Level

2.4.9. Editing a User at the Service Provider Level

2.4.10. Creating a Service Provider Role with Multiple Capabilities

- 2.4.11. Creating a Tenant Role on Service Provider Level with Single Capability
 - 2.4.12. Editing a Role
 - 2.4.13. Deleting a Role
 - 2.4.14. Accepting Usage Policy
- 2.5. Operating Company
 - 2.5.1. Creating an Operating Company
 - 2.5.2. Deleting an Operating Company
- 2.6. Distributed Services Deployment (SD-WAN)
 - 2.6.1. Distributed Services Deployment Workflow
 - 2.6.2. API Examples: Configuring the Enterprise Network
 - 2.6.3. API Examples: Viewing the Current Operational State of the System
 - 2.6.4. Notifications
 - 2.6.5. Notifications using Server Sent Events (SSE)
 - 2.6.6. Using Audit Logs for Information Retrieval
 - 2.6.7. Getting the list of Audit Logs
 - 2.6.8. Purging and archiving Audit Logs
 - 2.6.9. Displaying uCPE Device Alert Information
 - 2.6.10. Device Profile
- 2.7. Site Template
 - 2.7.1. Overview
 - 2.7.2. Creating a site using Site Templates
 - 2.7.3. Reading a site using Site Templates
 - 2.7.4. Updating a site using Site Templates
 - 2.7.5. Deleting a site using Site Templates
 - 2.7.6. Creating Spoke Site using Site Templates
- 3. NextGen FireWall (NGFW) Deployment
 - 3.1. Overview
 - 3.2. Configuring a Site
- 4. Service Assurance
 - 4.1. Overview
 - 4.2. Glossary
 - 4.3. Alarm Life Cycle
 - 4.3.1. Device Goes Down
 - 4.3.2. Device Restarts Successfully
 - 4.4. Supported Alarms in CSO
 - 4.4.1. Device Down/Unreachable

- 4.4.2. Cluster Down
- 4.4.3. DHCP Address Change Notification
- 4.4.4. WAN Interface Down
- 4.4.5. OAM IPSec Tunnel down
- 4.4.6. Overlay Tunnel Down
- 4.4.7. Underlay BGP Session Down
- 4.4.8. Dual homed Underlay BGP Session Down
- 4.4.9. Site Monitoring Stopped
- 4.4.10. VRR Down
- 4.4.11. Combined Alarm for “alarms present in the device”
- 4.4.12. Site-Edit Failure Alarm
- 4.4.13. Site-Edit Alarm for “DHCP Update”
- 4.4.14. DVPN tenant tunnel threshold exceeded Alarm
- 4.4.15. Provider-HUB Alarms
- 4.5. Main attributes of alarms payload
- 4.6. Few Examples for fetching alarm objects
 - 4.6.1. Get all active alarms for a tenant
 - 4.6.2. Get all active alarms for a site
 - 4.6.3. Get history of alarms for a tenant
 - 4.6.4. Get history of alarms for a site
 - 4.6.5. Filters Based on Alarm Attributes
 - 4.6.6. API Result Pagination
- 4.7. Alarm Payloads (JSON)
 - 4.7.1. Device Down/Unreachable
 - 4.7.2. Cluster Down
 - 4.7.3. DHCP Address Change Notification
 - 4.7.4. WAN Interface Down
 - 4.7.5. OAM IPSec Tunnel down
 - 4.7.6. Overlay Tunnel Down (GRE)
 - 4.7.7. Overlay Tunnel Down (GRE_Over_IPSec)
 - 4.7.8. Underlay BGP Session Down
 - 4.7.9. Dual Homed Underlay BGP Session Down
 - 4.7.10. Monitored Object Deleted
 - 4.7.11. VRR Down
 - 4.7.12. Combined Alarm For “alarms present in the device”
 - 4.7.13. Site-Edit Failure Alarm

4.7.14. Site-Edit Alarm for “DHCP Update”

4.7.15. DVPN Tenant Tunnel Threshold Exceeded Alarm

4.8. Performance Management

4.8.1. Overview

4.8.2. Service Metrics

4.8.3. Traffic Metrics

4.8.4. SLA Metrics

4.9. SDWAN Events

4.9.1. Overview

4.9.2. Dynamic VPN

4.9.3. Get DVPN events for a given site

4.9.4. Get DVPN events for a given time range

4.9.5. Link switch

4.9.6. Get link switch events for a given site

4.9.7. Get link switch events for a given time range

4.10. Upstream Notifications From CSO

4.10.1. Server-Sent Events

4.10.2. Syslog forwarding

5. Security Management RESTful API Reference and Logging

6. Glossary

7. API Reference

CSO HTTP API Reference and Developer Guide

Copyright

Juniper Networks, Inc.

1133 Innovation Way Sunnyvale, California 94089 USA

408-745-2000

www.juniper.net

Copyright © 2021, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

1. Introduction

Juniper® Contrail® Service Orchestration and Network Service Controller APIs offer the same capabilities that are available through the Contrail Service Orchestration (CSO) GUI.

This document is intended for application developers, software developers, and system administrators using CSO APIs to orchestrate processes for developing portals, applications, and automation.

Contrail Service Orchestration includes two key components: the Network Service Orchestrator and the Network Service Controller (NSC). Distributed deployments handle service orchestration using the CSO Network Service Controller (NSC). The NSC is a distributed domain controller that manages customer premises equipment (CPE) devices at multiple locations for enterprise customers.

The following CSO components connect to the CSO Network Service Orchestrator through the CSO's RESTful APIs:

- Administration Portal
- Customer Portal

This document is designed to help you get started with the CSO APIs.

1.1. Before You Begin

Before you begin, you must understand the following:

- CSO component architecture.
- RESTful and RPC-based HTTP API architecture.
- Message queuing and RabbitMQ message bus, to work with service assurance APIs.
- Provisioning the virtual machines (VMs) for the CSO node or server.
- Determining the size of the deployment.
- IP address of the VM.
- The fully qualified domain name (FQDN) of each Network Time Protocol (NTP) server.
- Single sign-on for Administrator Portal.

- Using transport layer security (TLS) to encrypt data.
- Using the OpenStack Keystone authentication service or an external Keystone service for authentication of CSO operations.
- IP addresses and default values of the microservices in the central region and in each regional region.

For more information, see **Before You Begin**

(https://www.juniper.net/documentation/en_US/cso5.4/topics/task/installation/cso-solution-installation.html).

1.2. Related Information

The following guides provide information on the CSO installation, upgrade, and deployment:

- **Contrail Service Orchestration Installation and Upgrade Guide**
(https://www.juniper.net/documentation/en_US/cso6.1.0/information-products/pathway-pages/cso-install-and-upgrade-guide.html)
- **Contrail Service Orchestration Deployment Guide**
(https://www.juniper.net/documentation/en_US/cso6.1.0/information-products/pathway-pages/deployment-guide.html)
- **Contrail Service Orchestration Monitoring and Troubleshooting Guide**
(https://www.juniper.net/documentation/en_US/cso6.1.0/information-products/pathway-pages/monitoring-troubleshooting-guide.html)

1.3. Understanding REST and RPC for HTTP APIs

The CSO HTTP APIs are available through endpoints to which you can send HTTP requests. For each operation that maps to a remote procedure call (RPC), the request pattern is as follows:

- HTTP-method: Specifies the type of operation. The methods can be: GET, PUT, POST, or DELETE.
- Body: Includes the JavaScript Object Notation (JSON) object with "input" as root.
- Response: Begins with the parent parameter "output".

The following sample request illustrates the pattern of an RPC request and its response:

POST /device-connectivity/disconnect-device

JSON

JSON Object Input

```
{
  "input" : {
    "connectionid" : "string",
    "deviceid" : "string",
    "webhook" : {
      "url" : "string"
    }
  }
}
```

Sample Response

```
{
  "output" : {
    "requestid" : "string"
  }
}
```

1.4. Microservice APIs

The CSO HTTP APIs are generated from a YANG model that enables descriptions of the available resources and functionality.

1.4.1. YANG Components

Each YANG file contains the following components:

- Resources: objects
- RPC: actions

1.4.2. Microservice YANG Example

Understanding the structure of YANG modeling files helps you use the APIs.

The following example uses "bank" as the module (object) to illustrate the YANG file structure for CSO microservices.

When using the CSO APIs, you do not use or access the YANG files directly. You work with JSON-formatted responses and send JSON-formatted request bodies with the corresponding structures.

```
module bank {
  yang-version 1;
  namespace "http://www.example.net/ns/bank";
  prefix "bank";

  import csp-common { prefix "csp"; }

  import ietf-yang-types {
    prefix yang;
  }

  organization "<organisation name>";
  description "bank";
  revision 2015-05-25 {
    description "Initial version";
  }

  list account {
    uses csp:entity;
    csp:vertex;
    key name;
    leaf balance {
      type uint32;
    }
    leaf first-name {
      type string;
    }
    leaf last-name {
      type string;
    }
    leaf age {
      type uint32;
    }
    leaf gender {
      type enumeration {
        enum M;
        enum F;
      }
    }
  }
  list phone {
    csp:has-edge;
    key uuid;

    leaf uuid {
      type leafref {
        path "../.../phone/uuid";
      }
    }
  }
}
```

```

    list user {
        csp:ref-edge;
        key uuid;

        leaf uuid {
            type leafref {
                path "../../user/uuid";
            }
        }
    }

    container credit {
        uses credit-info;
    }
}

grouping credit-info {
    leaf credit_name {type string;}
    leaf credit_score {type uint32;}
    leaf current_credit_cards {type uint32;}
    anyxml data {
        description "test";
    }
}

list user {
    description "A list of users in the system.";
    uses csp:entity;

    ordered-by user;
    config true;
    key "name";

    leaf user-type {
        type string;
    }
    leaf full-name {
        type string;
    }
}

rpc transfer {
    description "Synchronize service instance with JSM.";
    input {

        leaf accountid {
            type yang:uuid;
        }

        leaf amount {

```

```

        type uint32;
    }
    container schedule {
        leaf date {type string;}
        leaf bydate {type string;}
        leaf recurring {type boolean;}
    }
}
output {
    leaf status {
        type enumeration {
            enum success;
            //transfer is successful
            enum incomplete_funds;
            //not enough funds for transfer
            enum overdraft;
            //overdraft
        }
    }
}
}
}

rpc deposit {
    description "Deposits a credit to the account.";
    input {
        leaf accountid {
            type yang:uuid;
        }
        leaf amount {
            type uint32;
        }
    }

    output {
        leaf status {
            type string;
        }
        leaf transactionid {
            type yang:uuid;
        }
        leaf current_balance {
            type uint32;
        }
    }
}
}
}

```

1.4.3. Obtaining Component Information

When you send a valid GET request along with the authentication token to the following CSO services, the response provides information about the following services:

- tssm: Tenant, site, and service management
- topology-service: Topology services
- activation-service-central: Activation Service (Central)
- cslm: Certificate Management
- cms-central: Configuration Management Service (Central)
- data-view-central: Data View (Central)
- dms-central: Device Management Service (Central)
- iamsvc-noauth: IAM Utilities
- iamsvc: Identity and Authorization Management
- ims-central: Image Management Service (Central)
- policy-mgmt: Intent-based Policy Management
- inv-central: Inventory Management (Central)
- job-service: Job Service
- pslam: Policy and SLA Management Service
- sd: Security Management
- appvisibility: Security Management - Application Statistics
- ecm: Security Management - Events
- seci: Security Management - Reports
- shared-object: Shared Object
- signature-manager: Signature Manager
- fmpm-provider: Alerts

Table 1 provides information about the different URIs and the services they provide:

Table 1. Component Information

URI	Description

URI	Description
/tssm/customer	Lists all customers in the system
/tssm/site	Lists all sites in the system
/tssm/nfv-service-profile	Lists all service profiles in the system
/tssm/nfv-service-instance	Lists all service instances in the system
/topology-service/pop	Lists all POPs onboarded by the provider

Sample response for request /tssm/customer

```
{
  "customer": [
    {
      "fq_name": ["default-domain", "Customer-VJ", "Customer-VJ"],
      "uuid": "dc3ffc30-1b16-479d-959e-86a0ac9fc9bc",
      "uri": "/tssm/customer/dc3ffc30-1b16-479d-959e-86a0ac9fc9bc"
    }
  ],
  "total": 1
}
```

JSON

1.4.4. Obtaining Item Information

You can obtain information about specific objects, if you have a unique object identifier. To obtain customer details associated with the specified UUID, use the following request:

```
/tssm/customer/dc3ffc30-1b16-479d-959e-86a0ac9fc9bc
```

JSON

To obtain customer details associated with the specified fully qualified name, use the following request:

```
/tssm/customer/dc3ffc30-1b16-479d-959e-86a0ac9fc9bc?detail=true
```

JSON

Sample Response

```
{
  "customer": {
    "tenant_type": "small",
    "parent_uuid": "88f5fb2d-7dd7-412c-afa4-0b1a1ef980ef",
    "parent_type": "project",
    "tenantid": "88f5fb2d7dd7412cafa40b1a1ef980ef",
    "tenant_existed": "created",
    "display_name": "Customer-VJ",
    "name": "Customer-VJ",
    "fq_name": [
      "default-domain",
      "Customer-VJ",
      "Customer-VJ"
    ],
    "uuid": "dc3ffc30-1b16-479d-959e-86a0ac9fc9bc",
    "vpn_id": "6f880de0-930a-43f7-aeb1-5bd03a37da8d",
    "uri": "/tssm/customer/dc3ffc30-1b16-479d-959e-86a0ac9fc9bc",
    "networks": {
      "network": [
        {
          "network_name": "Customer-VJ-l3vpn_l3vpn",
          "vpn_id": "6f880de0-930a-43f7-aeb1-5bd03a37da8d"
        }
      ]
    },
    "deployment_scenario": "managed_wan",
    "parent_uri": "/tssm/project/88f5fb2d-7dd7-412c-afa4-0b1a1ef980ef"
  }
}
```

2. CSO and NSC



The API examples provided in this chapter are meant for illustrative purpose only. For more information about the specific APIs, see **Chapter 7 - API Reference**

Juniper Contrail Service Orchestration (CSO) is a product that is designed to help in the automation of distributed CPE domain as well as the ability to automate centralized provisioning of network services in a data center. CSO is a multitenant solution. It provides the ability to define a tenant topology, add sites to or delete sites from this topology, enable devices to be brought up automatically at the customer site, set up network connections defined in the topology, enable end-user configuration of CPE devices, and monitor devices and link status.

The Network Service Controller (NSC) is a CSO component that provides controller functionality of CSO except for the portals and design tools. The NSC is accessed mainly through APIs. NSC APIs enable third-party orchestrators to build customized portals on top of CSO. Both the CSO and NSC are managed through the same set of APIs.

This document provides an overview of the CSO architecture and the network model used for defining tenant topology, workflows needed to manage a distributed enterprise domain, API description for various workflow operations, and JSON input and output for the APIs.

CSO offers a number of customization possibilities for supporting various devices and connectivity options. Customization is expected to be performed by the Juniper Professional Services team or Juniper Networks-certified system integrators.

Figure 1 provides an overview of the CSO and NSC workflow.

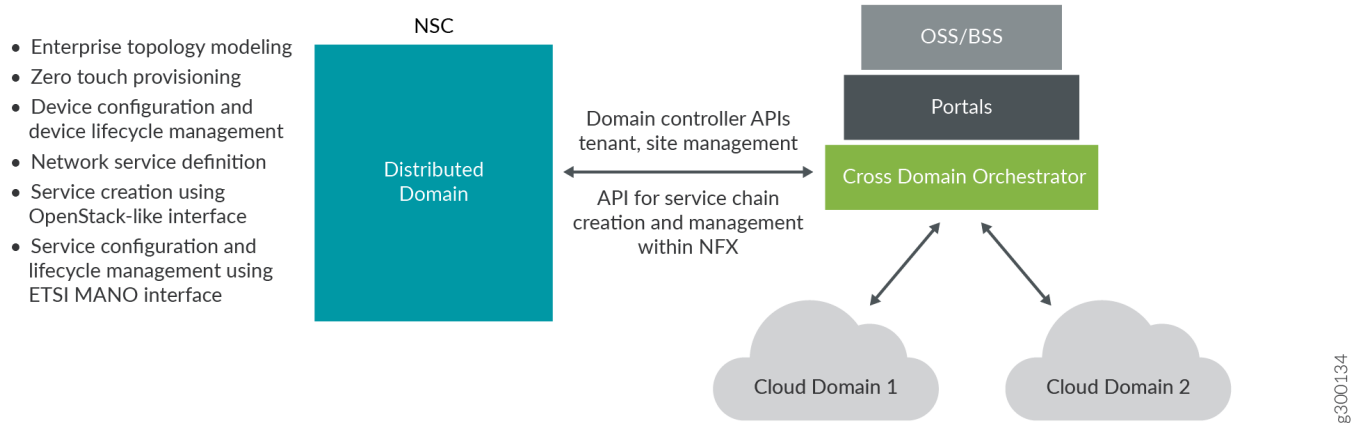


Figure 1. Network Service Controller Workflow

CSO can orchestrate virtualized network functions (VNFs) for both centralized and distributed domains. CSO manages distributed domains by using NSC APIs. The CSO and NSC use APIs to integrate with third-party orchestrators.

If a domain orchestrator uses the domain controller functions of NSC, the following functions are automatically handled by the NSC:

- Topology definition of where an NFX device is placed
- Zero Touch Provisioning (ZTP), of the CPE device at the customer premises
- Device-initiated connection (NFX and VNFs)
- Device management
- Device network connectivity management
- Device element management system (EMS) operations
- Higher-level APIs to instantiate network service chains including configuring, starting, and stopping network services.
- Monitoring device and connectivity functions for FMPM purposes.
- Monitoring VNFs for FMPM purposes

2.1. API Basics

This section provides information about the API basics.

2.1.1. CSO Services REST Interface Architecture

CSO uses microservice architecture. A microservice has YANG object model definition. A microservice exposes its functionality through an HTTP interface:

- Create, read, update, and delete (CRUD) operation on objects.
- RPC actions for complex actions such as creating a tenant or configuring a site.
- Notifications published on RabbitMQ when a certain condition is met.

Each microservice is exposed in a separate HTTP namespace. The generic URL to read an object is:

```
https://ip-address/namespace/object-type[/object-id]
```

JSON

Usually tenant, site and service management (TSSM) is the most common microservice that is used for REST APIs.

Example

The API to read the details of a specific customer:

```
https://ip-address/tssm/customer/<customer object uuid>
```

JSON

2.1.2. API Considerations for Performing RPC Operations

To perform RPC operations, send a POST request (with **auth-token**) to the API server.

Example

An API request to the TSSM microservice along with JSON code in the body that describes the tenant, using two JSON objects for tenant identification and topology type, respectively. The JSON body can contain as many child JSON objects, which describe sites for the tenant, as are needed.

```
/<CSO_Central_MS_ip>/tssm/onboard-tenant
```

JSON

HTTP Headers:

Key	Value
Content-Type	application/json

Key	Value
X-Auth-Token	token

2.1.3. Authentication Using Keystone

Each API request must contain a valid authentication token (**auth-token**).
To obtain an authentication token, send a GET request with the following JSON-formatted payload:

`http://<ip-address-of-Keystone-service>:5000/v3/auth/tokens`

JSON

Sample Request

```
{
  "auth": {
    "identity": {
      "methods": ["password"],
      "password": {
        "user": {
          "domain": {
            "id": "default"
          },
          "name": "{{username}}",
          "password": "{{password}}"
        }
      }
    },
    "scope": {
      "project": {
        "domain": {
          "id": "default"
        },
        "name": "{{project}}"
      }
    }
  }
}
```

JSON

A successful authentication request results in a response containing a response header with an alphanumeric value for the key 'X-Subject-Token:'. The value returned is supplied in all subsequent request headers until the token expires. It is used to authenticate the requests.

2.1.4. Monitoring Long-Running Jobs

Most of the API calls are asynchronous. The API calls returns a job ID. The northbound system is expected to monitor the job for completion status.

To monitor a long-running job, set up polling using GET requests with authentication tokens to your CSO server using the **job-ID**, and check for, the "**status**", "**success**", and "**complete**"* fields.

Send a GET request with authentication token to the CSO server:

```
/<csp-ms-vm>/job-service/job/<job-id>
```

JSON

The response contains information about the job, including start time, domain, job ID, type, and other data as shown in the following example.

Sample Response

```
{
  "job": {
    "status": "success",
    "start_time": 1471656407,
    "job_type": "csp.tssm_onboard",
    "results": "complete",
    "name": "onboard_demo101_csp.tssm_onboard_1471656407.25",
    "fq_name": [
      "default-domain",
      "default-project",
      "onboard_demo101_csp.tssm_onboard_1471656407.25"
    ],
    "uuid": "<job-id>",
    "uri": "/job-service/job/<job-id>"
  }
}
```

JSON

2.1.5. API Categories

CSO, along with its NSC component provides the ability to define a tenant topology, add sites to, or delete sites from this topology, enable devices to be brought up automatically at the customer site, set up network connections defined in the topology, enable end-user configuration of CPE devices, and monitor device and link status.

Almost all of the CSO and NSC functionality is exposed through REST APIs. External applications can interface with CSO and NSC through these APIs.

Table 2 provides information about the categories of the exposed APIs:

Table 2. CSO and NSC API Categories

API	Description
Catalog management	Manage network service descriptors and VNFs
VIM/POP management	Create define and manage VIM and POP data centers
Topology management	Insert and manage end-to-end CPE service topology (logical)
Site/customer creation	Manage customer or site objects and associate them with service topology nodes
Network design APIs	Define virtualized services and service chains
Site activation	Notify vCPE and uCPE device deployment topology and service placement
Identity management	Manage Identity for both enterprise and service provider users
Bootstrap service	Configure and manage device activation service
Device configuration	Define and manage the base configuration of VNF
Service placement/instantiation	Position and manage service chains in the customer topology
Device and service monitoring	Monitor the status of device network services and services topology
Root cause analysis/Troubleshooting	Trace and correlate between events alarms and logs
Zero touch and device management	Activate provision and manage NFX
Image management	Manage NFX device images
SD-WAN	Provision links for auto-VPN Discover VPN and distributed routing

API	Description
Abstracted routing	Create Layer 2 and Layer 3 service chains

2.2. CSO and NSC API Background Information

This section provides background information on the CSO and NSC APIs.

2.2.1. Enterprise Networking Model

Figure 2 illustrates the elements that constitute an enterprise network and how they communicate with each other. The elements represent the automation points in the network. The network services are attached or configured as part of the solution orchestration to form the automation points.

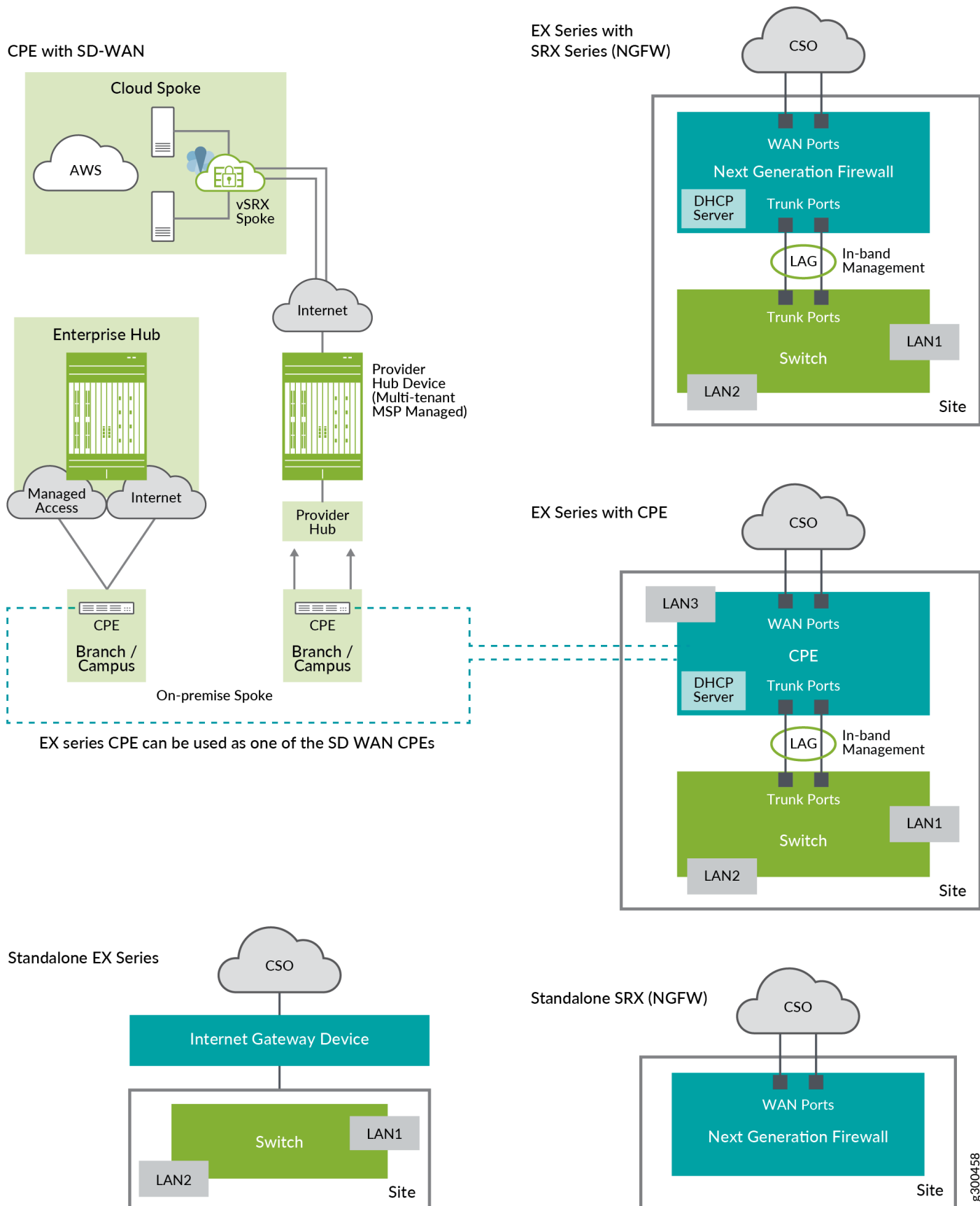


Figure 2. Enterprise Networking Topology

2.2.2. Site Property Hierarchy

The elements in the enterprise topology represent the customer sites based on their location, role, and management properties that is controlled by the NSC as shown in figure 3:

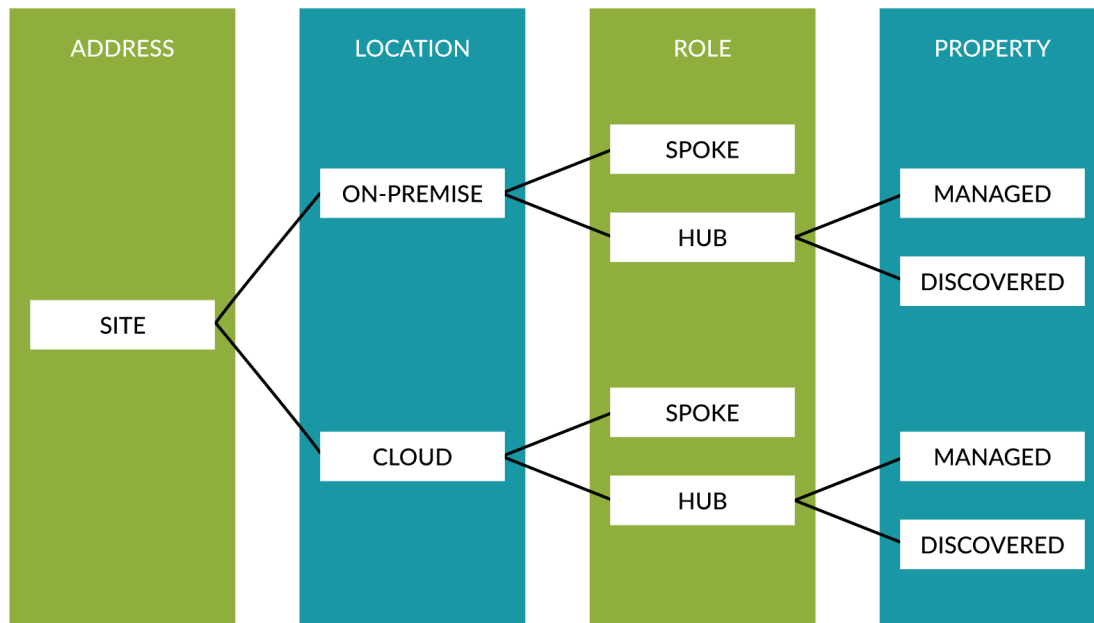


Figure 3. NSC Site Property Hierarchy

The following are the main elements of the enterprise networking topology:

- **On-premise spoke** represents an automation endpoint that is part of customer premises equipment at some physical location such as a branch office or point-of-sale location. Typically, the on-premises spoke sites are connected using overlay connections to all hub sites.
- **Enterprise hub** represents an automation endpoint that is part of customer premises equipment at headquarter or the main branch office, and acts as a hub for overlay connections for many spoke devices.
- **Cloud spoke (AWS)** represents an automation endpoint that is part of a customer's virtual path connection (VPC) in the AWS cloud. Typically, the cloud spoke sites are connected using overlay connections to Enter hub sites.
- **Provider hub (POP)** represents an automation endpoint that is part of a data center of POP location, and acts as a hub for overlay connections from many cloud spoke devices. Provider hubs are usually logical entities in a multitenant device (Provider hub device).

2.3. Enterprise Object Relationship

Enterprise Objects provides tools and frameworks for object-relational mapping. The enterprise objects consist of the following components:

- **Tenant** – High-level object describing a tenant.
- **Site group** – Object describing a group of sites. This object is used to group sites for ease of policy application.
- **Site** – Represents a node location in the enterprise network.
- **Intent policy** – Represents an enterprise-level service-level agreement (SLA) or security policy.
- **Department** – Represents an enterprise-wide object used in intent policies. One or more sites can have references to this object.
- **LAN segment** – Represents a VLAN, port group, or an IP prefix in the CPE device. When a LAN segment refers to its department, any intent policy at department level is moved into site-specific policy.
- **VPN** – Represents a network segment in the enterprise. Network segmentation for a tenant can be configured in the following methods:
 - One department – One VPN. Each VPN represents a network segment in the enterprise.
 - All departments in one VPN - The enterprise has no network segmentation and the enterprise network is part of only one VPN.
- **Device** – Represents the device at the CPE site.
- **Device template** – Represents all the workflow descriptions for automating the device operations including zero-touch provisioning, VNF management, and device Return Material Authorization (RMA).
- **Configuration template** – Represents the configuration templates used in various device workflows.

Figure 4 presents the relationship between the various enterprise objects and highlights the relationship between the various enterprise objects.

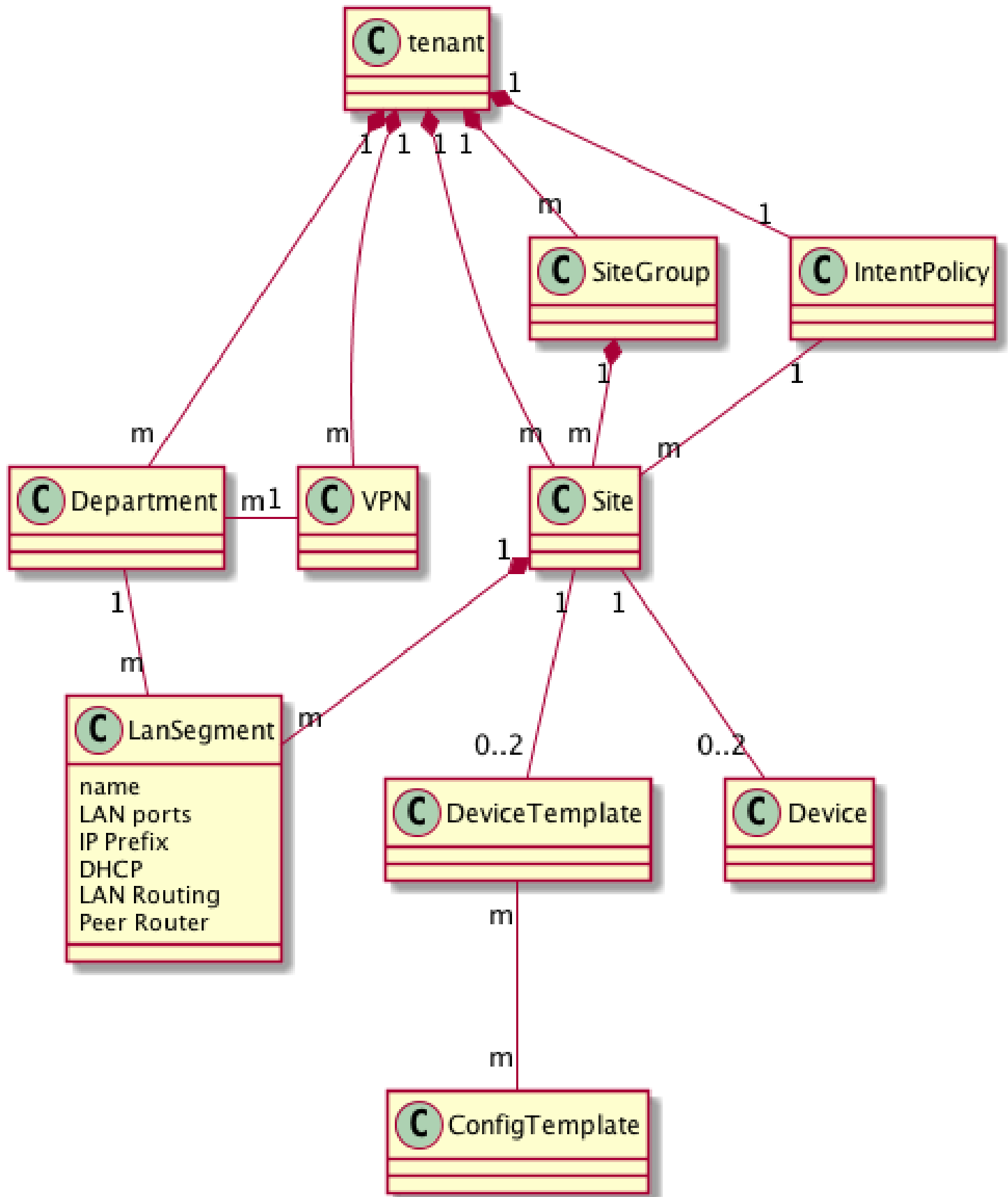


Figure 4. Enterprise Object Relationship

Figure 5 provides information on the enterprise object model.

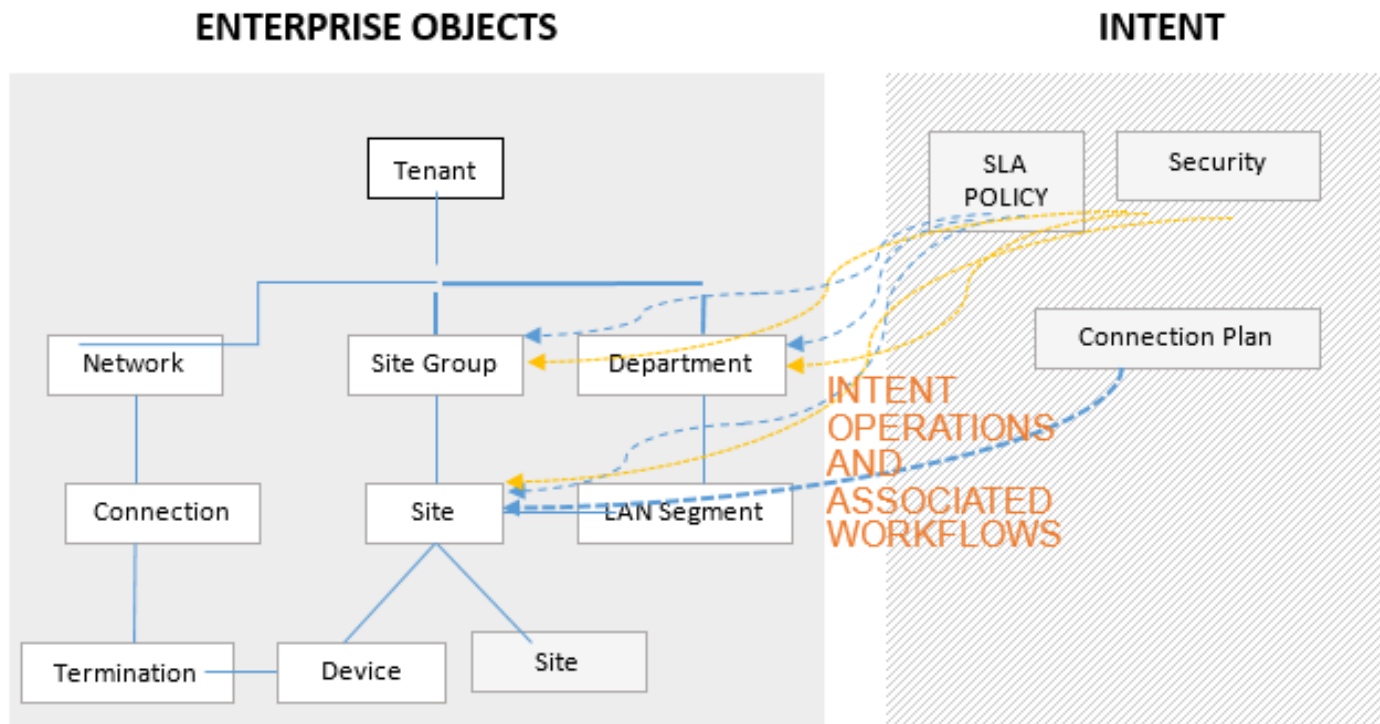


Figure 5. Enterprise Object Model

2.4. Role-Based Access Control

A role defines permissions required by users to perform a set of tasks. The CSO administrator can assign users to one or more roles depending on the tasks that the user is expected to perform. User roles enable you to classify users based on the privileges to perform tasks on CSO objects. Roles assigned to a user determine the tasks and actions that the user can perform.

You can perform the following operations by using the role-based access control (RBAC) APIs:

- Creating a User with One Custom Service Provider Role
- Creating a User with Two Custom Service Provider Roles
- Creating a User with One Tenant Role and One Service Provider Role at the Service Provider Level
- Creating a User with One Tenant Role at the Tenant Level
- Creating a User with Two Tenant Roles at the Tenant Level
- Editing a User at the Tenant Level
- Deleting a User at the Tenant Level
- Deleting a User at the Service Provider Level

- Editing a User at the Service Provider Level
- Creating a Service Provider Role with Multiple Capabilities
- Creating a Tenant Role on Service Provider Level with Single Capability
- Editing a Role
- Deleting a Role

For more information about the different tasks, payload, and response samples see **Identity and Authorization Management**

(https://uat.juniper.net/documentation/en_US/cso4.0/information-products/pathway-pages/API_Guide/iamsvc.html#tag/iamsvc-RPCs)

2.4.1. Creating a User with One Custom Service Provider Role

To create a user with one custom service provider (SP) role, send a POST request with the following JSON-formatted payload:

```
/iamsvc/create-user
```

JSON

JSON Object Input

```
{
  "input": {
    "name": "customUserOneSProle@mail.com",
    "project_role": [
      {
        "project_id": "42736b9c2a1a43509730591f8f1e55af",
        "role_id": "8d04ea55-6d5f-45fe-ae1b-8e7defcfe225"
      }
    ],
    "extra": [
      {
        "name": "first_name",
        "str_value": "customUserOneSProle"
      },
      {
        "name": "last_name",
        "str_value": "customUserOneSProle"
      }
    ],
    "generate_password": true
  }
}
```

JSON

Sample Response

JSON

```
{
  "output":{
    "status":"success",
    "uuid":"6174a1d8-204a-47fd-b8b5-209c7705da49",
    "details":"new_user"
  }
}
```

2.4.2. Creating a User with Two Custom Service Provider Roles

To create a user with two custom SP roles at the SP level, send a POST request with the following JSON-formatted payload:

```
/iamsvc/create-user
```

JSON

JSON Object Input

JSON

```
{
  "input":{
    "name":"customUserTwoSProles@mail.com",
    "project_role":[
      {
        "project_id":"42736b9c2a1a43509730591f8f1e55af",
        "role_id":"8d04ea55-6d5f-45fe-ae1b-8e7defcfe225"
      },
      {
        "project_id":"42736b9c2a1a43509730591f8f1e55af",
        "role_id":"50b0d647-89e8-4d1b-b7b0-397d3ba55e06"
      }
    ],
    "extra":[
      {
        "name":"first_name",
        "str_value":"customUserTwoSProles"
      },
      {
        "name":"last_name",
        "str_value":"customUserTwoSProles"
      }
    ],
    "generate_password":true
  }
}
```

Sample Response

JSON

```
{
  "output": {
    "status": "success",
    "uuid": "6174a1d8-204a-47fd-b8b5-209c7705da49",
    "details": "new_user"
  }
}
```

2.4.3. Creating a User with One Tenant Role and One Service Provider Role at the Service Provider Level

To create a user with one tenant role and one SP role at the SP level, send a POST request with the following JSON-formatted payload:

```
/iamsvc/create-user
```

JSON

JSON Object Input

JSON

```
{
  "input": {
    "name": "customUserOneSProleOneTenantRole@mail.com",
    "project_role": [
      {
        "project_id": "42736b9c2a1a43509730591f8f1e55af",
        "role_id": "8d04ea55-6d5f-45fe-ae1b-8e7defcfff225"
      }
    ],
    "extra": [
      {
        "name": "first_name",
        "str_value": "customUserOneSProleOneTenantRole"
      },
      {
        "name": "last_name",
        "str_value": "customUserOneSProleOneTenantRole"
      }
    ],
    "generate_password": true,
    "project_group_role": [
      {
        "project_group_id": "d3d553b6-1c55-49ee-b255-11ccff028305",
        "role_id": "6f5f91e2-a733-4feb-9775-6b4db3baa6b9"
      }
    ]
  }
}
```

Sample Response

JSON

```
{
  "output": {
    "status": "success",
    "uuid": "6174a1d8-204a-47fd-b8b5-209c7705da49",
    "details": "new_user"
  }
}
```

2.4.4. Creating a User with One Tenant Role at the Tenant Level

To create a user with one tenant role at the tenant level, send a POST request with the following JSON-formatted payload:

```
/iamsvc/create-user
```

JSON

JSON Object Input

JSON

```
{
  "input":{
    "name":"tenantUserOneTenantRole@mail.com",
    "project_role":[
      {
        "project_id":"95058babb1254382bdab758737262aeb",
        "role_id":"6f5f91e2-a733-4feb-9775-6b4db3baa6b9"
      }
    ],
    "extra":[
      {
        "name":"first_name",
        "str_value":"tenantUserOneTenantRole"
      },
      {
        "name":"last_name",
        "str_value":"tenantUserOneTenantRole"
      }
    ],
    "generate_password":true
  }
}
```

Sample Response

JSON

```
{
  "output":{
    "status":"success",
    "uuid":"6174a1d8-204a-47fd-b8b5-209c7705da49",
    "details":"new_user"
  }
}
```

2.4.5. Creating a User with Two Tenant Roles at the Tenant Level

To create a user with two tenant roles at the tenant level, send a POST request with the following JSON-formatted payload:

JSON

```
/iamsvc/create-user
```

JSON Object Input

JSON

```
{
  "input":{
    "name":"tenantUserTwoTenantRoles@mail.com",
    "project_role":[
      {
        "project_id":"95058babb1254382bdab758737262aeb",
        "role_id":"6f5f91e2-a733-4feb-9775-6b4db3baa6b9"
      },
      {
        "project_id":"95058babb1254382bdab758737262aeb",
        "role_id":"d6e984d2-a9fc-43a1-beb8-5ba6b980a02c"
      }
    ],
    "extra":[
      {
        "name":"first_name",
        "str_value":"tenantUserTwoTenantRoles"
      },
      {
        "name":"last_name",
        "str_value":"tenantUserTwoTenantRoles"
      }
    ],
    "generate_password":true
  }
}
```

Sample Response

JSON

```
{
  "output":{
    "status":"success",
    "uuid":"6174a1d8-204a-47fd-b8b5-209c7705da49",
    "details":"new_user"
  }
}
```

2.4.6. Editing a User at the Tenant Level

To edit a user at the tenant level, send a POST request with the following JSON-formatted payload:

JSON

```
/iamsvc/edit-user
```

JSON Object Input

JSON

```
{
  "input":{
    "name":"tenantWithAdmin@mail.com",
    "project_role":[
      {
        "project_id":"95058babb1254382bdab758737262aeb",
        "role_id":"9fe2ff9e-e438-4b18-94a9-0878d3e92bab"
      },
      {
        "project_id":"95058babb1254382bdab758737262aeb",
        "role_id":"c408eca4-6b47-4c6d-8b7f-d5cb4c38bded"
      }
    ],
    "extra":[
      {
        "name":"first_name",
        "str_value":"tenantWithAdminUpdated"
      },
      {
        "name":"last_name",
        "str_value":"tenantWithAdminUPdated"
      }
    ],
    "generate_password":true,
    "uuid":"9fd00b5a-fd17-4e3c-b5e4-b4bdb9cc3261"
  }
}
```

Sample Response

JSON

```
{
  "output":{
    "status":"success",
    "uuid": "a571aa45-9998-41ed-8277-94592a4d37f0",
    "details":""
  }
}
```

2.4.7. Deleting a User at the Tenant Level

To delete a user at the tenant level, send a POST request with the following JSON-formatted payload:

JSON

```
iamsvc/delete-user-if-no-other-project
```

JSON Object Input

JSON

```
{
  "input":{
    "uuid":"9fd00b5a-fd17-4e3c-b5e4-b4bdb9cc3261"
  }
}
```

Sample Response

JSON

```
{
  "output":{
    "status":"success",
    "details":""
  }
}
```

2.4.8. Deleting a User at the Service Provider Level

To delete a user at the SP level, send a POST request with the following JSON-formatted payload:

JSON

```
iamsvc/delete-user-if-no-other-project
```

JSON Object Input

JSON

```
{
  "input":{
    "uuid":"5f3fe710-7a84-45ab-8ee9-9985f1af9bc7"
  }
}
```

Sample Response

JSON

```
{
  "output":{
    "status":"success",
    "details":""
  }
}
```

2.4.9. Editing a User at the Service Provider Level

To edit a user on the SP level, use the following RESTful API with the JSON-formatted payload to:

- Update the first and last names of the user.
- Add a new SP role.
- Add existing roles.
- Add payload.

`iamsvc/edit-user`

JSON

JSON Object Input

```
{
  "input":{
    "name":"userMSPAdmin@mail.com",
    "project_role":[
      {
        "project_id":"42736b9c2a1a43509730591f8f1e55af",
        "role_id":"a9822f8a-598a-4178-a8ee-c86e51e638cd"
      },
      {
        "project_id":"42736b9c2a1a43509730591f8f1e55af",
        "role_id":"fc44c184-a724-42e0-a90d-3324c4419ba5"
      }
    ],
    "extra":[
      {
        "name":"first_name",
        "str_value":"userMSPAdminFirst"
      },
      {
        "name":"last_name",
        "str_value":"userMSPAdminLast"
      }
    ],
    "generate_password":true,
    "project_group_role":[
      {
        "project_group_id":"d3d553b6-1c55-49ee-b255-11ccff028305",
        "role_id":"9fe2ff9e-e438-4b18-94a9-0878d3e92bab"
      }
    ],
    "uuid":"a571aa45-9998-41ed-8277-94592a4d37f0"
  }
}
```

JSON

Sample Response

JSON

```
{
  "output": {
    "status": "success",
    "uuid": "a571aa45-9998-41ed-8277-94592a4d37f0",
    "details": ""
  }
}
```

2.4.10. Creating a Service Provider Role with Multiple Capabilities

To create a service provider role at the SP level with multiple capabilities, use the following RESTful API with the JSON-formatted payload:

```
iamsvc/create-role
```

JSON

JSON Object Input

JSON

```
{
  "input": {
    "name": "customSProle",
    "role_scope": "SP",
    "role_type": "custom",
    "capabilities": [
      "Dashboard:R", "Alert
Definitions:C,R,U,D", "TenantDevices:R,Reboot,PushLicense", "Network
Services:R,Allocate,Detach"
    ],
    "description": "description"
  }
}
```

Sample Response

JSON

```
{
  "output": {
    "status": "success",
    "uuid": "b0790ffc-99f0-47ce-b3ce-9385bc5eeaa",
    "details": ""
  }
}
```

2.4.11. Creating a Tenant Role on Service Provider Level with Single Capability

To create a tenant role at the SP level with single capability, use the following RESTful API with the JSON-formatted payload:

`iamsvc/create-role`

JSON

JSON Object Input

```
{
  "input": {
    "name": "customEnterpriseRole",
    "role_scope": "Enterprise",
    "role_type": "custom",
    "capabilities": [
      "Dashboard:R"
    ],
    "description": "description"
  }
}
```

JSON

Sample Response

```
{
  "output": {
    "status": "success",
    "uuid": "b0790ffc-99f0-47ce-b3ce-9385bc5eeaa",
    "details": ""
  }
}
```

JSON

2.4.12. Editing a Role

To edit a role, use the following RESTful API with the JSON-formatted payload:

`/iamsvc/edit-role`

JSON

JSON Object Input

JSON

```
{
  "input": {
    "uuid": "d0f1c149-05c7-4c34-8ad1-c30ef5ec6efd",
    "capabilities": [
      "Roles:C,R,U,D"
    ],
    "description": "description"
  }
}
```

Sample Response

JSON

```
{
  "output": {
    "status": "success",
    "details": ""
  }
}
```

2.4.13. Deleting a Role

To delete a role, use the following RESTful API with the JSON-formatted payload:

JSON

```
/iamsvc/delete-role
```

JSON Object Input

JSON

```
{
  "input": {
    "uuid": "d0f1c149-05c7-4c34-8ad1-c30ef5ec6efd"
  }
}
```

Sample Response

JSON

```
{
  "output": {
    "status": "success",
    "details": ""
  }
}
```

2.4.14. Accepting Usage Policy

To set the usage policy acceptance information for the current user, use the following RESTful API with the JSON-formatted payload:

`/iamsvc/accept-usage-policy`

JSON

JSON Object Input

```
{
  leaf user_id {
    type yang:uuid;
    description
      "UUID of the user whose usage policy information has to be set.";
  }
  leaf policy_url {
    type yang:uuid;
    description
      "The url for the usage policy accepted";
  }
  leaf policy_id {
    type yang:uuid;
    description
      "The id for the usage policy accepted";
  }
}
```

JSON

Sample Response

```
{
  leaf status {
    type response;
    description
      "Status of the RPC call.";
  }
  leaf details {
    type string;
    description
      "Details of the set user usage policy details, error message if failure occurs.";
  }
}
csp:doc-privacy-lvl "public";
}
```

JSON

2.5. Operating Company

Contrail Service Orchestration (CSO) supports operating companies in a service provider environment. An Operating Company (OpCo) can be created under the Global Service Provider (SP). An OpCo is a region-specific service provider that can create and manage its own tenants and provide services to them. Each OpCo is a subset of the global service provider and functions as a service provider for its own tenants. Each OpCo can use a common CSO instance instead of using its own CSO installation.

You can use RESTful APIs to create or delete an operating company. Use the following APIs to perform specific tasks:

- Creating an Operating Company
- Deleting an Operating Company

2.5.1. Creating an Operating Company

To onboard an operating company, use the following API with the JSON-formatted payload:

`create-opco`

JSON

```
{
  "input": {
    "name": "opco1",
    "use_parent_tenant_users_authentication": true,
    "use_parent_msp_users_authentication": true,
    "password_expiration_interval": 0,
    "admin_user": {
      "name": "jdoe@opco1.com",
      "role_id": [
        "b54a5139-3fbe-48e3-bee0-0a3c2f595c50",
        "9fe2ff9e-e438-4b18-94a9-0878d3e92bab"
      ],
      "first_name": "Joe",
      "last_name": "Doe"
    }
  }
}
```

JSON

Sample Response

JSON

```
{
  "output": {
    "status": "in-progress",
    "reason": null,
    "jobid": "4eb2767e-baca-4571-b943-fade665fca93"
  }
}
```

2.5.2. Deleting an Operating Company

To delete an operating company, use the following API with the JSON-formatted payload:

`delete-opco`

JSON

```
{
  "input": {
    "name": "opco1"
  }
}
```

JSON

Sample Response

```
{
  "output": {
    "status": "in-progress",
    "reason": null,
    "jobid": "af0b7efa-abf2-4583-af51-231eb8ca4543"
  }
}
```

JSON

2.6. Distributed Services Deployment (SD-WAN)

Distributed Service Orchestration is managed through the NSC. You can perform the following tasks by using the RESTful APIs:

- Define tenant topologies
- Add or delete sites to existing topologies
- Control automatic enabling of devices at the customer site
- Set up network connections defined in the topology
- Enable end-user configuration of CPE devices

- Monitor device and link status

2.6.1. Distributed Services Deployment Workflow

Figure 6 provides an overview of a typical end-to-end SD-WAN workflow that the customer administrator is expected to follow.

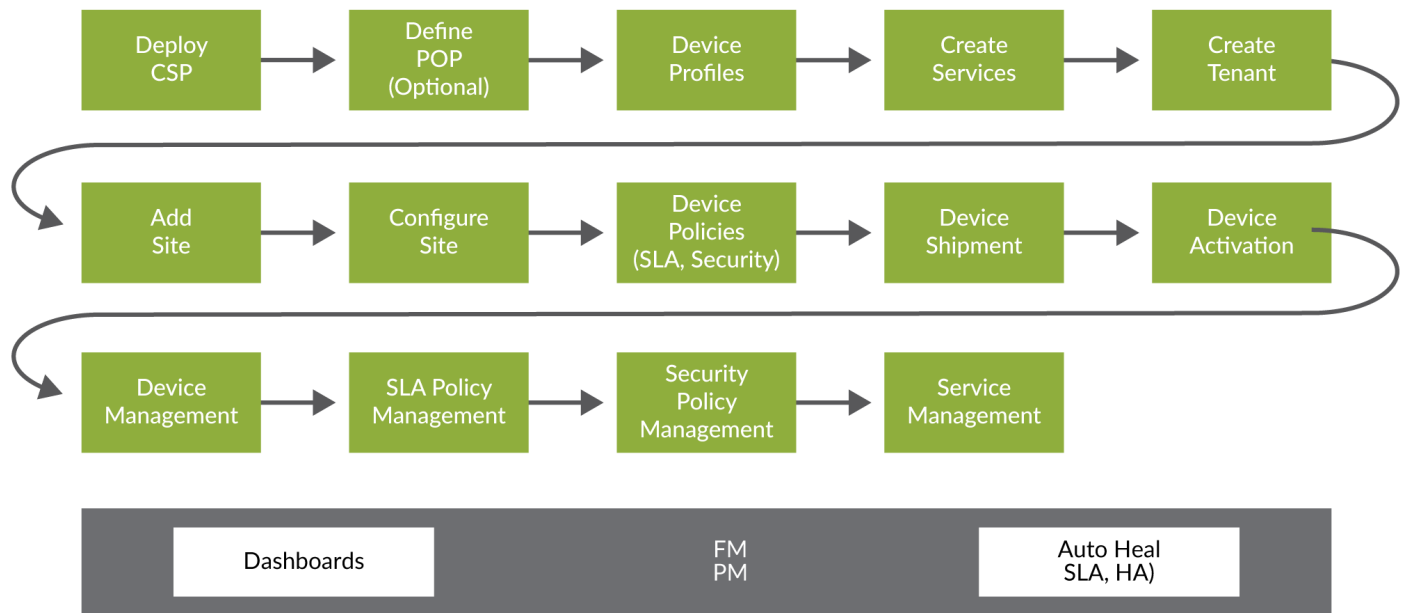


Figure 6. NSC SD-WAN Workflow

An administrator can perform the following SD-WAN workflow tasks:

- **CSP Deployment workflow** - Use this workflow for SD-WAN day-zero preconfiguration, such as creating pre-load device profiles, defining VPN and routing topologies, and preparing relevant configuration templates. The POP workflow also can be preloaded if the customer is a service provider.
- **Device Profile workflow** - Use this workflow to load device profiles, which provide information about the device type, connectivity options for the site, and initial configuration workflow data.
- **Network Service Package workflow** - Use this workflow to load the service package that are defined using designer tools and configuration templates.
- **Create Tenant workflow** - Use this workflow to define tenant-specific parameters, such as topology type and deployment type.

- Create Site workflow - Use this workflow to define site-specific parameters, connectivity plans, topology-related connectivity parameters, and activation parameters.
- Define Policy workflow - Use this workflow to define enterprise-wide SLA and security policies.
- Device Activation workflow - Use this workflow to initially power on the device and enter the code for activation on the portal or device console. When the device is activated, the VPN routing topologies are automatically created. Additionally, if the device (site) is part of any enterprise-wide policies, the device-specific policy rules are automatically loaded onto the device.
- Device Management workflow - Use this workflow to monitor device status and manage Administrator Portal.
- SLA Policy Management workflow - Use this workflow to monitor and manage SLA performance in the Administrator Portal.
- Security Policy Management workflow - Use this workflow to monitor and manage enterprise-wide security policies in Administrator Portal.
- Service Management workflow - Use this workflow to deploy network services on-premise or centralized services in Administrator Portal.



For all workflows, CSO FMPM subsystems continuously monitors fault and performance data and updates the monitoring dashboards. Monitoring dashboards provide visibility into the network performance, service performance, and alert performance data. The FMPM subsystem also feeds data the route manager to continuously adjust network paths to meet SLA targets.

2.6.2. API Examples: Configuring the Enterprise Network

The information provided in this section is applicable only for customer portal development using the CSO and NSC APIs. You can skip this section, if you only need to read the operational state of the system and monitor the system status.

This chapter provides describes the following tasks:

- Importing a POP
- Adding a Provider Hub Device
- Onboarding a Tenant

- Adding a Department
- Creating a Site
- Configuring a Site
- Adding a LAN Segment
- Deleting a LAN Segment
- Adding On-Premise Spoke Site
- Configuring Spoke Site
- Configuring enterprise-hub site
- Activating a Spoke Device
- Upgrading a Site
- Removing a Site
- Deleting a Tenant
- Deleting a POP Object
- Shipping a Device

Importing a POP

To import a POP, send a POST request to your CSO server, with JSON-formatted code in the payload that describes the POP:

```
POST http://<CSO_Central_MS_IP>/tssm/import-pop
```

JSON

JSON Object Input

```
curl -vk -X POST -H "Cache-Control: no-cache" \
-H "X-Auth-Token: bbf35b4c222e47e2848d186c0dfe8e24" \
-H "Content-Type: application/json" \
-d '
{
  "input": {
    "pop": [
      {
        "dc_name": "${regional_name}",
        "name": "${pop_name1}",
        "address": {
          "street": "1134 Innovation Way",
          "city": "Sunnyvale",
          "state": "CA",
          "zip_code": "94089",
          "country": "USA"
        },
        "device": [
          {
            "name": "${pe_device1}",
            "device_ip": "${pe_ip_addr1}",
            "family": "${pe_family}",
            "assigned_device_profile": "${pe_device_profile}",
            "authentication": {
              "username": "${pe_username}",
              "password": "${pe_password}"
            }
          }
        ]
      }
    ]
  }
}
```

Adding a Provider Hub Device

The following example shows how to add a Provider hub device to the system.

To add a provider hub device at Global level, send a POST request to the server with the following JSON-formatted payload:

```
http://<CSO_Central_MS_ip>/tssm/configure-sites
```

JSON Object Input

```

{
  "input": {
    "tenant_name": "default-project",
    "job_name_prefix": "sbmesh-hub1-cl",
    "site": [{
      "on_premise_site_info": {
        "region": "regional",
        "pop": "sbmesh-pop1",
        "site_role": "HUB",
        "ha_info": {
          "ha_topology": "STANDALONE"
        },
      },
      "device": [{
        "wan_link": [{
          "wan_link_type": "MPLS",
          "local_interface": "ge-0/0/2",
          "overlay_tunnel": [],
          "static_ip_assignment": {
            "ip_address": "54.1.22.1/24",
            "gateway_ip": "54.1.22.254"
          },
        },
        {
          "wan_link_type": "MPLS",
          "local_interface": "ge-0/0/3",
          "overlay_tunnel": [],
          "static_ip_assignment": {
            "ip_address": "54.1.23.1/24",
            "gateway_ip": "54.1.23.254"
          },
        },
        {
          "wan_link_type": "Internet",
          "local_interface": "ge-0/0/0",
          "overlay_tunnel": [],
          "static_ip_assignment": {
            "ip_address": "54.1.20.1/24",
            "gateway_ip": "54.1.20.254"
          },
        },
        {
          "wan_link_type": "DATA_ONLY",
          "wan_link_name": "WAN_0",
          "address_assignment": "STATIC",
          "vlan_id": 1120
        }
      ],
    },
  ],
}

```

```

        "wan_link_type": "Internet",
        "local_interface": "ge-0/0/1",
        "overlay_tunnel": [],
        "static_ip_assignment": {
            "ip_address": "54.1.21.1/24",
            "gateway_ip": "54.1.21.254"
        },
        "traffic_type": "DATA_ONLY",
        "wan_link_name": "WAN_1",
        "address_assignment": "STATIC",
        "vlan_id": 1121
    }],
    "device_name": "sbmesh-hub1-cl",
    "device_template":
"Auto_SRX_Advanced_SDWAN_HUB_option_1",
    "device_details": {
        "serial_number": "84a23ab28a47",
        "boot_image": ""
    },
    "vpn_authentication": "preshared_key",
    "oam_traffic": {
        "ip_prefix": "37.0.0.2/32"
    }
    },
    "site_capabilities": "OAM_AND_DATA"
},
"site_name": "sbmesh-hub1-cl",
"user_defined_properties": [{
    "name": "oam-ce-vlan",
    "value": "1129"
}, {
    "name": "oam-ce-intf",
    "value": "ge-0/0/0"
}, {
    "name": "oam-ce-intf-prefix",
    "value": "54.1.29.1/24"
}, {
    "name": "oam-gateway",
    "value": "54.1.29.2"
}, {
    "name": "ebgp_peer_as",
    "value": "54000"
}]
}
}

```

To add an enterprise hub device at Tenant level, send a POST request to the CSO server with the following JSON-formatted payload:

http://<CSO_Central_MS_ip>/tssm/configure-sites

JSON Object Input

```
{
  "input": {
    "tenant_name": "Color",
    "job_name_prefix": "Create-Site-for-Yelow",
    "deployment_scenario": "managed_wan_v2",
    "site": [
      {
        "site_name": "Yelow",
        "cloud_hub_site_info": {
          "hub_device": "Yellow",
          "wan_links": [
            "WAN_5",
            "WAN_2",
            "WAN_0",
            "WAN_1",
            "WAN_3",
            "lo0.0"
          ],
          "pop": "Nature"
        },
        "site_basic_properties": {
          "site_address": {
            "country": "US"
          },
          "site_description": "",
          "site_role": "HUB",
          "cloud_service": "NONE",
          "site_type": "cloud"
        }
      }
    ]
  }
}
```

Onboarding a Tenant

Send a POST request with the authentication token to your CSO server with a JSON-formatted body that describes the tenant using a minimum of two JSON objects, one each for tenant identification and the associated topology type. The JSON body can contain as many child JSON objects as needed to describe sites for the tenant.

To onboard a tenant into the system, send a POST request with the JSON-formatted payload:

POST <http://<ip-addr>/tssm/onboard-tenant>

JSON

JSON Object Input

JSON

```
{
  "input": {
    "tenant_admin": {
      "admin_user_name": "testtenant_admin@testtenant.com",
      "last_name": "admin",
      "admin_user_password": "Juniper123!",
      "first_name": "testtenant",
      "password_expiration_interval": 0
    },
    "tenant_type": "small",
    "tenant_name": "testtenant",
    "password_expiration_radio": "never",
    "departments": [
      {
        "vpn_name": "testtenant_DefaultVPN",
        "department_name": "Default"
      }
    ],
    "deployment": "SDWAN",
    "vpn": [
      {
        "vpn_name": "testtenant_DefaultVPN"
      }
    ],
    "managed_wan_topology_v2": {}
  }
}
```

Adding a Department

To add a department object for a tenant, send a POST request with the following JSON-formatted payload:

http://<CSO_Central_MS_ip>/tssm/add-department-to-site/

JSON

JSON Object Input

```
{
  "input": {
    "sites": [
      "Demo"
    ],
    "departments": [
      "CompanyName-test"
    ]
  }
}
```

Creating a Site

The tenant administrator uses the create site API to add a site object. You need the following information in order to use this API:

- Site name
- Site type
- Site role
- Device template
- WAN and LAN links that needs to be activated on the site devices.

To create a site object for a tenant, send a POST request with the following JSON-formatted payload:

```
https://<cso-host>/tssm/create-sites
```

NOTE: cso-host is the domain name, it changes with the change of instances in CSO.

JSON Object Input

```

{
  "input": {
    "tenant_name": "tenant_15549507",
    "deployment_scenario": "managed_wan_v2",
    "site": [
      {
        "site_name": "s-srx-15549507",
        "site_basic_properties": {
          "local_breakout": {},
          "gatewaySite": false,
          "site_type": "on_premise",
          "cloud_service": "EDGE",
          "site_address": {
            "country": "US",
            "state": "CA",
            "street": "juniper",
            "zip_code": "94085",
            "city": "sunnyvale"
          },
          "device_redundancy": false,
          "network_seg": false,
          "device_template": [
            {
              "wan_link_info": [
                {
                  "wan_link_type": "Internet",
                  "provider": "ATT",
                  "wan_link": "WAN_0",
                  "subscribed_bandwidth": 1000,
                  "exclusive_for_local_breakout": false,
                  "_sys_reserved_row": "273518d4-7c64-dc05-badd-6e681366582c",
                  "cost": 10,
                  "default_link": false,
                  "local_breakout_enabled": false,
                  "cost_currency": "USD",
                  "preferred_breakout_link": false,
                  "backup_link": false
                },
                {
                  "wan_link_type": "Internet",
                  "provider": "COMCAST",
                  "wan_link": "WAN_1",
                  "subscribed_bandwidth": 500,
                  "exclusive_for_local_breakout": false,
                  "_sys_reserved_row": "452d8511-c61b-0d75-3a6c-d7873c174f7a",
                  "cost": 20,
                  "default_link": false,
                  "local_breakout_enabled": false,

```

```

        "cost_currency": "USD",
        "preferred_breakout_link": false,
        "backup_link": false
    }
],
"template_name": "SRX_Advanced_SDWAN_CPE_option_1",
"lan_segment": [
    {
        "department": "D1",
        "dhcp": false,
        "ip_prefix": "10.10.10.10/24",
        "lan_ports": [
            "LAN_4"
        ],
        "lan_segment_name": "lan"
    }
],
"device_name": "s-srx-15549507"
}
],
"0": {
    "department": "D1",
    "dhcp": false,
    "ip_prefix": "10.10.10.10/24",
    "lan_ports": [
        "LAN_4"
    ],
    "lan_segment_name": "lan"
},
"site_role": "SPOKE",
"sla_mgmt": "COARSE",
"device_profile_name": "SRX as SD-WAN CPE",
"site_name": "s-srx-15549507",
"site_group": null,
"site_contact": {
    "phone_number": "514325544",
    "contact_name": "admin",
    "email_address": "a@juniper.net"
},
"dvpn_params": {
    "delete_dvpn_threshold": "1",
    "create_dvpn_threshold": "5"
},
"topology": "Bandwidth Optimized"
}
}
]
}
}
}

```

Configuring a Site

Use the Configure site API to set up the overlay connectivity to the enterprise-hub and the provider-hub sites. Ensure that you have the service provider credentials, in order to configure a site.

To configure a site object for a tenant, send a POST request with the following JSON-formatted payload:

```
https://<cso-host>/tssm/create-sites
```

JSON

NOTE: cso-host is the domain name, it changes with the change of instances in CSO.

JSON Object Input

```

{
  "input": {
    "tenant_name": "tenant_15549507",
    "job_name_prefix": "tenant_15549507-s-srx-15549507",
    "site": [
      {
        "on_premise_site_info": {
          "device": [
            {
              "device_template": "SRX_Advanced_SDWAN_CPE_option_1",
              "is_gateway_site": false,
              "wan_link": [
                {
                  "mesh_tag": [],
                  "overlay_tunnel": [
                    {
                      "peer_info": {
                        "interface_name": "WAN_0",
                        "internet_gw_ip": "10.155.95.254",
                        "peer_device": "s-hub-15549507"
                      },
                      "tunnel_endpoint_role": "SPOKE",
                      "tunnel_type": "GRE_IPSEC",
                      "tunnel_id": 0
                    }
                  ],
                  "wan_link_type": "Internet",
                  "local_interface": "ge-0/0/0",
                  "used_for_oam": true,
                  "nat_info": {
                    "nat_enabled": false
                  },
                  "static_ip_assignment": {
                    "gateway_ip": "10.155.95.254",
                    "ip_address": "192.168.30.2/24"
                  },
                  "local_breakout_enabled": false,
                  "traffic_type": "DATA_ONLY",
                  "vpn": [
                    {
                      "vpn_name": "tenant_15549507_DefaultVPN"
                    }
                  ],
                  "wan_link_name": "WAN_0",
                  "address_assignment": "STATIC",
                  "mesh_overlay_link_type": "GRE_IPSEC"
                }
              ],
              "mesh_tag": [],
              "overlay_tunnel": [

```

```

        {
            "peer_info": {
                "interface_name": "WAN_1",
                "internet_gw_ip": "10.155.95.254",
                "peer_device": "s-hub-15549507"
            },
            "tunnel_endpoint_role": "SPOKE",
            "tunnel_type": "GRE_IPSEC",
            "tunnel_id": 0
        }
    ],
    "wan_link_type": "Internet",
    "local_interface": "ge-0/0/1",
    "used_for_oam": false,
    "nat_info": {
        "nat_enabled": false
    },
    "static_ip_assignment": {
        "gateway_ip": "10.155.95.254",
        "ip_address": "192.168.30.3/24"
    },
    "local_breakout_enabled": false,
    "traffic_type": "DATA_ONLY",
    "vpn": [
        {
            "vpn_name": "tenant_15549507_DefaultVPN"
        }
    ],
    "wan_link_name": "WAN_1",
    "address_assignment": "STATIC",
    "mesh_overlay_link_type": "GRE_IPSEC"
}
],
"device_name": "s-srx-15549507",
"device_family": "juniper-srx",
"device_details": {
    "serial_number": "SIMSRXSPOKE15555457",
    "activation_code": "545454"
},
"oam_traffic": {
    "ip_prefix": "10.155.95.2/32"
}
}
],
"hub_sites": [
    {
        "hub_role": "PRIMARY",
        "hub_name": "s-hub-15549507"
    }
]
],

```

```

    "region": "regional",
    "site_role": "spoke",
    "ha_info": {
      "ha_topology": "STANDALONE"
    },
    "site_name": "s-srx-15549507",
    "properties": {
      "property": [
        {
          "name": "site_advanced_config",
          "value": {
            "timezone": "Africa/Abidjan",
            "nameserver": [
              "8.8.8.8"
            ]
          }
        }
      ]
    }
  }
}

```

Adding a LAN Segment

To add a LAN segment at a site, send a POST request with the following JSON-formatted payload:

```
http://<CSO_Central_MS_ip>/tssm/add-delete-lan-segments/
```

JSON

JSON Object Input

```
{
  "input": {
    "devices": [
      {
        "delete_lan_segments_list": [],
        "lan_segment": [
          {
            "additional_config": {
              "dhcp": {}
            },
            "ip_prefix": "172.27.17.1/24",
            "lan_segment_name": "LAN-test",
            "vlan": 17,
            "lan_ports": [
              "LAN_5"
            ],
            "department": "CompanyName-test",
            "dhcp": false
          }
        ],
        "device_name": "Red_CPE1"
      }
    ]
  }
}
```

Deleting a LAN Segment

To delete a LAN segment from a site, send a POST request with the following JSON-formatted payload:

```
http://<CSO_Central_MS_ip>/tssm/add-delete-lan-segments/
```

JSON Object Input

JSON

```
{
  "input": {
    "devices": [
      {
        "device_name": "nfx150spoke",
        "delete_lan_segments_list": [
          "lans4444",
          "ls556"
        ],
        "lan_segment": [
          ]
        }
      ]
    }
  }
}
```

Activating a Spoke Device

If a spoke device is using zero touch provisioning (ZTP), use the following API to activate the device. This API is expected to be invoked by the tenant administrator. Using this API, the tenant administrator provides the serial number and activation code for the device at a site to the system. This information is used to complete the zero touch provisioning of the device and bring it up to the provisioned state.

To activate a spoke device with ZTP enabled, send a POST request with the following JSON-formatted payload:

```
http://<CSO_Central_MS_ip>/tssm/start-device-bootstrap
```

JSON

JSON Object Input

```
{
  "input": {
    "device_uuid": "asdasdasdasdasd1234sfss",
    "authenticate_device": {
      "serial_number": "ABCDEF3456",
      "activation_code": "121212"
    }
  }
};
```

JSON

To activate a spoke device which does not use ZTP, instead uses an interactive bring-up workflow, send a POST request with the following JSON-formatted payload:

`http://<CSO_Central_MS_ip>/tssm/start-device-bootstrap`

JSON

JSON Object Input

```
{"input": {  
  "device_uuid": "asadasdasd1234"  
}};
```

JSON

Upgrading a Site

Use the **site_upgrade** RESTful APIs to perform the following functions:

- Analyzing the Site Upgrade
- Obtaining the Site Upgrade Analysis Report
- Performing the Upgrade

Analyzing the Site Upgrade

To perform an upgrade analysis for a site, send a POST request with the following JSON-formatted payload:

`http://<CSO_Central_MS_ip>/tssm/analyze_site_upgrade/`

JSON

You can use either the device ID or the site ID as shown:

```
{  
  "input" : {  
    "site_uuids": [  
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",  
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"  
    ]  
  }  
}
```

JSON

or

JSON

```
{
  "input" : {
    "device_uuids":[
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}
```



You can use the device ID to perform the upgrade analysis for enterprise hub devices.

Sample Response

```
{"output": {"report": [], "job_id": "0247ceb9-b097-410f-98b1-289c5302c155", "jobid": "0247ceb9-b097-410f-98b1-289c5302c155"}}
```

JSON

Obtaining the Site Upgrade Analysis Report

To obtain the site upgrade analysis report, send a GET request with the following JSON-formatted payload:

```
/tssm/get_upgrade_analysis_report
```

JSON

You can use either the device ID or the site ID as shown:

```
{
  "input" : {
    "site_uuids":[
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"
    ]
  }
}
```

JSON

or

```
{
  "input" : {
    "device_uuids":[
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}
```

Sample Response

```

{
  output : {
    upgrade_needed : < MANDATORY|OPTIONAL|NOT_NEEDED >,
    upgrade_impact_checks : [
      {
        check_type : IMAGE_SUPPORT
        message : "Support for this image is deprecated"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_SERVICES
        message : "Tunnel to Hub will be re-established"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_HUB
        message : "Hub needs to be upgraded"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_OTHER_SITES
        message : "Since it is a Full-Mesh topology, other
          sites need to be upgraded as well",
        message_type : WARNING
      },
      {
        check_type : COMPATIBILITY_WITH_NEW_FEATURES,
        message : "AppQoE, Local-breakout will not work on
          this site without upgrade"
        message_type : INFO
      }
    ],
    upgrade_steps : [
      {
        description : "Upgrade Image",
        expected_time : 20
      },
      {
        description : "Modify Config",
        expected_time : 5
      }
    ]
  },
  upgrade_total_expected_time : 25,

  upgrade_pre_requisites : [
    "Download JUNOS 18.2 image to CSO before proceeding with
      upgrade",
  ]
}

```

```

    ],
    upgrade_post_recommendations : [
        "Please upgrade other sites and hub in the topology",
    ]
}
}

```

Performing the Upgrade

To upgrade a site, send a POST request with the following JSON-formatted payload:

```
http://<CSO_Central_MS_ip>/tssm/upgrade-site/
```

JSON

You can use either the device ID or the site ID as shown:

```

{
  "input" : {
    "site_uuids":[
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"
    ]
  }
}

```

JSON

or

```

{
  "input" : {
    "device_uuids":[
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}

```

JSON



You can use the device ID to perform the site upgrade for hub devices.

Sample Response

```

{
  output : {
    upgrade_needed : < MANDATORY|OPTIONAL|NOT_NEEDED >,
    upgrade_impact_checks : [
      {
        check_type : IMAGE_SUPPORT
        message : "Support for this image is deprecated"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_SERVICES
        message : "Tunnel to Hub will be re-established"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_HUB
        message : "Hub needs to be upgraded"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_OTHER_SITES
        message : "Since it is a Full-Mesh topology, other
          sites need to be upgraded as well",
        message_type : WARNING
      },
      {
        check_type : COMPATIBILITY_WITH_NEW_FEATURES,
        message : "AppQoE, Local-breakout will not work on
          this site without upgrade"
        message_type : INFO
      }
    ],
    upgrade_steps : [
      {
        description : "Upgrade Image",
        expected_time : 20
      },
      {
        description : "Modify Config",
        expected_time : 5
      }
    ]
  },
  upgrade_total_expected_time : 25,

  upgrade_pre_requisites : [
    "Download JUNOS 18.2 image to CSO before proceeding with
      upgrade",
  ]
}

```

```
    ],  
    upgrade_post_recommendations : [  
      "Please upgrade other sites and hub in the topology",  
    ]  
  }  
}
```

Adding On-Premise Spoke Site

To add On-premise spoke site, send a POST request with the following JSON formatted payload:

```

{
  "input": {
    "tenant_name": "Color",
    "deployment_scenario": "managed_wan_v2",
    "site": [
      {
        "site_name": "White",
        "site_basic_properties": {
          "local_breakout": {
            "enabled": false
          },
          "site_name": "White",
          "sla_mgmt": "FINE",
          "cloud_service": "EDGE",
          "site_address": {
            "country": "US"
          },
          "device_redundancy": false,
          "network_seg": false,
          "device_template": [
            {
              "wan_link_info": [
                {
                  "enable_pppoe": false,
                  "wan_link_type": "Internet",
                  "local_breakout_enabled": false,
                  "wan_link": "WAN_2",
                  "subscribed_bandwidth": 2,
                  "exclusive_for_local_breakout": false,
                  "_sys_reserved_row": "55eefda7-44b7-bfd7-5561-31ce5ec7d433",
                  "cost": 2,
                  "access_type": "Ethernet",
                  "default_link": false,
                  "provider": "a",
                  "cost_currency": "USD",
                  "backup_link": false
                },
                {
                  "enable_pppoe": false,
                  "wan_link_type": "Internet",
                  "local_breakout_enabled": false,
                  "wan_link": "WAN_3",
                  "subscribed_bandwidth": 2,
                  "exclusive_for_local_breakout": false,
                  "_sys_reserved_row": "05a5c566-0497-6867-2a3c-8598db7759bf",
                  "cost": 2,
                  "access_type": "Ethernet",
                  "default_link": false,

```

```

        "provider": "a",
        "cost_currency": "USD",
        "backup_link": false
    },
    ],
    "template_name": "NFX_Advanced_SDWAN_CPE_option_1",
    "lan_segment": [
        {
            "ip_prefix": "xx.xx.xx.x/24",
            "lan_segment_name": "WLan",
            "vlan": 110,
            "lan_ports": [
                "LAN_1"
            ],
            "department": "WDept",
            "dhcp": false
        }
    ],
    "device_name": "White"
}
],
"0": {
    "ip_prefix": "xx.xx.xx.x/24",
    "lan_segment_name": "WLan",
    "vlan": 110,
    "lan_ports": [
        "LAN_1"
    ],
    "department": "WDept",
    "dhcp": false
},
"site_type": "on_premise",
"site_role": "SPOKE",
"enable_mh": true,
"device_profile_name": "NFX_Advanced_SDWAN_CPE_option_1",
"site_group": "",
"topology": "Full Mesh"
}
}
]
}
}

```

Configuring Spoke Site

To configure a spoke site, send a POST request with the following JSON formatted payload:

```

{
  "input": {
    "tenant_name": "Color",
    "job_name_prefix": "Color-White",
    "site": [
      {
        "on_premise_site_info": {
          "device": [
            {
              "device_template": "NFX_Advanced_SDWAN_CPE_option_1",
              "device_details": {
                "serial_number": "DC0416AF0057",
                "activation_code": "545454"
              },
              "oam_traffic": {
                "ip_prefix": "xx.xx.xx.x/32"
              },
              "wan_link": [
                {
                  "overlay_tunnel": [
                    {
                      "peer_info": {
                        "interface_name": "WAN_0",
                        "internet_gw_ip": "51.51.51.254",
                        "peer_device": "Yellow"
                      },
                      "tunnel_endpoint_role": "SPOKE",
                      "tunnel_type": "GRE_IPSEC",
                      "tunnel_id": 0
                    }
                  ],
                  "enable_pppoe": false,
                  "wan_link_type": "Internet",
                  "local_interface": "ge-0/0/8",
                  "used_for_meshing": true,
                  "nat_info": {
                    "nat_enabled": false
                  },
                  "access_type": "Ethernet",
                  "traffic_type": "OAM_AND_DATA",
                  "vlan_id": 960,
                  "local_breakout_enabled": false,
                  "used_for_oam": true,
                  "static_ip_assignment": {
                    "gateway_ip": "xx.xx.xx.xxx",
                    "ip_address": "xx.xx.xx.x/24"
                  },
                  "vpn": [
                    {
                      "vpn_name": "Color_DefaultVPN"
                    }
                  ]
                }
              ]
            }
          ]
        }
      ]
    }
  }
}

```

```

    }
  ],
  "wan_link_name": "WAN_2",
  "address_assignment": "STATIC",
  "connect_to_hubs": true
},
{
  "overlay_tunnel": [
    {
      "peer_info": {
        "interface_name": "WAN_2",
        "internet_gw_ip": "xx.xx.xx.xxx",
        "peer_device": "Yellow"
      },
      "tunnel_endpoint_role": "SPOKE",
      "tunnel_type": "GRE_IPSEC",
      "tunnel_id": 0
    }
  ],
  "enable_pppoe": false,
  "wan_link_type": "Internet",
  "local_interface": "ge-0/0/9",
  "used_for_meshing": true,
  "nat_info": {
    "nat_enabled": false
  },
  "access_type": "Ethernet",
  "traffic_type": "DATA_ONLY",
  "vlan_id": 970,
  "local_breakout_enabled": false,
  "used_for_oam": true,
  "static_ip_assignment": {
    "gateway_ip": "xx.xx.xx.xxx",
    "ip_address": "xx.xx.xx.x/24"
  },
  "vpn": [
    {
      "vpn_name": "Color_DefaultVPN"
    }
  ],
  "wan_link_name": "WAN_3",
  "address_assignment": "STATIC",
  "connect_to_hubs": true
}
],
"device_name": "White"
}
],
"hub_sites": [
  {

```

```

        "hub_role": "PRIMARY",
        "hub_name": "Yellow"
    },
    ],
    "region": "regional",
    "site_role": "spoke",
    "ha_info": {
        "ha_topology": "STANDALONE"
    },
    },
    "site_name": "White",
    "properties": {
        "property": [
            {
                "name": "site_advanced_config",
                "value": {
                    "timezone": "Asia/Calcutta",
                    "nameserver": [
                        "10.209.194.133"
                    ]
                }
            }
        ]
    }
}

```

Configuring enterprise-hub site

To configure a spoke site, send a POST request with the following JSON formatted payload:

```

{
  "input": {
    "tenant_name": "Color",
    "job_name_prefix": "Color-White",
    "site": [
      {
        "on_premise_site_info": {
          "device": [
            {
              "device_template": "NFX_Advanced_SDWAN_CPE_option_1",
              "device_details": {
                "serial_number": "DC0416AF0057",
                "activation_code": "545454"
              },
              "oam_traffic": {
                "ip_prefix": "xx.xx.xx.x/32"
              },
              "wan_link": [
                {
                  "overlay_tunnel": [
                    {
                      "peer_info": {
                        "interface_name": "WAN_0",
                        "internet_gw_ip": "51.51.51.254",
                        "peer_device": "Yellow"
                      },
                      "tunnel_endpoint_role": "SPOKE",
                      "tunnel_type": "GRE_IPSEC",
                      "tunnel_id": 0
                    }
                  ],
                  "enable_pppoe": false,
                  "wan_link_type": "Internet",
                  "local_interface": "ge-0/0/8",
                  "used_for_meshing": true,
                  "nat_info": {
                    "nat_enabled": false
                  },
                  "access_type": "Ethernet",
                  "traffic_type": "OAM_AND_DATA",
                  "vlan_id": 960,
                  "local_breakout_enabled": false,
                  "used_for_oam": true,
                  "static_ip_assignment": {
                    "gateway_ip": "xx.xx.xx.xxx",
                    "ip_address": "xx.xx.xx.x/24"
                  },
                  "vpn": [
                    {
                      "vpn_name": "Color_DefaultVPN"
                    }
                  ]
                }
              ]
            }
          ]
        }
      ]
    }
  }
}

```

```

    }
  ],
  "wan_link_name": "WAN_2",
  "address_assignment": "STATIC",
  "connect_to_hubs": true
},
{
  "overlay_tunnel": [
    {
      "peer_info": {
        "interface_name": "WAN_2",
        "internet_gw_ip": "xx.xx.xx.xxx",
        "peer_device": "Yellow"
      },
      "tunnel_endpoint_role": "SPOKE",
      "tunnel_type": "GRE_IPSEC",
      "tunnel_id": 0
    }
  ],
  "enable_pppoe": false,
  "wan_link_type": "Internet",
  "local_interface": "ge-0/0/9",
  "used_for_meshing": true,
  "nat_info": {
    "nat_enabled": false
  },
  "access_type": "Ethernet",
  "traffic_type": "DATA_ONLY",
  "vlan_id": 970,
  "local_breakout_enabled": false,
  "used_for_oam": true,
  "static_ip_assignment": {
    "gateway_ip": "xx.xx.xx.xxx",
    "ip_address": "xx.xx.xx.x/24"
  },
  "vpn": [
    {
      "vpn_name": "Color_DefaultVPN"
    }
  ],
  "wan_link_name": "WAN_3",
  "address_assignment": "STATIC",
  "connect_to_hubs": true
}
],
"device_name": "White"
}
],
"hub_sites": [
  {

```

```
        "hub_role": "PRIMARY",
        "hub_name": "Yellow"
    }
],
"region": "regional",
"site_role": "spoke",
"ha_info": {
    "ha_topology": "STANDALONE"
}
},
"site_name": "White",
"properties": {
    "property": [
        {
            "name": "site_advanced_config",
            "value": {
                "timezone": "Asia/Calcutta",
                "nameserver": [
                    "10.209.194.133"
                ]
            }
        }
    ]
}
}
]
}
```

Ensure that the following attribute is set, when you configure the site workflow for an enterprise-hub site:

```
"on_premise_gateway": true,
```

JSON

Set the following properties in the on-premise-site-info, to configure enterprise-hub using a spoke site:

```
"name": "on_premise_site_info",
"value": {
  "gateway_sites": [
    {
      "gateway_role": "PRIMARY_GW",
      "gateway_name": "gw1-vsrx"
    }
  ],

```

JSON

Upgrading a Site

Use the site_upgrade RESTful APIs to perform the following functions.

- Analyze the site upgrade
- Obtain the site upgrade analysis report
- Perform the site upgrade

Analyzing the Site Upgrade

To perform an upgrade analysis for a site, send a POST request with the following JSON formatted payload:

```
tssm/analyze_site_upgrade
```

JSON

You can use either the device ID or the site ID as shown:

```
{
  "input" : {
    "site_uuids":[
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"
    ]
  }
}
```

JSON

or

```
{
  "input" : {
    "device_uuids":[
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}
```

JSON



You can use the device ID to perform the upgrade analysis for hub devices.

Example Response:

```
{ "output": { "report": [], "job_id": "0247ceb9-b097-410f-98b1-289c5302c155", "jobid": "0247ceb9-b097-410f-98b1-289c5302c155" }}
```

JSON

Obtaining the Site Upgrade Analysis Report

To obtain the site upgrade analysis report, send a GET request with the following JSON formatted payload:

```
/tssm/get_upgrade_analysis_report
```

JSON

You can use either the device ID or the site ID as shown:

```
{
  "input" : {
    "site_uuids": [
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"
    ]
  }
}
```

JSON

or

```
{
  "input" : {
    "device_uuids": [
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}
```

JSON



You can use the device ID to perform the site upgrade for hub devices.

Example Response:

```

{
  output : {
    upgrade_needed : < MANDATORY|OPTIONAL|NOT_NEEDED >,
    upgrade_impact_checks : [
      {
        check_type : IMAGE_SUPPORT
        message : "Support for this image is deprecated"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_SERVICES
        message : "Tunnel to Hub will be re-established"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_HUB
        message : "Hub needs to be upgraded"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_OTHER_SITES
        message : "Since it is a Full-Mesh topology, other
          sites need to be upgraded as well",
        message_type : WARNING
      },
      {
        check_type : COMPATIBILITY_WITH_NEW_FEATURES,
        message : "AppQoE, Local-breakout will not work on
          this site without upgrade"
        message_type : INFO
      }
    ],
    upgrade_steps : [
      {
        description : "Upgrade Image",
        expected_time : 20
      },
      {
        description : "Modify Config",
        expected_time : 5
      }
    ]
  },
  upgrade_total_expected_time : 25,

  upgrade_pre_requisites : [
    "Download JUNOS 18.2 image to CSO before proceeding with
      upgrade",
  ]
}

```

```

    ],
    upgrade_post_recommendations : [
        "Please upgrade other sites and hub in the topology",
    ]
}
}

```

Performing the Upgrade

To upgrade a site, send a POST request with the following JSON formatted payload:

```
<CSO_Central_MS_ip>:80/tssm/upgrade_site
```

JSON

You can use either the device ID or the site ID as shown:

```

{
  "input" : {
    "site_uuids":[
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"
    ]
  }
}

```

JSON

or

```

{
  "input" : {
    "device_uuids":[
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}

```

JSON



You can use the device ID to perform the site upgrade for hub devices.

Example Response:

```

{
  output : {
    upgrade_needed : < MANDATORY|OPTIONAL|NOT_NEEDED >,
    upgrade_impact_checks : [
      {
        check_type : IMAGE_SUPPORT
        message : "Support for this image is deprecated"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_SERVICES
        message : "Tunnel to Hub will be re-established"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_HUB
        message : "Hub needs to be upgraded"
        message_type : WARNING
      },
      {
        check_type : IMPACT_ON_OTHER_SITES
        message : "Since it is a Full-Mesh topology, other
          sites need to be upgraded as well",
        message_type : WARNING
      },
      {
        check_type : COMPATIBILITY_WITH_NEW_FEATURES,
        message : "AppQoE, Local-breakout will not work on
          this site without upgrade"
        message_type : INFO
      }
    ],
    upgrade_steps : [
      {
        description : "Upgrade Image",
        expected_time : 20
      },
      {
        description : "Modify Config",
        expected_time : 5
      }
    ]
  },
  upgrade_total_expected_time : 25,

  upgrade_pre_requisites : [
    "Download JUNOS 18.2 image to CSO before proceeding with
      upgrade",
  ]
}

```

```

    ],
    upgrade_post_recommendations : [
        "Please upgrade other sites and hub in the topology",
    ]
}
}

```

Removing a Site

To remove a site, send a POST request with the following JSON-formatted payload:

```
https/<csp-ms-vm>/tssm/remove-site
```

JSON

JSON Object Input

```

root@centralmsvm:/opt/csp/logs/tssm-api/apidump# more 20180228082750587.json
{
  "input": {
    "tenant_name": "customer1",
    "remove_tenant": false,
    "job_name_prefix": "Site Delete for customer1",
    "sites": [
      {
        "site_name": "Demo"
      }
    ],
    "forced": true
  }
}

```

JSON

Deleting a Tenant

To delete a tenant, send a POST request with the following JSON-formatted payload:

```
https/<csp-ms-vm>/tssm/remove-site
```

JSON

JSON Object Input

JSON

```
{
  "input": {
    "job_name_prefix": "Tenant Delete",
    "tenant_name": "customer-A",
    "remove_tenant": true,
    "forced": true,
    "sites": [
      ]
  }
}
```

Deleting a POP Object

To delete a POP object, send a POST request with the following JSON-formatted payload:

POST <http://<central-ip>/topology-service/remove-pop>

JSON

JSON Object Input

```
{
  "input": {
    "job_name_prefix": "Delete-PoP",
    "pop": [{
      "name": "pop-A"
    }]
  }
}
```

JSON

Shipping a Device

To ship a device, send a POST request to with the following input payload:

http://<CSO_Central_MS_ip>:80/tssm/ship-device

JSON

JSON Object Input:

```
curl -vk -X POST -H "Cache-Control: no-cache" \
-H "X-Auth-Token: bbf35b4c222e47e2848d186c0dfe8e24" \
-H "Content-Type: application/json" \
-d '
{
  "input": {
    "shipped_device": [
      {
        "customer_name": "${customer1}",
        "site_name": "${site1}",
        "serial_number": "${serial_number1}",
        "activation_code": "${activation_code}"
      }
    ]
  }
}
```

2.6.3. API Examples: Viewing the Current Operational State of the System

This section provides information about the APIs that can be used to view the current operational state of the system:

- Obtaining a List of Existing Tenants and Associated UUIDs
- Obtaining the Tenant List
- Obtaining the Tenant Details
- Obtaining the Tenant Sites
- Obtaining the Site Details
- Obtaining the Site Upgrade Details
- Obtaining the List of CPE Devices
- Obtaining the CPE Details
- Obtaining the Alerts History
- Obtain the Current Alerts
- Obtaining the List of Top Five Alerts

Obtaining a List of Existing Tenants and Associated UUIDs

This API uses the TSSM microservice to obtain the list of tenants.

To obtain the list of existing tenants and associated UUIDs, send a GET request with the authentication token to your API server:

GET /<csp-ms-vm>/tssm/customer

The response to the GET request provides the list of all the user names and the associated UUIDs.

Sample Response

```
{
  "href": "http://xx.xxx.xx.xx/tssm/customer/d1ebc753-24a8-445a-bc4b-e51a296f6c87",
  "fq_name": [
    "default-domain",
    "Tenant_VJ",
    "Tenant_VJ"
  ],
  "uuid": "d1ebc753-24a8-445a-bc4b-e51a296f6c87" #tenant uuid
}
```

The API illustrated above uses the TSSM microservice to obtain a list of tenants; however, you can also use the dataview microservice APIs to get a full operational view of the system. The CSO Web UI uses the dataview microservice to gather information about the operational state of the system along with the following information:

- Tenants
- Sites
- Devices
- Current configuration state
- Alerts
- Alarms



While the dataview APIs provide full operational view of the system, note that these APIs are written specifically to gather information corresponding to how the CSO portal views the system. Hence the information about these APIs is subject to changes in the CSO portal from release to release.

The examples in the remaining tasks in this section show how to use the dataview APIs to view the current operation state of the system.

Obtaining the Tenant List

The following cURL example contains the JSON-formatted data to obtain a list of tenants:

JSON

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
"https://xxx.xx.xx.xxx:443/data-view-central/tenant"
```

Sample Response

JSON

```
{  
  "total": 3,  
  "tenant": [  
    {  
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant/6bd6ad4a-df54-4fb5-b093-0a117a61b040",  
      "fq_name": [  
        "default-project"  
      ],  
      "uuid": "6bd6ad4a-df54-4fb5-b093-0a117a61b040"  
    },  
    {  
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant/6fd928e7-ae8d-4716-872d-0bac893b01a3",  
      "fq_name": [  
        "DallasHybridWAN"  
      ],  
      "uuid": "6fd928e7-ae8d-4716-872d-0bac893b01a3"  
    },  
    {  
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant/01818ad1-d587-4a88-add1-9a996e165911",  
      "fq_name": [  
        "DallasSDWAN"  
      ],  
      "uuid": "01818ad1-d587-4a88-add1-9a996e165911"  
    }  
  ]  
}
```

Obtaining the Tenant Details

The following cURL example contains the JSON-formatted data to obtain a details of tenants:

JSON

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
https://xxx.xx.xx.xxx:443/data-view-central/tenant/6fd928e7-ae8d-4716-872d-0bac893b01a3
```

Sample Response

JSON

```
{
  "tenant": {
    "administrator": [
      "hw_admin@dallashybridwan.com"
    ],
    "count_critical": 2,
    "tenant_type": "small",
    "customer_uuid": "6fd928e7-ae8d-4716-872d-0bac893b01a3",
    "last_changed": "2018-02-22T01:01:47.668007",
    "user_defined_properties": [],
    "href": "http://xxx.xx.xxx/data-view-central/tenant/6fd928e7-ae8d-4716-872d-0bac893b01a3",
    "nfv_service_profile_ids": [
      "2f34d312-ee5a-4a36-aae5-902c169e7ec5",
      "af8ab0de-aed8-47d7-ace0-7ae0d78d2cde"
    ],
    "display_name": "DallasHybridWAN",
    "number_of_sites": 1,
    "name": "DallasHybridWAN",
    "count_minor": 0,
    "fq_name": [
      "DallasHybridWAN"
    ],
    "uuid": "6fd928e7-ae8d-4716-872d-0bac893b01a3",
    "number_of_assigned_services": 2,
    "activated_services": 0,
    "perms2": {
      "owner": "e6fd2e78262e4f53bafef19a51e4bb083",
      "owner_access": 7,
      "global_access": 0,
      "share": []
    },
    "deployment_scenario": "managed_wan",
    "project_id": "e6fd2e78-262e-4f53-bafe-19a51e4bb083",
    "count_major": 9
  }
}
```

Obtaining the Tenant Sites

The following cURL example contains the JSON-formatted data to obtain a list of tenant sites and their details:

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
https://xxx.xx.xx.xxx:443/data-view-central/tenant-sites
```

Sample Response

```
{
  "tenant-sites": [
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant-sites/7b409402-b931-4434-a2b6-d367164ea7d0",
      "fq_name": [
        "srx1500-2-1-HUB"
      ],
      "uuid": "7b409402-b931-4434-a2b6-d367164ea7d0"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant-sites/fce8080b-1fde-4e59-8363-790f9e86b7e3",
      "fq_name": [
        "srx1500-2-1-HUB"
      ],
      "uuid": "fce8080b-1fde-4e59-8363-790f9e86b7e3"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant-sites/50d24e14-431a-4c75-adc6-760129feb1d4",
      "fq_name": [
        "NFX1-site"
      ],
      "uuid": "50d24e14-431a-4c75-adc6-760129feb1d4"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant-sites/2e3dd917-6522-4d57-a1f3-cf11a7c7a8e6",
      "fq_name": [
        "NFX2-site"
      ],
      "uuid": "2e3dd917-6522-4d57-a1f3-cf11a7c7a8e6"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/tenant-sites/4324405a-645c-4798-af95-a32825245906",
      "fq_name": [
        "NFX6-site"
      ],
      "uuid": "4324405a-645c-4798-af95-a32825245906"
    }
  ],
  "total": 5
}
```

Obtaining the Site Details

The following cURL example contains the JSON-formatted data to obtain the tenant-site details:

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
"https://xxx.xx.xx.xxx:443/data-view-central/tenant-sites/50d24e14-431a-4c75-adc6-  
760129feb1d4"
```

Sample Response

```

{
  "tenant-sites": {
    "status": "CONFIGURED",
    "count_critical": 0,
    "tenant_name": "DallasHybridWAN",
    "href": "http://xxx.xx.xx.xxx/data-view-central/tenant-sites/50d24e14-431a-4c75-adc6-760129feb1d4",
    "site_type": "on_premise",
    "device": [
      {
        "connection_type": "DEVICE_INITIATED",
        "device_fq_name_str": "default-domain:DallasHybridWAN:NFX1-site_CPE1",
        "device_template_name": "NFX_Managed_Internet_CPE_DAL",
        "device_template_id": "2b3acc63-4e2b-4e27-84c8-076036ef0520",
        "device_family_info": {
          "name": "domain-name-nfx",
          "family": "NFX"
        },
        "device_serial_number": "DD1917AF0110",
        "device_type": "cpe",
        "ems_id": "99e4e3e8-1759-11e8-942c-0242ac106241",
        "management_state": "PROVISIONED",
        "device_id": "110d248c-0b6e-4621-9423-9ea2ca381ee6"
      ]
    ],
    "display_name": "NFX1-site",
    "overlay_links": 0,
    "device_templates": [
      {
        "device_template_id": "2b3acc63-4e2b-4e27-84c8-076036ef0520",
        "device_template_name": "NFX_Managed_Internet_CPE_DAL"
      }
    ],
    "name": "NFX1-site",
    "count_minor": 0,
    "project_id": "e6fd2e78-262e-4f53-bafe-19a51e4bb083",
    "fq_name": [
      "NFX1-site"
    ],
    "uuid": "50d24e14-431a-4c75-adc6-760129feb1d4",
    "topo_role": "spoke",
    "pop_name": "regional",
    "perms2": {
      "owner": "e6fd2e78262e4f53bafe19a51e4bb083",
      "owner_access": 7,
      "global_access": 0,
      "share": []
    },
    "number_of_services_activated": 0,
    "location": ""
  }
}

```

```

    "coordinates": "41.33617,-75.9632636",
    "count_major": 5,
    "tenant_uuid": "6fd928e7-ae8d-4716-872d-0bac893b01a3",
    "tssm_site_id": "f58f1598-1d82-411c-81f4-bc540359e9b3"
  }
}

```

Obtaining the Site Upgrade Details

To check whether a site is due for upgrade, send the following GET request to the API server:

POST http://<ip-addr>/tssm/check_for_site_upgrade

JSON

You can use either the site ID or the device ID as shown in the following JSON-formatted payloads:

```

{
  "input" : {
    "site_uuids": [
      "06883ca4-a0b5-4d19-b153-7fdb97cae3e3",
      "e90d3cd8-118b-4b69-840d-7ba2e332785c"
    ]
  }
}

```

JSON

or

```

{
  "input" : {
    "device_uuids": [
      "9191a184-abe0-498d-915e-1cac8517bfd9",
      "0d0f66fc-bea3-4870-b20a-ccde834e817a"
    ]
  }
}

```

JSON



For hub devices, the device ID can be used for upgrade analysis.

Sample Response

```
{  
  output : {  
    upgrade_needed : <MANDATORY|OPTIONAL|NOT_NEEDED>  
  }  
}
```

Obtaining the List of CPE Devices

The following cURL example contains the JSON-formatted data to obtain the list of CPE devices.

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
"https://xxx.xx.xx.xxx:443/data-view-central/cpe"
```

Sample Response

```
{
  "total": 5,
  "cpe": [
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/cpe/0e220aca-4745-4d1b-b762-defe69c6802c",
      "fq_name": [
        "srx1500-2-1-HUB"
      ],
      "uuid": "0e220aca-4745-4d1b-b762-defe69c6802c"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/cpe/5a75c96c-0c11-4a3a-9880-e23a2589bf47",
      "fq_name": [
        "NFX2-site_CPE1"
      ],
      "uuid": "5a75c96c-0c11-4a3a-9880-e23a2589bf47"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/cpe/110d248c-0b6e-4621-9423-9ea2ca381ee6",
      "fq_name": [
        "NFX1-site_CPE1"
      ],
      "uuid": "110d248c-0b6e-4621-9423-9ea2ca381ee6"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/cpe/8359e034-9f74-4a46-9ccc-9783f9e537c9",
      "fq_name": [
        "NFX6-site_CPE1"
      ],
      "uuid": "8359e034-9f74-4a46-9ccc-9783f9e537c9"
    },
    {
      "href": "http://xxx.xx.xx.xxx/data-view-central/cpe/60447c59-1b21-418b-bd4b-3b75e903ec87",
      "fq_name": [
        "vrr-169.47.71.108"
      ],
      "uuid": "60447c59-1b21-418b-bd4b-3b75e903ec87"
    }
  ]
}
```

Obtaining the CPE Details

The following cURL example contains the JSON-formatted data to obtain details of the CPE devices

```
-vk -H "Cache-Control: no-cache" \
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \
"https://xxx.xx.xx.xxx:443/data-view-central/cpe/110d248c-0b6e-4621-9423-9ea2ca381ee6"
```

JSON

Sample Response

```
{
  "cpe": {
    "pop_uuid": "20723e9b-5d14-4f61-9304-67e4c2607d24",
    "site_name": "NFX1-site",
    "tenant_name": "DallasHybridWAN",
    "number_of_active_services": 0,
    "perms2": {
      "owner": "e6fd2e78262e4f53baf9a51e4bb083",
      "owner_access": 7,
      "global_access": 0,
      "share": []
    },
    "href": "http://xxx.xx.xx.xxx/data-view-central/cpe/110d248c-0b6e-4621-9423-9ea2ca381ee6",
    "wan_links": 1,
    "device_type": "cpe",
    "device_template_id": "2b3acc63-4e2b-4e27-84c8-076036ef0520",
    "name": "NFX1-site_CPE1",
    "device_template_name": "NFX_Managed_Internet_CPE_DAL",
    "fq_name": [
      "NFX1-site_CPE1"
    ],
    "uuid": "110d248c-0b6e-4621-9423-9ea2ca381ee6",
    "os_version": "15.1X53-D47.4",
    "ems_uuid": "99e4e3e8-1759-11e8-942c-0242ac106241",
    "device_family": "domain-name-nfx",
    "pop_name": "regional",
    "state": "unknown",
    "management_status": "PROVISIONED",
    "site_uuid": "50d24e14-431a-4c75-adc6-760129feb1d4",
    "location": "",
    "serial_number": "DD19XXXX10",
    "status_message": "Ztp success",
    "model_name": "NFX"
  }
}
```

JSON

Obtaining the Alerts History

The following cURL example contains the JSON-formatted data to obtain the alerts history:

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
"https://xxx.xx.xx.xxx:443/data-view-central/db-alerts-history"
```

JSON

Sample Response

```
{  
  "db-alerts-history": [],  
  "total": 0  
}
```

JSON

Obtain the Current Alerts

The following cURL example contains the JSON-formatted data to obtain the list of current alerts:

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
"https://xxx.xx.xx.xxx:443/data-view-central/db-current-alerts"
```

JSON

Sample Response

```
{  
  "total": 1,  
  "db-current-alerts": [  
    {  
      "display_name": "db_current_alert",  
      "uuid": "afbc96a2-32ac-11e8-a434-0242ac106227",  
      "number_of_critical_alerts": 0,  
      "number_of_minor_alerts": 0,  
      "number_of_major_alerts": 0,  
      "fq_name": [  
        "db_current_alert"  
      ]  
    }  
  ]  
}
```

JSON

Obtaining the List of Top Five Alerts

The following cURL example contains the JSON-formatted data to obtain the list of top five alerts:

```
-vk -H "Cache-Control: no-cache" \  
-H "X-Auth-Token: 9469eeb87f3d4ae9bb315b515edeb0cd" \  
"https://xxx.xx.xx.xxx:443/data-view-central/db-top5-pops-alerts"
```

Sample Response

```
{  
  "total": 0,  
  "db-top5-pops-alerts": []  
}
```

2.6.4. Notifications

CSO and NSC use a message bus scheme (RabbitMQ) to publish notifications about system events. The consumers of CSO and NSC are expected to register to appropriate channels on the message bus to receive information about various events.

The following sample snippet shows how to register to an EMS event and receive notification about device status.

```
#!/usr/bin/env python
import pika

# connection to rabbitmq Server
connection =
pika.BlockingConnection(pika.ConnectionParameters(host='cso_rabbitmq_infra_ip',
port=cso_rabbitmq_infra_port, credentials=pika.credentials.PlainCredentials('username',
'password'))))

channel = connection.channel()

# Declare exchange - dms-notification is the exchange to receive notification events from
Device Management Service
For dms (device management service) generic notification you should listen on the exchange
dms_notification (type: topic)

If you want to receive all the state change message then use the routing key '#'

If you want to receive all notification for a specific device use routing key
"device_uuid"+"."+ '#'

If you want to receive all notification for a specific component on NFX use routing key
"#"+"."+ 'JDM'

channel.exchange_declare(exchange='dms_notification', type='topic')

# Queue name to create - queue name
queue_name = 'name of queue to receive messages'
channel.queue_declare(queue_name)

# Bind queue and exchange
channel.queue_bind(exchange='dms_notification', queue=queue_name, routing_key='#')

# Function to be called when message is received.
def callback(ch, method, properties, body):
    print(" [x] %r:%r" % (method.routing_key, body))

# Register callback
channel.basic_consume(callback, queue=queue_name, no_ack=True)

print 'Starting Consumer...'
channel.start_consuming()
```

Payload Format for Notification Messages

```
{"device_id": "", "device_state": "", "device_previous_state": ""}
```

YANG Mapping

```
notification device_state_changed {  
  description  
    "Notify services about device's state change.";  
  leaf device_id {  
    type yang:uuid;  
    description  
      "Device id."; // format sitename-nfx  
  }  
  leaf device_state {  
    type ems:DeviceManagementStateEnum;  
    description  
      "Device's new state.";  
  }  
  leaf device_previous_state {  
    type ems:DeviceManagementStateEnum;  
    description  
      "Device's previous state.";  
  }  
}
```

Device Management State Enumerators

```
typedef DeviceManagementStateEnum {
  type enumeration {
    enum "EXPECTED" {
      description
        "device is modeled and is expected to be activated.";
    }
    enum "ACTIVATION_IN_PROGRESS" {
      description
        "device activation is in progress";
    }
    enum "ACTIVE" {
      description
        "device is active";
    }
    enum "AUTH_FAILED" {
      description
        "device authentication failed";
    }
    enum "RMA" {
      description
        "device is in RMA state";
    }
    enum "ZERIOZED" {
      description
        "device is in factory default state";
    }
    enum "READY_FOR_RESTORE" {
      description
        "device is ready for restoration";
    }
  }
  description
    "Management state of device from device management perspective,
    device activation states will be available in activation service";
}
```

2.6.5. Notifications using Server Sent Events (SSE)

For notifications, CSO admin-portal relies on server sent events technology (SSE), using SSE API a browser or http_client you will be able to setup one way communication with the server to receive updates on modeled backend Data Base objects.

Sample Syntax

```
curl -H "x-auth-token: $TOKEN" https://localhost/streams/csp --insecure
```

Syntax with Filter

```
curl -H "x-auth-token: $TOKEN" https://localhost/streams/csp?filter=<micro-service-name1:object-name1>,<micro-service-name2:object-name2> --insecure
```

JSON

Sample object names in CSO:

- job-service:job
- topology-service:device
- topology-service:site
- topology-service:pop
- data-view-central:image

Example

Fetch Keystone Token

```
curl -X POST \
  https://10.155.81.123/v3/auth/tokens \
  -H 'Content-Type: application/json' \
  -d '{
    "auth": {
      "identity": {
        "methods": ["password"],
        "password": {
          "user": {
            "domain": {
              "id": "default"
            },
            "name": "cspadmin",
            "password": "Embe1mpls!"
          }
        }
      },
      "scope": {
        "project": {
          "domain": {
            "id": "default"
          },
          "name": "default-project"
        }
      }
    }
  }' \
  -k \
  -v
```

Sample Response

```
HTTP/1.1 201 Created
Content-Length: 2575
X-Subject-Token: b2b8193fe03d41cd9d0e2f8cb2c5b9bb
Vary: X-Auth-Token
```

```
export TOKEN=b2b8193fe03d41cd9d0e2f8cb2c5b9bb
```

```
curl -H "x-auth-token: $TOKEN" https://10.155.81.123/streams/csp --insecure
```

Sample Response

```
event: message
data: {"oper": "CREATE", "uuid": "48be4550-1e4f-4e10-b75c-7074f7daefc2", "request-id":
"req-7770135a-3b67-4932-a590-9fbca66793f4", "namespace": "topology-service", "tenantid":
"37758946276840d590c34007a69950fe", "perms2": {"owner":
"37758946276840d590c34007a69950fe", "owner_access": 7, "global_access": 0, "share":
[{"tenant_access": 5, "tenant": "share.descendant_projects"}]}, "publish_at":
1556383101.917935, "type": "pop", "obj_dict": {"fq_name": ["default-domain", "pop-test"],
"uuid": "48be4550-1e4f-4e10-b75c-7074f7daefc2", "pop_type": "regular", "parent_type":
"domain", "longitude": "-100.4458825", "name": "pop-test", "perms2": {"owner":
"37758946276840d590c34007a69950fe", "owner_access": 7, "global_access": 0, "share":
[{"tenant_access": 5, "tenant": "share.descendant_projects"}]}, "id_perms": {"enable":
true, "uuid": {"uuid_mslong": "5241703226714050064", "uuid_lslong":
"13212559054475030466"}, "created": "2019-04-27T16:38:21.906054", "description": null,
"creator": "cspadmin", "user_visible": true, "last_modified": "2019-04-
27T16:38:21.906054", "modifier": "cspadmin", "permissions": {"owner": "cspadmin",
"owner_access": 7, "other_access": 7, "group": "admin", "group_access": 7}}, "address":
{"city": null, "country": "US", "street2": null, "state": null, "street": null,
"zip_code": null}, "latitude": "39.7837304", "display_name": "pop-test", "parent_uuid":
"f7574dd1-5978-477a-ae fd-9e85363b2e02"}}
```

Table 3 provides information on Notification body responses:

Table 3. Notification Body Responses

Attribute	Description	Example values
oper	Type of CUD operation on the DB object	CREATE, UPDATE, DELETE
namespace	Microservice name	Topology-service, ems-central, data-view-central
uuid	Unique identifier of object	48be4550-1e4f-4e10-b75c-7074f7daefc2
type	Object type	Device, pop, site, customer
fq_name	Full qualified domain name	["default-domain", "pop-test"]

Using Filters while Subscribing

If you want to subscribe to device change events and FMPM alarms the following filter has to be used:

```
curl -H "x-auth-token: $TOKEN" https://10.155.81.123/streams/csp?filter=topology-  
service:device,fmpm-provider:alert_status_object --insecure
```

JSON

Here is an example of a open-source monitoring solution that allows one to receive alerts/events/alarms from CSO and take action as needed (send message to Slack, index in a SYSLOG collector, send to Kafka bus, etc.)

https://github.com/packetferret/cso_monitoring

For more information on alters and alarms refer to 'Service Assurance' chapter.

2.6.6. Using Audit Logs for Information Retrieval

Use the audit logs to extract useful information from the system. Audit logs are generated whenever a user or administrator operations are performed on the system. CSO generates audit log messages on RabbitMQ.

RabbitMQ messages are published on the csp.audit_log exchange. On the csp.audit_log exchange, each message type has a different routing key. The exchange allows you to create a consumer queue with selective routing keys. Other messages published on the exchange are not delivered to the queue.

In addition to the routing key, the payload format of audit log RabbitMQ message is:

```
{  
  "status": "One of 'in-progress', 'success', 'failed'",  
  "username": "Current login user name performing the activity",  
  "timestamp": "Timestamp of the activity",  
  "message": "Human readable audit log message",  
  "task_name": "Name of the task",  
  "service_name": "Name of the CSO micro service",  
  "namespace": "Namespace of the object",  
  "object_type": "Type of the object, e.g. site, tenant",  
  "object_id": "uuid of the target object"  
}
```

JSON

A combination of namespace, object_type and object_id will be used to make REST API call to get the object details. With the knowledge of how the objects are laid out internally in CSO/NSC, a northbound system receiving these audit logs can use the above information to fetch additional

useful information about the objects from the system.

After the object type and the object ID are received from the audit log, additional information about the object can be received by making appropriate RESTful API calls to the microservice associated with the object.

Internal Relationship of Various Objects

An understanding of the internal relationship between the various objects enables you to use the system effectively. The figures 7 - 8 show how the various objects are laid out internally.

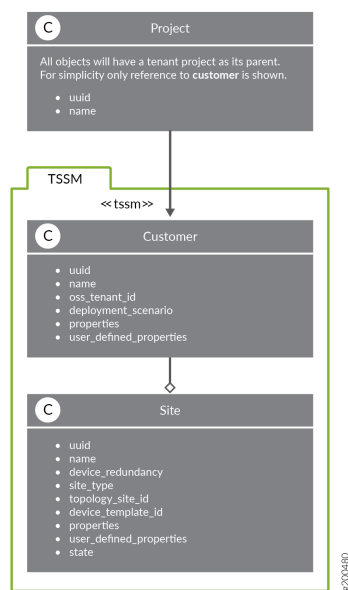
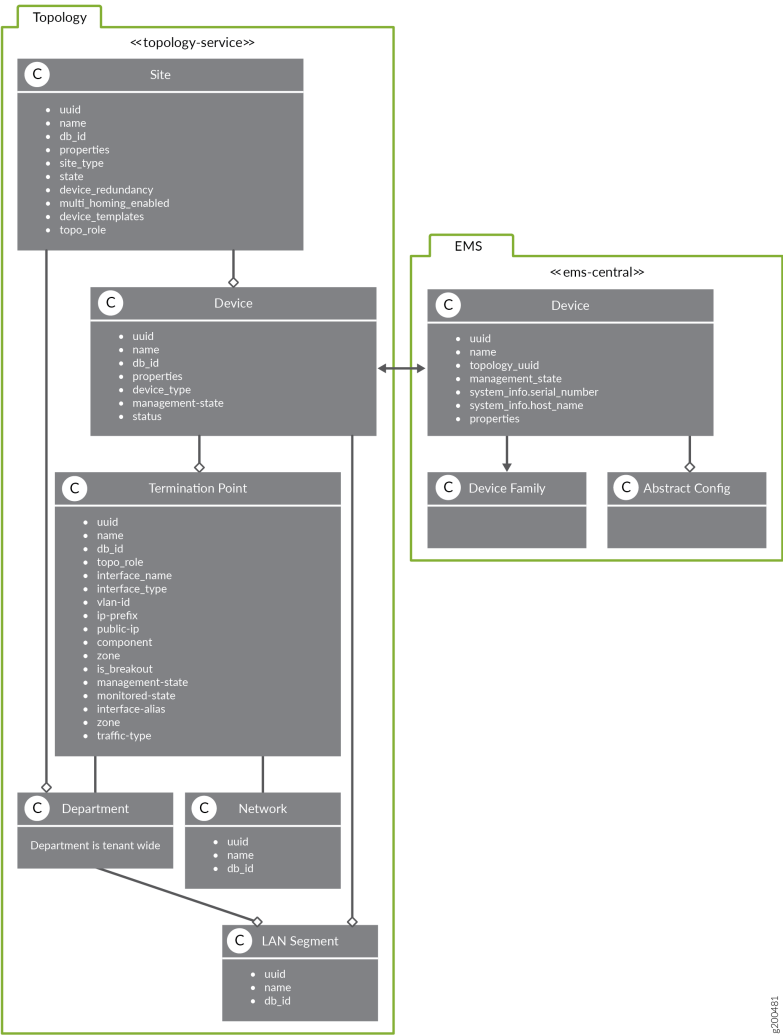


Figure 7. Project TSSM Relationship



1800028

Figure 8. Topology EMS Relationship

Information Retrieval Example Using Audit Logs as Starting Point

This section shows how information can be recursively obtained using audit logs as a starting point.

The example starts by listening to audit log messages for site operations.

Message Example

```
Routing keys = device.create, device.update, device.provision
```

JSON

A sample message received on the message bus using the above routing keys:

JSON

```
{
  "status": "success",
  "username": tenant-ABCcorp-admin,
  "service_name": "csp-tssm",
  "timestamp": "2017-12-17T19:46:01.103Z",
  "message": "Configure Site",
  "task_name": "csp.tssm_create_sites",
  "namespace": "tssm",
  "object_type": "site",
  "object_id": " ad67d0d5-2a8a-41c1-b0a7-2fdd44af5023"
}
```

The audit log received above indicates a site with object identifier " ad67d0d5-2a8a-41c1-b0a7-2fdd44af5023" is being operated on.

To obtain the site, send a GET request to:

```
https://<server-address>/tssm/site/<site-uuid>
```

JSON

Example

```
https://10.208.135.53/tssm/site/ad67d0d5-2a8a-41c1-b0a7-2fdd44af5023
```

JSON

Sample JSON Response

```

{
  "site": {
    "parent_uuid": "acb9b7d4-3388-4509-bbc9-44971518b4d1",
    "parent_type": "customer",
    "site_type": "on_premise",
    "display_name": "site-premise-a",
    "device_template_id": "0deeb00a-a65b-35ad-a8ea-05a706de2661",
    "properties": {
      "property": [
        {
          "name": "site_advanced_config",
          "value": {
            "nameserver": "10.8.8.8",
            "foobar_site_id": "foobar_site_id_00001",
            "foobar_wan_id_mapping": [
              {
                "foobar_wan_id": "foobar_wan_0_00001",
                "wan_link": "wan_0"
              },
              {
                "foobar_wan_id": "foobar_wan_1_00002",
                "wan_link": "wan_1"
              }
            ]
          }
        }
      ]
    }
  },
  "name": "site-premise-a",
  "fq_name": [
    "default-domain",
    "Foobar",
    "Foobar",
    "site-premise-a"
  ],
  "uuid": "ad67d0d5-2a8a-41c1-b0a7-2fdd44af5023",
  "topology_site_id": "a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01fc",
  "uri": "/tssm/site/ad67d0d5-2a8a-41c1-b0a7-2fdd44af5023",
  "state": "provisioned",
  "parent_uri": "/tssm/customer/acb9b7d4-3388-4509-bbc9-44971518b4d1"
}

```

Obtaining the Connectivity Information Associated with a Site

In addition to the site being created in TSSM, a site is also created in the topology microservice which provides all the connectivity information about the site.

To obtain the topology site object information, send a GET request to:

```
https://<server-address>/topology-service/site/<topology-site-uuid>
```

JSON

Example

```
https://10.208.135.53/topology-service/site/a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01f
```

JSON

Sample JSON Response

```
{
  "site": {
    "db_id": "51778429-e8ee-446a-8ad0-592056f8b77a",
    "parent_uuid": "875578ab-395a-4554-8051-05803312778d",
    "cloud_service": "EDGE",
    "parent_type": "project",
    "longitude": "-100.4458825",
    "update_number": 5,
    "site_type": "on_premise",
    "address": {
      "city": null,
      "country": "US",
      "street2": null,
      "state": null,
      "street": null,
      "zip_code": null
    },
    "fq_name": [
      "default-domain",
      "test",
      "london"
    ],
    "properties": {
      "property": [
        {
          "name": "site_basic_properties",
          "value": {
            "local_breakout": {
              "breakout_type": "site_wide_breakout",
              "enabled": true
            },
            "site_type": "on_premise",
            "cloud_service": "EDGE",
            "site_address": {
              "city": null,
              "country": "US",
              "street2": null,
              "state": null,
              "street": null,
              "zip_code": null
            },
            "multi_homing_enabled": false,
            "device_template": [
              {
                "wan_link_info": [
                  {
                    "backup_link": false,
                    "preferred_breakout_link": false,
                    "provider": "ATT",
                    "subscribed_bandwidth": 1000,

```

```

        "wan_link": "WAN_0",
        "exclusive_for_local_breakout": false,
        "cost": 20,
        "default_link": false,
        "local_breakout_enabled": false,
        "cost_currency": "USD",
        "wan_link_type": "MPLS"
    },
    {
        "backup_link": false,
        "preferred_breakout_link": true,
        "provider": "Comcast",
        "subscribed_bandwidth": 2000,
        "wan_link": "WAN_1",
        "exclusive_for_local_breakout": false,
        "cost": 10,
        "default_link": false,
        "local_breakout_enabled": true,
        "cost_currency": "USD",
        "wan_link_type": "Internet"
    }
],
"template_name": "NFX_Advanced_SDWAN_CPE_option_1",
"authentication": null,
"lan_segment": [
    {
        "additional_config": null,
        "password": null,
        "ip_prefix": "1.1.1.1/24",
        "protocol": "ospfv2",
        "auth_key": null,
        "lan_segment_name": "Finance",
        "static_routing_gateway": [],
        "vlan": 200,
        "area_code": null,
        "md5_checksum": null,
        "routing_segment": null,
        "authentication_option": null,
        "department": "Finance",
        "dhcp": false,
        "ospf_additional_config": null,
        "advertise_remote_route": null,
        "lan_ports": [
            "LAN_1"
        ]
    }
],
"device_name": "london_CPE1"
}
],

```

```

        "site_description": null,
        "site_role": "SPOKE",
        "site_meta": null,
        "site_contact": null,
        "site_group": []
      }
    ]
  },
  "device_templates": [
    "e4b7a848-68ca-359e-9538-ca60bf980856"
  ],
  "name": "london",
  "display_name": "london",
  "uuid": "a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01fc",
  "description": null,
  "uri": "/topology-service/site/a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01fc",
  "topo_role": "spoke",
  "multi_homing_enabled": false,
  "state": "CONFIGURATION-FAILED",
  "latitude": "39.7837304",
  "parent_uri": "/topology-service/project/875578ab-395a-4554-8051-05803312778d"
}
}

```



Querying Topology-service objects does not return by default referenced objects. It returns only first level attributes.

To obtain the topology site object information with references to related objects, send a GET request to:

```
https://<server-address>/topology-service/site/<topology-site-uuid>?exclude_refs=false
```

JSON

Example

```
https://10.208.135.53/topology-service/site/a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01f?exclude_refs=false
```

JSON

Sample JSON Response

```
{
  "site": {
    "db_id": "51778429-e8ee-446a-8ad0-592056f8b77a",
    "parent_uuid": "875578ab-395a-4554-8051-05803312778d",
    "cloud_service": "EDGE",
    "department_refs": [
      {
        "to": [
          "default-domain",
          "test",
          "Finance"
        ],
        "uuid": "06b7373c-a41d-405c-b11c-c38f40405aac",
        "attr": null,
        "uri": "/topology-service/department/06b7373c-a41d-405c-b11c-c38f40405aac"
      }
    ],
    "parent_type": "project",
    "longitude": "-100.4458825",
    "update_number": 5,
    "site_type": "on_premise",
    "address": {
      "city": null,
      "country": "US",
      "street2": null,
      "state": null,
      "street": null,
      "zip_code": null
    },
    "fq_name": [
      "default-domain",
      "test",
      "london"
    ],
    "properties": {
      "property": [
        {
          "name": "site_basic_properties",
          "value": {
            "local_breakout": {
              "breakout_type": "site_wide_breakout",
              "enabled": true
            },
            "site_type": "on_premise",
            "cloud_service": "EDGE",
            "site_address": {
              "city": null,
              "country": "US",
              "street2": null,
              "state": null,

```

```

    "street": null,
    "zip_code": null
  },
  "multi_homing_enabled": false,
  "device_template": [
    {
      "wan_link_info": [
        {
          "backup_link": false,
          "preferred_breakout_link": false,
          "provider": "ATT",
          "subscribed_bandwidth": 1000,
          "wan_link": "WAN_0",
          "exclusive_for_local_breakout": false,
          "cost": 20,
          "default_link": false,
          "local_breakout_enabled": false,
          "cost_currency": "USD",
          "wan_link_type": "MPLS"
        },
        {
          "backup_link": false,
          "preferred_breakout_link": true,
          "provider": "Comcast",
          "subscribed_bandwidth": 2000,
          "wan_link": "WAN_1",
          "exclusive_for_local_breakout": false,
          "cost": 10,
          "default_link": false,
          "local_breakout_enabled": true,
          "cost_currency": "USD",
          "wan_link_type": "Internet"
        }
      ],
      "template_name": "NFX_Advanced_SDWAN_CPE_option_1",
      "authentication": null,
      "lan_segment": [
        {
          "additional_config": null,
          "password": null,
          "ip_prefix": "1.1.1.1/24",
          "protocol": "ospfv2",
          "auth_key": null,
          "lan_segment_name": "Finance",
          "static_routing_gateway": [],
          "vlan": 200,
          "area_code": null,
          "md5_checksum": null,
          "routing_segment": null,
          "authentication_option": null,

```

```

        "department": "Finance",
        "dhcp": false,
        "ospf_additional_config": null,
        "advertise_remote_route": null,
        "lan_ports": [
            "LAN_1"
        ]
    },
    ],
    "device_name": "london_CPE1"
}
],
"site_description": null,
"site_role": "SPOKE",
"site_meta": null,
"site_contact": null,
"site_group": []
}
}
],
},
"device_templates": [
    "e4b7a848-68ca-359e-9538-ca60bf980856"
],
"name": "london",
"display_name": "london",
"uuid": "a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01fc",
"description": null,
"uri": "/topology-service/site/a97b1b7a-0b7e-4ad4-9f2e-41bb36dd01fc",
"topo_role": "spoke",
"multi_homing_enabled": false,
"device_refs": [
    {
        "to": [
            "default-domain",
            "test",
            "london_CPE1"
        ],
        "uuid": "c128116c-1954-42c2-aca8-f7c52c319bd1",
        "attr": {
            "device_role": [
                "cpe"
            ],
            "pep_roles": []
        },
        "uri": "/topology-service/device/c128116c-1954-42c2-aca8-f7c52c319bd1"
    }
],
"state": "CONFIGURATION-FAILED",
"latitude": "39.7837304",

```

```
    "parent_uri": "/topology-service/project/875578ab-395a-4554-8051-05803312778d"  
  }  
}
```

Obtaining Tenant Details using the Tenant Object ID

The “Get site object details using to the site object id” API above returned details about the parent object (tenant) in the field "parent_uuid": "acb9b7d4-3388-4509-bbc9-44971518b4d1". This information can be used to find information about the tenant object.

To obtain the tenant mapping ID with TSSM, send a GET request to:

```
https://<server-address>/tssm/customer/<customer_object_id>
```

JSON

Example:

```
https://10.208.135.53/tssm/customer/acb9b7d4-3388-4509-bbc9-44971518b4d1
```

JSON

Sample JSON Response

```
{
  "customer": {
    "tenant_type": "medium",
    "parent_uuid": "875578ab-395a-4554-8051-05803312778d",
    "parent_type": "project",
    "sites": [
      {
        "to": [
          "default-domain",
          "test",
          "test",
          "london"
        ],
        "uri": "/tssm/site/51778429-e8ee-446a-8ad0-592056f8b77a",
        "uuid": "51778429-e8ee-446a-8ad0-592056f8b77a"
      }
    ],
    "tenant_existed": "created",
    "user_defined_properties": [
      {
        "name": "foobar_tenant_id",
        "value": "WF12345"
      }
    ],
    "display_name": "test",
    "tenantid": "875578ab395a4554805105803312778d",
    "properties": {
      "property": [
        {
          "name": "users",
          "value": [
            "admin@test.com"
          ]
        },
        {
          "name": "default-tenant-topology",
          "value": "mesh"
        },
        {
          "name": "default-fullmesh-type",
          "value": "dense"
        },
        {
          "name": "default-max-links-per-site-in-fullmesh",
          "value": 2
        },
        {
          "name": "default-tunnel-type",
          "value": "GRE_IPSEC"
        }
      ]
    }
  }
}
```

```

    ]
  },
  "name": "test",
  "fq_name": [
    "default-domain",
    "test",
    "test"
  ],
  "uuid": "fcbacabf-1e3b-418e-b94d-d51c42197ac6",
  "vpn_id": "502da34c-774f-4e9d-ad79-1415e107f5e1",
  "uri": "/tssm/customer/fcbacabf-1e3b-418e-b94d-d51c42197ac6",
  "networks": {
    "network": [
      {
        "network_name": "test",
        "vpn_id": "e484c577-bede-47c2-a15b-ae68ed1b1f84"
      },
      {
        "network_name": "test_DefaultVPN",
        "vpn_id": "502da34c-774f-4e9d-ad79-1415e107f5e1"
      }
    ]
  },
  "deployment_scenario": "managed_wan_v2",
  "parent_uri": "/tssm/project/875578ab-395a-4554-8051-05803312778d"
}

```

2.6.7. Getting the list of Audit Logs

To get the list of all Audit Log records which are saved in CSO database, send a GET request to:

<https://<server-address>/ems-central/audit-log?detail=true>

JSON

Example:

Sample JSON Response

```

{
  "total": 1,
  "audit-log": [
    {
      "status": "success",
      "region_id": "central",
      "display_name": "audit_log_9c660952-38ed-415d-a11d-78238da90ed0",
      "service_name": "IAMSVC-NOAUTH",
      "object_type": "authentication",
      "parent_type": "project",
      "user_name": "cspadmin",
      "perms2": {
        "owner": "ebd10158c37b4a118ae00b446772146a",
        "owner_access": 7,
        "global_access": 0,
        "share": [
          {
            "tenant_access": 4,
            "tenant": "c127e0655ac44a0e813b3c5f3df297fe"
          }
        ]
      },
      "fq_name": [
        "default-domain",
        "Bengaluru",
        "audit_log_9c660952-38ed-415d-a11d-78238da90ed0"
      ],
      "message": "The user cspadmin has successfully logged into the context Bengaluru",
      "parent_uuid": "ebd10158-c37b-4a11-8ae0-0b446772146a",
      "uuid": "8f032ff3-3f04-4f77-a6f3-4930a640c4a5",
      "user_id": "a5532d36-e51f-4465-9660-ab70113062dc",
      "name": "audit_log_9c660952-38ed-415d-a11d-78238da90ed0",
      "tenant_id": "ebd10158c37b4a118ae00b446772146a",
      "namespace": "iamsvc-noauth",
      "uri": "/ems-central/audit-log/8f032ff3-3f04-4f77-a6f3-4930a640c4a5",
      "object_id": "a5532d36-e51f-4465-9660-ab70113062dc",
      "user_ip": "10.215.153.124",
      "object_name": "cspadmin",
      "id_perms": {
        "enable": true,
        "uuid": {
          "uuid_mslong": 10305133094134632311,
          "uuid_lslong": 12030039502933247141
        }
      },
      "created": "2019-05-02T06:10:19.834350",
      "description": null,
      "creator": "cspadmin",
      "user_visible": true,
      "last_modified": "2019-05-02T06:10:19.834350",
    }
  ]
}

```

```

        "modifier": "cspadmin",
        "permissions": {
            "owner": "cspadmin",
            "owner_access": 7,
            "other_access": 7,
            "group": "_member_",
            "group_access": 7
        }
    },
    "task_name": "login and context switch",
    "timestamp": 1556777419607,
    "type": "audit_log",
    "parent_uri": "/ems-central/project/ebd10158-c37b-4a11-8ae0-0b446772146a"
}
]
}

```

2.6.8. Purging and archiving Audit Logs

When system run a very long time, there may be many audit logs, so customer can use this rpc to cleanup old audit logs to release more CSO space. During purge, if customer select archive, CSO will backup the audit log to a remote server or to local swift server.

To purge the Audit Logs, send a POST request to:

https://<server_address>/ems-central/purge_audit_log

JSON

Example:

JSON Object Input

```

{
  "input": {
    "older_than_days": 15,
    "isArchive": true,
    "archive_mode": "REMOTE",
    "archive_usr_name": "root",
    "archive_usr_pwd": "Embe1mpls",
    "archive_svr_ip": "10.204.251.95",
    "archive_svr_path": "/root"
  }
}

```

JSON

Sample Response

```
{
  "output": {
    "result": "success",
    "job_id": "86421d4e-c873-4de9-b3d8-a401b8edc512"
  }
}
```

2.6.9. Displaying uCPE Device Alert Information

Alerts and alarms can be configured in the system by creating monitoring objects and waiting for alert notifications on RabbitMQ message bus.

Subscribe to the following RabbitMQ parameters for alert information:

- Name - **internal_alert_exchange**
- Exchange type - topic
- Routing key – #

You can either use alert queries or listen to alert notifications to obtain alert information.

Obtaining Alert Information Through Query

In the CSP solution, the Fault Management and Performance Monitoring (FMPM) microservice is responsible for fault management. Alerts and alarms can be raised, as a response to faults. The `alert_object` objects are first-class objects and can be queried through a rich set of APIs (for details, refer to CSP-HAPI documentation that allows multiple filters based on the object fields and type). `Alert_objects` are treated as immutable internally.

The FMPM microservice also reflects the status of fault as `alert_status_object`. Similar to `alert_object`, these are first-class objects in the CSP and can leverage the rich set of APIs from CSO and NSC. The following example highlights the difference between these two objects:

- When the device does not respond:
- One `alert_object` is created with severity as “critical”
- One `alert_status_object` is created with severity as “critical”
- When the device starts to respond:
- Another `alert_object` is created with severity as “normal” (indicates “clearing”)

- Previous “alert_status_object” is modified and the following severity is updated:
 - severity (“normal”)
- last_update_time (as the second timestamp)
- counter (2)

Example: **alert_status_object**

```
{
  "object_type": "UCPE_DEVICE",
  "alert_type": "host",
  "alert_origin": "host",
  "severity": "critical",
  "start_time": 1465910341,
  "reason": "Down",
  "id": "cb9acdf7-b341-44a7-b987-788dc21a41b0 ",
  "object_id": "dd52c5fd-c6e8-4233-a244-f3c7f9436252",
  "device": "cb9acdf7-b341-44a7-b987-788dc21a41b0",
  "tenant": "cefdd68f-19b4-4ef7-9f31-313d9f089416",
  "region": "d5ad04bf-7e8d-4ee0-a3e8-8d30a6a7c38f",
  "site": "329ddc02-a6f3-4d9c-989d-dedad8129845",
  "pop": "38ba27f7-9084-4816-aa63-f116fe3e301b"
}
```

JSON

Support for asynchronous notification of alerts from CSO Release 3.1 onwards. In releases before CSO Release 3.1, alert information needs to be explicitly queried with the FMPM service. The query requires device object ID in EMS service as input parameter.

Given the tenant name and site name perform the following steps to get alert information about the device object at site.

Step 1: Obtaining the Enterprise Topology Site ID

Use the following information to obtain the enterprise topology site ID of a given tenant name and site name:

Resource_name: topo_site_uuid

Rest_api: service_name: local.csp-topology

Method: POST

URI: /topology-service/fqname-to-id

http_body:

JSON

```
{
  "fq_name": ["default-domain", "{{tenant_name}}", "{{site_name}}"],
  "type": "site"
}
```

Step 2: Obtaining the Device Object in Topology Service from Site Object in Enterprise Topology

Use the following information to obtain the device object in topology service from site object in enterprise topology:

Resource_name: topo_dev

Input_resources:- topo_dev

Rest_api: service_name: local.csp-topology

Method: GET

URI:

```
/topology-service/device?back_ref_id={{topo_site_uuid}}
```

JSON

Step 3: Obtaining the EMS Device Object ID from the Device Object in Topology Service

Send the following information to obtain the EMS device object ID from device object in topology service.

```
Device-id is topo_dev.db_id
```

JSON

Step 4: Obtaining the Alert Status on Device using the Following Query to FMPM Service

Send the following query to the FMPM microservice to obtain alert status on the device.

Method: GET

```
URL:/fmpm-provider/alter_status_object?count=False&filter=id+eq+<<device-
id>>+and+severity+eq+critical+alert_type+eq+host
```

JSON

Sample JSON Output

JSON

```

{{
  'fq_name': '2ce1fb29-a2aa-45a9-a3e4-400efb720696', #fully qualified name of device
  'uuid': '71c95689-0c74-470e-84d9-179847fe7e31', #alert object uuid
  'uri': '/fmpm-provider/alert_object/71c95689-0c74-470e-84d9-179847fe7e31'
#url to get more alert details
}}
```

If device is reachable, then the API returns an empty list in the response.

If the list is not empty, use the URI listed in the alert object. The API fetches more information about the alert by performing a GET operation using the URI displayed in the preceding output.

Sample: Alert Object

JSON

```

{
  "alert_object":{
    "alert_type":"service",
    "fq_name":"1ba8e64a-c38a-4ef9-813f-a1b40833cce8",
    "severity":"critical",
    "start_time":1474105605,
    "object_type":"UCPE_DEVICE",
    "site":"SITE-001",
    "object_id":"/VSRX/ipsec/vpn/default-vpn/status",
    "server":"c78ee64c-ac08-45fb-a5c4-1d86f9aa3ba4",
    "reason":["'131073 is inactive'"],
    "pop":"POP1",
    "device":"c78ee64c-ac08-45fb-a5c4-1d86f9aa3ba4",
    "region":"dc2",
    "id":"1ba8e64a-c38a-4ef9-813f-a1b40833cce8",
    "tenant":"TENANT-001"
  }
}
```

Use the following API to obtain the current overall status of the device issue:

JSON

```
GET "/ems-central/device/{deviceId}" get "management_state"
```

Sample Output

```

{
  "device": {
    "parent_uuid": "8d3d2314-a51c-445a-a2d7-7a3aba60e095", # device id in topology
    service?
    "display_name": "Juniper-site-13-NFX-250",
    "parent_type": "project",
    "system_info": {
      "serial_number": "123123123",
      "host_name": "default_host"
    },
    "perms2": {
      "owner": "1c01e0503c7b4bec9915dc56087667e6",
      "owner_access": 7,
      "global_access": 7,
      "share": []
    },
    "fq_name": [
      "default-domain",
      "Juniper",
      "Juniper-site-13-NFX-250"
    ],
    "management_state": "EXPECTED", # current state of the device
    "name": "Juniper-site-13-NFX-250",
    "device_family_refs": [
      {
        "to": [
          "default-domain",
          "juniper-nfx"
        ],
        "uuid": "60465774-e602-40ab-bb53-0d6e2fcadf98", #device family id
        "attr": null,
        "uri": "/ems-central/device-family/60465774-e602-40ab-bb53-0d6e2fcadf98"
        #uri to get device family info.
      }
    ],
    "uuid": "54839c47-2a06-4bd2-b884-41216787df53", #device uuid?
    "region": "regional",
    "uri": "/ems-central/device/54839c47-2a06-4bd2-b884-41216787df53", #uri to get
    device info
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 6089882950596709000,
        "uuid_lslong": 13295823611631230000
      },
      "created": "2016-10-06T18:22:43.207968",
      "description": null,
      "creator": "tenant-ABCcorp-admin",
      "user_visible": true,
      "last_modified": "2016-10-06T18:22:43.207968",

```

```

    "permissions": {
      "owner": "tenant-ABCcorp-admin",
      "owner_access": 7,
      "other_access": 7,
      "group": "_member_",
      "group_access": 7
    }
  },
  "abstract_configs": [
    {
      "to": [
        "default-domain",
        "Juniper",
        "Juniper-site-13-NFX-250",
        "stageone_config"
      ],
      "uri": "/ems-central/abstract-config/b53b17a5-b4d0-4c39-ac68-980e85176f02",
      "uuid": "b53b17a5-b4d0-4c39-ac68-980e85176f02" #abstract config id
    }
  ],
  "parent_uri": "/ems-central/project/8d3d2314-a51c-445a-a2d7-7a3aba60e095",
  "unique_id": "123123123"
}

```

Use the following API to obtain information about the topology site issue:

```

resource_name: topo_site_uuid
rest_api:
  service_name: local.csp-topology
  method: POST
  uri: /topology-service/fqname-to-id
  http_body: |
    {
      "fq_name": ["default-domain", "{{tenant_name}}", "{{site_name}}"],
      "type": "site"
    }

```

JSON

Use the following API to obtain information about the topology site including alarms issue:

```
GET "/data-view-central/tenant-sites/{topologySiteId}" get number of critical alarms
```

JSON

Sample Output

JSON

```
{
  "tenant-sites": {
    "status": "activated",
    "count_critical": 0, # Count of critical alarms
    "display_name": "Juniper-site-13",
    "tenant_name": "Juniper",
    "href": "http://localhost:82/data-view-central/tenant-sites/09cbbefa-dbb3-4302-bad6-56ab5c84d0d0", #Question: what is this reference? Is this reg to tenant page in dataview?
    "site_type": "on_premise",
    "ems_id": "2288ff29-254d-4fad-a549-03002b84cced",
    "name": "Juniper-site-13",
    "count_minor": 0,
    "fq_name": [
      "Juniper-site-13"
    ],
    "uuid": "09cbbefa-dbb3-4302-bad6-56ab5c84d0d0", #topo site uuid
    "coordinates": "",
    "pop_name": "pop_pe1",
    "number_of_services_activated": 0,
    "tssm_site_id": "34c710cc-db7b-461d-aafa-aa732266d5a8",
    "pnf_id": "",
    "count_major": 0,
    "tenant_uuid": "0aa4286c-274a-40e5-96fe-cbf20db1838c",
    "location": "site1 street, site1 ciity"
  }
}
```

Use the following API to obtain monitored data information the uCPE device network service.

POST `/fmpm-provider/get_perfparams"`

JSON

Input Payload

```
{
  "input": {
    "ns_id": nsId
  }
}
```

JSON

Sample Response

```
{
  "output": {
    "status": "success",
    "vnf_params": [
      {
        "status": "up",
        "params": {
          "vnf": [],
          "uptime": {
            "percentage": "100.0",
            "absolute": "2 days, 19:41:24"
          },
          "sessions": "5",
          "timestamp": "1475894131",
          "rate": {
            "right": {
              "input": "0.1 Mbps",
              "ifname": "ge-0/0/1",
              "output": "0.39 Mbps"
            },
            "left": {
              "input": "0.0 Mbps",
              "ifname": "ge-0/0/0",
              "output": "0.0 Mbps"
            }
          }
        },
        "vnf-image": "vsrx"
      },
      {
        "device_id": "afe7ce25-2959-4d48-8900-f815140e741e"
      }
    ],
    "ns_id": null
  }
}
```

Obtaining Alert Information through Alert Notifications

From JCS release 3.1 onwards alert information can be gathered using notifications. Alerts and alarms can be received by creating monitoring objects and waiting for alert notifications on the RabbitMQ message bus.

Subscribe to the following RabbitMQ parameters for alert information:

- Name - **internal_alert_exchange**
- Exchange Type - topic
- Routing key – #

The following monitoring objects are supported in JCS 3.3:

- UCPE_DEVICE – uCPE device monitoring object
- UCPE_VNF – monitoring object for VNF deployed on the device
- VCPE_VNF - monitoring object for VNF deployed with centralized services
- CPE_DEVICE - monitoring object for vCPE device (centralized services)
- HUB - monitoring object for hub device
- NFX_CLUSTER_NODE - monitoring object for NFX cluster node (dual CPE)
- NFX_CLUSTER - monitoring object for NFX cluster device (dual CPE)
- SRX_CLUSTER - monitoring object for SRX cluster device (dual CPE)
- SRX_CLUSTER_NODE - monitoring object for SRX cluster device (dual CPE)

The following list provides the list of monitoring objects that are supported in addition to the mandatory parameters when you create the monitoring object:

Monitoring object for uCPE device

```
ucpe_device_mandatory_params = {'region',  
                                'pop',  
                                'tenant',  
                                'site',  
                                'id',  
                                'object_type'}
```

JSON

Monitoring object for virtual CPE (vCPE) device

(Relevant only when using centralized services).

```
cpe_device_mandatory_params = {'region',  
                                'pop',  
                                'tenant',  
                                'site',  
                                'id',  
                                'object_type',  
                                'image_type',  
                                'components'}
```

JSON

Monitoring the Objects for VNF Deployed on uCPE Devices

JSON

```
ucpe_vnf_mandatory_params = {'region',  
                              'pop',  
                              'tenant',  
                              'site',  
                              'ip',  
                              'id',  
                              'object_type',  
                              'network_service',  
                              'server',  
                              'image_type',  
                              'components'}
```

Monitoring the Objects for VNF Deployed on vCPE Devices

(Relevant only for centralized services).

JSON

```
vcpe_vnf_mandatory_params = {'region',  
                              'pop',  
                              'tenant',  
                              'site',  
                              'ip',  
                              'id',  
                              'object_type',  
                              'network_service',  
                              'image_type',  
                              'components'}
```

Monitoring Object for Hub Device.

JSON

```
hub_device_mandatory_params = {'region',  
                                'tenant',  
                                'id',  
                                'object_type',  
                                'image_type',  
                                'role',  
                                'components'}
```

Monitoring Object for Cluster Node

(To be used when site has dual CPE devices in cluster mode).

```
cluster_node_device_mandatory_params = {'region',  
                                         'pop',  
                                         'tenant',  
                                         'site',  
                                         'id',  
                                         'cluster_id',  
                                         'object_type',  
                                         'image_type',  
                                         'components'}
```

Monitoring Object for Cluster Device

(To be used when site has dual CPE devices in cluster mode)

```
cluster_device_mandatory_params = {'region',  
                                    'pop',  
                                    'tenant',  
                                    'site',  
                                    'id',  
                                    'cluster_nodes',  
                                    'cluster_id',  
                                    'object_type',  
                                    'image_type',  
                                    'components'}
```

You can also create monitoring objects through a batch command as shown in the following example:

```
"input":{
  "services":[
    {
      "service_type":"CHECK",
      "service_name":"/SRX/interface/WAN_1",
      "action":"ADD",
      "object_id":"e812dec0-5fda-4633-9359-f540c6c96cf2",
      "attributes":{"
        "local_breakout":"no",
        "service_value":"WAN_1",
        "interface_name":"ge-0/0/3",
        "service_category":"underlay",
        "component_name":"GWR"
      }}
    },
    {
      "service_type":"CHECK",
      "service_name":"/SRX/interface/WAN_0",
      "action":"ADD",
      "object_id":"e812dec0-5fda-4633-9359-f540c6c96cf2",
      "attributes":{"
        "local_breakout":"no",
        "service_value":"WAN_0",
        "interface_name":"ge-0/0/2",
        "service_category":"underlay",
        "component_name":"GWR"
      }}
    },
    {
      "service_type":"CHECK",
      "service_name":"/SRX/interface/WAN_0",
      "action":"ADD",
      "object_id":"e812dec0-5fda-4633-9359-f540c6c96cf2",
      "attributes":{"
        "local_breakout":"no",
        "service_value":"WAN_0",
        "interface_name":"ge-0/0/2",
        "service_category":"underlay",
        "component_name":"GWR"
      }}
    },
    {
      "service_type":"CHECK",
      "service_name":"/JCP/interface/WAN_0",
      "action":"ADD",
      "object_id":"e812dec0-5fda-4633-9359-f540c6c96cf2",
      "attributes":{"
        "local_breakout":"no",
        "service_value":"WAN_0",
        "interface_name":"ge-0/0/8",
```

```

        "service_category": "underlay",
        "component_name": "JCP"
    },
    {
        "service_type": "CHECK",
        "service_name": "/JCP/interface/WAN_1",
        "action": "ADD",
        "object_id": "e812dec0-5fda-4633-9359-f540c6c96cf2",
        "attributes": {
            "local_breakout": "no",
            "service_value": "WAN_1",
            "interface_name": "ge-0/0/9",
            "service_category": "underlay",
            "component_name": "JCP"
        }
    },
    {
        "service_type": "CHECK",
        "service_name": "/JCP/interface/WAN_0",
        "action": "ADD",
        "object_id": "e812dec0-5fda-4633-9359-f540c6c96cf2",
        "attributes": {
            "local_breakout": "no",
            "service_value": "WAN_0",
            "interface_name": "ge-0/0/8",
            "service_category": "underlay",
            "component_name": "JCP"
        }
    },
    {
        "service_type": "CHECK",
        "service_name": "/SRX/interface/GWR.WAN_1.DATA/dhcp_status",
        "action": "ADD",
        "object_id": "e812dec0-5fda-4633-9359-f540c6c96cf2",
        "attributes": {
            "service_value": "WAN_1",
            "interface_name": "ge-0/0/3.0",
            "service_category": "underlay",
            "component_name": "GWR"
        }
    },
    {
        "service_type": "CHECK",
        "service_name": "/SRX/interface/GWR.WAN_0.DATA/dhcp_status",
        "action": "ADD",
        "object_id": "e812dec0-5fda-4633-9359-f540c6c96cf2",
        "attributes": {
            "service_value": "WAN_0",
            "interface_name": "ge-0/0/2.0",

```

```

        "service_category": "underlay",
        "component_name": "GWR"
    },
    {
        "service_type": "CHECK",
        "service_name": "/SRX/interface/GWR.WAN_0.OAM/dhcp_status",
        "action": "ADD",
        "object_id": "e812dec0-5fda-4633-9359-f540c6c96cf2",
        "attributes": {
            "service_value": "WAN_0",
            "interface_name": "ge-0/0/2.0",
            "service_category": "underlay",
            "component_name": "GWR"
        }
    },
    {
        "service_type": "CHECK",
        "service_name": "/JCP/interface/LAN_1",
        "action": "ADD",
        "object_id": "e812dec0-5fda-4633-9359-f540c6c96cf2",
        "attributes": {
            "service_value": "ge-0/0/1",
            "link_name": "LAN_1",
            "service_category": "LAN",
            "component_name": "JCP"
        }
    }
]
}

```

The following example provides information about an alarm object received in the notification bus:

Service Alarms

```

{
  "input":{
    "alert_obj":{
      "category":"alarm",
      "alert_type":"service",
      "severity":"critical",
      "sub_system":"CSO",
      "start_time":1520270389,
      "object_type":"SRX_CLUSTER",
      "site":"5bebdea3-bd8d-4d77-bca9-24e5d5e659b7",
      "object_id":"/SRX/gre-ipsec/vpn/f6d51f08484caaef9e7102015bef2b3e",
      "server":"81c84a65-0eef-4baa-b044-7b0e784def04",
      "source":"device",
      "reason":"IPSEC TUNNEL DOWN",
      "pop":"5b8c7355-d49f-4fcb-812c-5b12d12adaf6",
      "device":"81c84a65-0eef-4baa-b044-7b0e784def04",
      "attributes":{
        "region_display_name":"regional",
        "src":{
          "site_name":"dcpe-spoke",
          "device_name":"dcpe-spoke",
          "role":"spoke",
          "wan_name":"WAN_1",
          "overlay_interface":"gr-0/0/0.4001",
          "underlay_interface":"reth1"
        },
        "interface_name":"gr-0/0/0.4001",
        "underlay_link_name":"WAN_1",
        "dst":{
          "site_name":"dcpe-hub",
          "device_name":"dcpe-hub",
          "role":"hub",
          "wan_name":"WAN_1",
          "overlay_interface":null,
          "underlay_interface":"ge-0/0/3"
        },
        "link_encapsulation":"GRE_OVER_IPSEC",
        "pop_display_name":"regional",
        "service_value":"f6d51f08484caaef9e7102015bef2b3e",
        "service_category":"overlay",
        "overlay_link_name":"DCPE-SPOKE_WAN_1_DCPE-HUB_WAN_1_GRE_IPSEC_0",
        "peer_id":"c96843fb-e4e0-4527-bdd8-d8f86612af06",
        "component_name":"SRX"
      },
      "region":"1c679272-41fd-460b-848c-cfadb3a540bd",
      "id":"f25fd6f4-29c5-48e7-83ed-2f94c4aef5af",
      "tenant":"bdc529a2-f325-4eb6-bae4-ca1955d59834"
    }
  }
}

```

```

    }
  }

```

Host Alarms

JSON

```

{
  "input":{
    "alert_obj":{
      "category":"alarm",
      "alert_type":"host",
      "severity":"critical",
      "sub_system":"CSO",
      "start_time":1520409563,
      "object_type":"SRX_CLUSTER",
      "site":"5bebdea3-bd8d-4d77-bca9-24e5d5e659b7",
      "object_id":"81c84a65-0eef-4baa-b044-7b0e784def04",
      "server":"81c84a65-0eef-4baa-b044-7b0e784def04",
      "source":"device",
      "reason":"Host is DOWN",
      "pop":"5b8c7355-d49f-4fcb-812c-5b12d12adaf6",
      "attributes":{
        "region_display_name":"regional",
        "pop_display_name":"regional"
      },
      "region":"1c679272-41fd-460b-848c-cfadb3a540bd",
      "id":"eb65bf1b-a187-4972-a044-ee32de73b9a4",
      "tenant":"bdc529a2-f325-4eb6-bae4-ca1955d59834"
    }
  }
}

```

2.6.10. Device Profile

Device Profile models device EMS operations with a list of workflows.

Workflow examples:

- Zero touch provisioning
- VPN links bring-up
- Stage2-workflows (creation of VLANs, and DHCP configuration)

Juniper Networks defines the device profiles for supported devices, and is packaged as part of the NSC product. The Juniper PS team can extend or customize device profiles in the field, as and when required. Most of the workflows are internally used by NSC during NFX bring-up. Only

stage2-workflows are exposed to the portal layer directly for enabling configuration of the LAN network behind the NFX device by the customer administrator. Juniper builds the device profile stage2 workflows based on the input from vendors partnering for higher layer applications (portals).

Complete the following procedure to configure device from the higher layer applications using NSC:

Step 1 - Juniper to build device profile workflows needed for higher layer applications

Higher layer application must specify the configuration screens provided in the customer portal and input collected. Higher layer application must also specify if any of the configuration parameters need to be auto-resolved using the data provided during site or tenant creation. Based on that data, Juniper Networks builds the workflow needed to perform such configuration. Higher layer application requires to be aware of the workflow identifiers and associate them with the appropriate Web UI screens.

Step 2 - Resolve Device Profile

When the user selects a device to configure from the portal, the system needs to identify the device profile associated with site, and the corresponding workflow associated with the Web UI screen. Initiate the following the API to resolve the device profile. This API lists the configuration templates that can be later invoked to build abstract configuration, and push it to the device.

To resolve a device profile, send a POST request with the following JSON-formatted payload:

```
POST /dms-central/resolve_device_profile
```

JSON

JSON Object Input

```
{
  "input": {
    "device_profile_id": "deviceProfileId",
    "workflow_name": "stage-2-config"
  }
}
```

JSON

Step 3 - Create and Update Abstract configuration

Build abstract configuration for a template by providing the values for configuration parameters. PUT operations are used to save the configuration when the user clicks **Save** in the Web UI. When the Web UI restarts, the saved configuration is retrieved and displayed.

To create abstract configuration, send a POST request with the following JSON-formatted payload:

POST/PUT/ems-central/abstract-config

JSON

JSON Object Input

```
{
  "abstract-config": {
    "parent_type": "device",
    "fq_name": [
      "default-domain",
      "default-project",
      "d59",
      "JUNOS/snmp-config"
    ],
    "parent_uuid": "79e1e75f-c81b-4ab9-8c39-a9ac42b65451",
    "candidate_config": {
      "config_blob": "{\"snmp\":{\"location\":\"test_loc\"}}"
    },
    "template_refs": [
      {
        "to": [
          "snmp_location_template"
        ],
        "uuid": "8808c584-1849-4792-95b6-dd145fffac55"
      }
    ]
  }
}
```

JSON

Step 4 - Get Abstract Configuration

The following CRUD API can be used to retrieve the saved configuration values. It is useful, when you restart the Web UI.

To obtain the abstract configuration, use the following CRUD API:

GET /ems-central/abstract-config/{id}

JSON

Step 5 - Publish abstract configuration

When you complete entering the configuration variables, and click **apply** in the Web UI, the configuration is pushed to the device using the publish and deploy APIs. The publish API takes the abstract configuration, renders the configuration by performing parameter substitution, and keeps it ready for pushing it to the device.

To publish the abstract configuration, send a POST request with the following JSON-formatted payload:

POST /cms-central/publish_configuration

JSON

JSON Object Input

```
{
  "input": {
    "abstract_configs" : [
      {
        "fqname": [
          "default-domain",
          "default-project",
          "d59",
          "JUNOS/snmp-config"
        ]
      }
    ]
  }
}
```

JSON

Step 6 - Deploy Abstract Configuration

The deploy API gathers all the rendered configurations, and pushes them to the device.

To deploy the abstract configuration, send a POST request with the following JSON-formatted payload:

POST /cms-central/deploy_configuration

JSON

JSON Object Input

JSON

```
{
  "input": {
    "abstract_configs" : [
      {
        "fqname": [
          "default-domain",
          "default-project",
          "d59",
          "JUNOS/snmp-config"
        ]
      }
    ],
    "url" : "amqp://guest:guest@xx.xxx.xxx.xxx:5672/?
exchange=myexchange&routing_key=check"
  }
}
```

Step 7 - Notification to Receive Device Configuration Deploy Status

The following is an example of a notification to receive the device configuration deploy status information:

JSON

```
notification_deploy_configuration_response {
  description
    "This notification is sent response to the deploy_configuration RPC";
  leaf requestid {
    type yang:uuid;
    description
      "A generated unique id";
  }
  leaf status {
    type ems-types:StatusType;
    description
      "indicates success/failure of the deploy API";
  }
  leaf description {
    type string;
    description
      "Holds the generic error message or warnings";
  }
  list details {
    key "abstract_config_uuid";
    uses deploy_configuration_result;
  }
}
}
```

Information Retrieval Using Audit Logs as Starting Point

To retrieve information using audit logs as the starting point, use the following API:

```
Routing keys = site.create, site.configure, site.provision
```

JSON

Sample JSON Response

```
{
  "status": "success",
  "username": tenant-ABCcorp-admin,
  "service_name": "csp-tssm",
  "timestamp": "2017-12-17T19:46:01.103Z",
  "message": "Configure Site",
  "task_name": "csp.tssm_create_sites",
  "namespace": "tssm",
  "object_type": "site",
  "object_id": " ad67d0d5-2a8a-41c1-b0a7-2fdd44af5023"
}
```

JSON

2.7. Site Template

2.7.1. Overview

A site template helps to specify values for many of the attributes used to add a site. It allows to create a template for site and then allows you to deploy it across multiple sites that share the same set of values (for attributes already specified in the site template) and only specify values for site-specific attributes. Site templates are available only for on-premise spoke sites.

2.7.2. Creating a site using Site Templates

To create a site object using site template, send a POST request with the following JSON-formatted payload:

```
https://<cso-host>/tssm/site-template
```

JSON

NOTE: cso-host is the domain name, it changes with the change of instances in CSO.

JSON Object Input

```
{
  "site-template": {
    "type": "CUSTOM",
    "template_name": "SdwanSRX",
    "fq_name": [
      "default-domain",
      "tenant_1444",
      "SdwanSRX"
    ],
    "parent_type": "customer",
    "site": [
      {
        "site_name": "SdwanSRX",
        "site_basic_properties": {
          "0": {
            "lan_segment_type": "direct",
            "vlan": 784,
            "dhcp": false,
            "department": "D1",
            "lan_segment_name": "lan1",
            "lan_ports": [
              "LAN_3"
            ]
          },
        },
        "site_group": [],
        "dvpn_params": {
          "create_dvpn_threshold": "5",
          "delete_dvpn_threshold": "2"
        },
        "site_address": {
          "country": "US"
        },
        "site_name": "SdwanSRX",
        "site_role": "SPOKE",
        "network_seg": true,
        "cloud_service": "EDGE",
        "site_type": "on_premise",
        "topology": "standalone",
        "device_template": [
          {
            "template_name": "SRX_Advanced_SDWAN_CPE_option_1",
            "device_name": "SdwanSRX",
            "wan_link_info": [
              {
                "wan_link": "WAN_0",
                "wan_link_type": "Internet",
                "cost_currency": "USD",
                "local_breakout_enabled": false,
                "provider": "ISP1",
                "cost": 800,
              }
            ]
          }
        ]
      }
    ]
  }
}
```

```

        "default_link": false,
        "backup_link": false,
        "preferred_breakout_link": false,
        "subscribed_bandwidth": 1000
        "enable_pppoe": false
    },
    {
        "wan_link": "WAN_1",
        "wan_link_type": "Internet",
        "cost_currency": "USD",
        "local_breakout_enabled": false,
        "provider": "ISP1",
        "cost": 800,
        "default_link": false,
        "backup_link": false,
        "preferred_breakout_link": false,
        "subscribed_bandwidth": 1000
        "enable_pppoe": false
    }
],
"lan_segment": [
    {
        "lan_segment_type": "direct",
        "vlan": 784,
        "dhcp": false,
        "department": "D1",
        "lan_segment_name": "lan1",
        "lan_ports": [
            "LAN_3"
        ]
    }
]
},
"site_deployment_capabilities": [
    "SDWAN"
],
},
"properties": {
    "property": [
        {
            "name": "site_advanced_config",
            "value": {
                "nameserver": [
                    "8.8.8.8",
                    "8.8.4.4"
                ],
                "ntpserver": "time.google.com",
                "timezone": "PST"
            }
        }
    ]
}

```

```

    }
  ]
},
"on_premise_site_info": {
  "site_role": "spoke",
  "ha_info": {
    "ha_topology": "STANDALONE"
  },
  "device": [
    {
      "device_family": "juniper-srx",
      "device_template": "SRX_Advanced_SDWAN_CPE_option_1",
      "device_template_name": "SRX_Advanced_SDWAN_CPE_option_1",
      "device_details": {
        "auto_activate": true,
        "boot_image": ""
      },
      "wan_link": [
        {
          "wan_link_name": "WAN_0",
          "wan_link_type": "Internet",
          "used_for_oam": true,
          "local_interface": "ge0/0/0",
          "address_assignment": "DHCP",
          "preferred_breakout_link": false,
          "used_for_meshing": false,
          "traffic_type": "DATA_ONLY",
          "backup_link": false,
          "default_link": false,
          "vpn": [
            {
              "vpn_name": "D1"
            }
          ]
        }
      ],
      {
        "wan_link_name": "WAN_1",
        "wan_link_type": "Internet",
        "local_interface": "ge-0/0/1",
        "address_assignment": "STATIC",
        "preferred_breakout_link": false,
        "used_for_meshing": false,
        "used_for_oam": false,
        "traffic_type": "DATA_ONLY",
        "backup_link": false,
        "default_link": false,
        "vpn": [
          {
            "vpn_name": "D1"
          }
        ]
      }
    }
  ]
}

```

```

    ]
  }
]
"oam_traffic": {},
"device_role": "SDWAN",
"device_template_name": "SRX_Advanced_SDWAN_CPE_option_1"
}
],
"gateway_sites": [
  {
    "gateway_name": "GW11444",
    "gateway_role": "PRIMARY_GW"
  }
],
"region": "regional"
}
}
],
"extra_attr";{
  "created_by": "tenant--ABCcorp-admin"
}
}
}

```

JSON Response:

```

{
  "sitetemplate": {
    "uuid": "c443bf4a6b564a2bac875bddf1391690",
    "fq_name": [
      "defaultdomain",
      "tenant_1444",
      "sdwanSRX"
    ],
    "parent_uuid": "d49e701bb7a1412fae56789de5d60c8e",
    "uri": "/tssm/sitetemplate/c443bf4a6b564a2bac875bddf1391690",
    "parent_uri": "/tssm/customer/d49e701bb7a1412fae56789de5d60c8e",
    "name": "sdwanSRX"
  }
}

```

JSON

2.7.3. Reading a site using Site Templates

To read a site object using site template, send a GET request with the following JSON-formatted payload:

JSON

```
https://<cso-host>/tssm/site-template?detail=true&exclude_refs=false
```

NOTE: `cso-host` is the domain name, it changes with the change of instances in CSO.

2.7.4. Updating a site using Site Templates

To update a site object using site template, send a PUT request with the following JSON-formatted payload:

JSON

```
https://<cso-host>/tssm/site-template/<template_uuid>
```

NOTE: `cso-host` is the domain name, it changes with the change of instances in CSO.

JSON Object Input

```

{
  "site-template": {
    "type": "CUSTOM",
    "template_name": "sdwan",
    "fq_name": [
      "default-domain",
      "tenant_127",
      "sdwan"
    ],
    "parent_type": "customer",
    "site": [
      {
        "template_name": "sdwan",
        "on_premise_site_info": {
          "device": [
            {
              "device_family": "juniper-nfx",
              "device_template": "NFX_Advanced_SDWAN_CPE_option_1",
              "device_template_name": "NFX_Advanced_SDWAN_CPE_option_1",
              "device_details": {
                "boot_image": "",
                "auto_activate": false
              },
              "wan_link": [
                {
                  "wan_link_name": "WAN_0",
                  "wan_link_type": "Internet",
                  "local_interface": "ge-0/0/10",
                  "used_for_meshing": false,
                  "address_assignment": "DHCP",
                  "access_type": "Ethernet",
                  "backup_link": false,
                  "preferred_breakout_link": false,
                  "traffic_type": "OAM_AND_DATA",
                  "default_link": false,
                  "used_for_oam": true,
                  "vpn": [
                    {
                      "vpn_name": "D1"
                    }
                  ]
                }
              ]
            }
          ],
          "oam_traffic": {},
          "device_role": "SDWAN"
        }
      ],
      "region": "regional",
      "site_role": "spoke",
      "gateway_sites": [

```

```

    {
      "gateway_name": "GW2-127",
      "gateway_role": "PRIMARY_GW"
    }
  ],
  "ha_info": {
    "ha_topology": "STANDALONE"
  }
},
"site_name": "sdwan",
"properties": {
  "property": [
    {
      "name": "site_advanced_config",
      "value": {
        "nameserver": [
          "8.8.8.8",
          "8.8.4.4"
        ],
        "ntpserver": "time.google.com",
        "timezone": "PST"
      }
    }
  ]
},
"site_basic_properties": {
  "0": {
    "lan_segment_type": "direct",
    "lan_segment_name": "lan1",
    "vlan": 1703,
    "lan_ports": [
      "LAN_0"
    ],
    "department": "D1",
    "dhcp": false
  },
  "site_name": "sdwan",
  "site_type": "on_premise",
  "cloud_service": "EDGE",
  "site_address": {
    "country": "US"
  },
  "site_deployment_capabilities": [
    "SDWAN"
  ],
  "network_seg": true,
  "device_template": [
    {
      "wan_link_info": [
        {

```

```

        "wan_link": "WAN_0",
        "wan_link_type": "Internet",
        "cost_currency": "USD",
        "access_type": "Ethernet",
        "local_breakout_enabled": false,
        "provider": "ISP1",
        "cost": 800,
        "default_link": false,
        "backup_link": false,
        "preferred_breakout_link": false,
        "subscribed_bandwidth": 1002,
        "enable_pppoe": false
    }
],
"device_name": "sdwan",
"lan_segment": [
    {
        "lan_segment_type": "direct",
        "lan_segment_name": "lan1",
        "vlan": 1703,
        "lan_ports": [
            "LAN_0"
        ],
        "department": "D1",
        "dhcp": false
    }
],
"template_name": "NFX_Advanced_SDWAN_CPE_option_1"
}
],
"site_role": "SPOKE",
"site_group": [],
"dvpn_params": {
    "delete_dvpn_threshold": "2",
    "create_dvpn_threshold": "5"
},
"topology": "standalone"
}
}
],
"extra_attr": {}
}
}

```

2.7.5. Deleting a site using Site Templates

To delete a site object using site template, send a DELETE request with the following JSON-formatted payload:

JSON

```
https://<cso-host>/tssm/site-template/<template_uuid>
```

NOTE: `cso-host` is the domain name, it changes with the change of instances in CSO.

2.7.6. Creating Spoke Site using Site Templates

To create a spoke site object using site template, send a POST request with the following JSON-formatted payload:

JSON

```
https://<cso-host>/tssm/create-sites-using-template
```

NOTE: `cso-host` is the domain name, it changes with the change of instances in CSO.

SDWAN with SRX Series device profile:

JSON Object Input

```

{
  "input": {
    "site_template_id": "cc4998ee-27dd-4c10-a24f-709792a3cdb8",
    "site_specific_data": [
      {
        "site_name": "site1",
        "site_address": {
          "country": "US"
        },
        "device_details": [
          {
            "wan_link": [
              {
                "wan_link_name": "WAN_0"
              },
              {
                "wan_link_name": "WAN_1",
                "static_ip_assignment": {
                  "ip_address": "2.1.1.2/24",
                  "gateway_ip": "1.1.1.1"
                }
              }
            ],
            "device_role": "SDWAN",
            "serial_number": "1A898BC01122",
            "oam_ip_prefix": "192.168.255.40/32",
            "lan_segment": [
              {
                "lan_segment_type": "direct",
                "lan_segment_name": "lan1",
                "vlan": 3840,
                "lan_ports": [
                  "LAN_0"
                ],
                "department": "D1",
                "dhcp": false,
                "ip_prefix": "10.1.11.1/24"
              }
            ]
          }
        ]
      }
    ]
  }
}

```

SDWAN(SRX device profile) with LAN :

JSON Object Input

JSON

```
{
  "serial_number": [
    "1A98BC355122"
  ],
  "device_role": "LAN_DEVICE_EX",
  "device_name": "switchEx1",
  "lan_segment": [],
  "dhcp_subnet": "10.1.11.0/24" => change "dhcp_subnet" to "mgmt_subnet"
}
```

Standalone LAN :

JSON Object Input

JSON

```
{
  "input": {
    "site_template_id": "5718860c-3943-4440-b11f-65b7214445b5",
    "site_specific_data": [
      {
        "site_name": "Site5",
        "site_address": {
          "country": "US"
        },
        "device_details": [
          {
            "serial_number": [
              "13462RAC4300"
            ],
            "device_role": "LAN_DEVICE_EX",
            "device_name": "switchEx5",
            "lan_segment": []
          }
        ]
      }
    ]
  }
}
```

Hybrid WAN :

JSON Object Input

```
{
  "input": {
    "site_template_id": "662b4e17-82f0-4569-8065-b3a6fc54d6b4",
    "site_specific_data": [
      {
        "site_name": "Site6",
        "site_address": {
          "country": "US"
        },
        "device_details": [
          {
            "oam_traffic": {},
            "wan_traffic": [
              {
                "wan_link_name": "WAN_0",
                "vlan_id": 52,
                "local_ip_prefix": "1.2.3.4/5",
                "remote_ip_prefix": "2.3.4.5/6"
              }
            ],
            "device_role": "HYBRID_WAN",
            "serial_number": "45373RDE735"
          }
        ]
      }
    ]
  }
}
```

Next Gen Firewall with LAN :

JSON Object Input

```
{
  "serial_number": [
    "1A98BC455122"
  ],
  "activation_code": "1234",
  "device_role": "LAN_DEVICE_EX",
  "device_name": "switch8",
  "lan_segment": [],
  "dhcp_subnet": "10.1.11.0/24"
}
```

3. NextGen FireWall (NGFW) Deployment

3.1. Overview

The next generation firewall device provides security and networking services at the perimeter or edge in virtualized private or public cloud environments. The next generation firewall device includes features such as CSO managed firewall, NAT, UTM, SSL, and device configuration of zones, routing-instances and interfaces. SRX Series services gateways or NFX Series device can be added as a next generation firewall device.

The EX Series devices are added as Layer 2 switches to deliver switching services. Contrail Service Orchestration (CSO) supports provisioning, configuring, and monitoring switching devices either behind a Juniper CPE device, or a stand-alone switch that is connected to third-party device.

Figure 11 shows a site with LAN and Firewall capabilities managed by CSO.

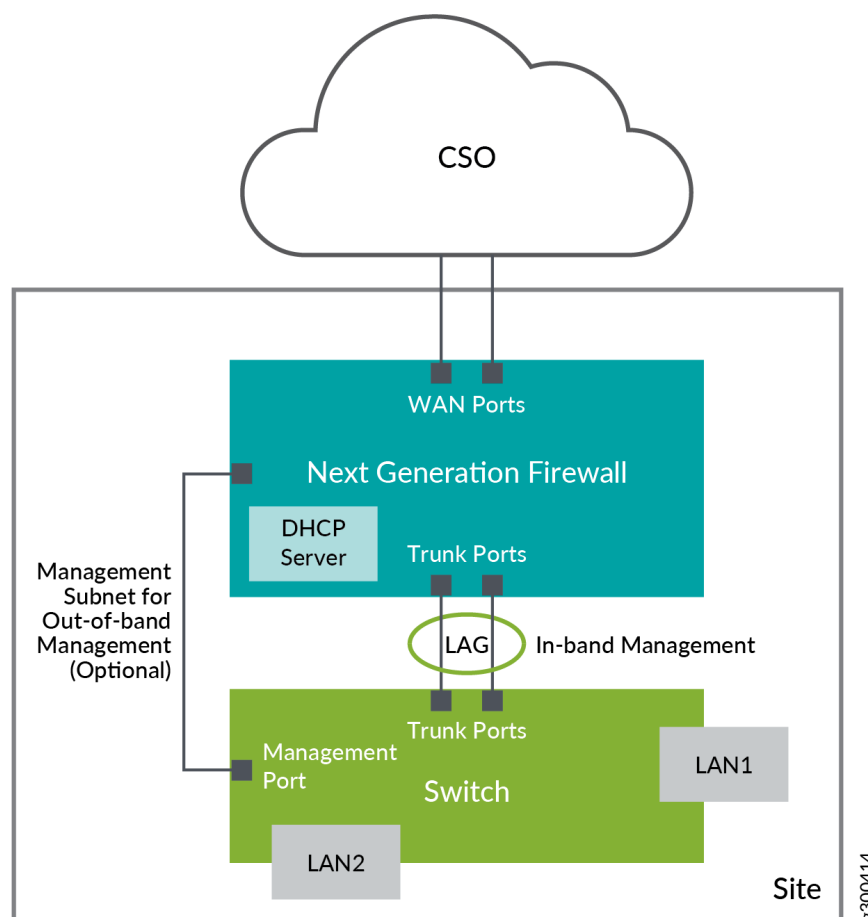


Figure 9. Site with LAN and Firewall Capabilities



You cannot add a LAN to the next-generation firewall by using CSO.

The switch and the firewall are connected to each other through trunkports. The trunkports can be combined to form a LAG for higher output and redundancy. Traffic from LAN segments connected to the switch are routed to the firewall through the trunk ports for further routing into the WAN.

You can use both in-band and out-of-band management for managing the switch. By default, the switch is managed by using in-band management, where in, the trunk ports carry the management traffic in addition to data. For out-of-band management, you can use any port on the firewall to connect with the management port of the switch.

The DHCP server, configured on the firewall, runs on the following ports:

- Trunk ports to provide DHCP information to all devices connected to the switch and the in-band management port on the switch.
- Out-of-band management port on the firewall to provide DHCP information to the management port on the switch.
- LAN ports on the firewall to provide DHCP information to the devices connected to the LAN ports.

When you perform ZTP on a site with both WAN and LAN capabilities, the following is the sequence of steps that are executed to configure the firewall, and switch:

1. After you configure a site with a firewall and switch:
 - If automatic activation is enabled for the firewall, CSO pushes the Stage-1 configuration and Stage-2 configuration on the firewall and provisions the firewall.
 - If manual activation is enabled, you must provide the device activation code. After the activation code is validated, CSO pushes the the Stage-1 configuration and Stage-2 configuration on the firewall and provisions the firewall.
2. After the firewall is provisioned the switch is provisioned as follows:
 - If zero touch provisioning (ZTP) is disabled for the switch, you must manually configure the stage-1 configuration on the switch.

After the Stage-1 configuration is committed, the switch has the outbound SSH

configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch

- If ZTP is enabled:
- If automatic activation is also enabled, CSO pushes the stage-1 and stage-2 configuration and provisions the switch.
- If automatic activation is disabled, you must manually activate the switch by providing the switch activation code.

After the switch is activated, CSO pushes the stage-1 and stage-2 configuration on to the switch for provisioning.

When you add a switch to an already provisioned site, the following sequence of steps are executed to provision the switch:

1. CSO pushes the Stage-2 configuration again onto the firewall to enable DHCP and configure LAG on the trunk ports connected to the switch.
2. The DHCP configuration on the firewall provides the IP address of CSO to the switch and the switch connects to CSO through the firewall.
3. After establishing connection with CSO:
 - If ZTP is disabled for the switch, you must manually configure the stage-1 configuration on the switch.

After the Stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch.
 - If ZTP is enabled:
 - If auto-activation is also enabled, CSO pushes the stage-1 and stage-2 configuration and provisions the switch.
 - If auto-activation is disabled, you must manually activate the switch by providing the switch activation code. After the switch is activated, CSO pushes the stage-1 and stage-2 configuration on the switch for provisioning.

3.2. Configuring a Site

To create and configure a site, send a POST request with the following JSON-formatted payload:

<https://<ip-addr>/tssm/configure-sites>

JSON

JSON Object Input

```

{
  "input": {
    "tenant_name": "sdauto_addr_055532",
    "deployment_scenario": "managed_wan",
    "site": [
      {
        "site_name": "NGFW",
        "site_basic_properties": {
          "site_group": [],
          "site_address": {
            "country": "US"
          },
          "site_name": "NGFW",
          "site_role": "SPOKE",
          "cloud_service": "EDGE",
          "site_type": "on_premise",
          "topology": "standalone",
          "device_template": [
            {
              "template_name": "SRX_Standalone_Pre_Staged_ZTP",
              "device_name": "NGFW",
              "wan_link_info": [
                {
                  "wan_link_name": "WAN_0",
                  "wan_link_type": "Internet"
                }
              ]
            }
          ]
        },
        "site_deployment_capabilities": [
          "STANDALONE_SRX"
        ]
      },
      {
        "properties": {
          "property": [
            {
              "name": "site_advanced_config",
              "value": {
                "nameserver": [
                  "8.8.8.8",
                  "8.8.4.4"
                ],
                "ntpserver": "time.google.com",
                "timezone": "PST",
                "fw_uuid": "b52327c4-27ed-488c-bf23-78dcda033681",
                "nat_id": "3812",
                "in_band_mgmt_port": "ge-0/0/0"
              }
            }
          ]
        }
      }
    ]
  }
}

```

```

    },
    "hybrid_wan_site_info": {
      "site_role": "spoke",
      "ha_info": {
        "ha_topology": "STANDALONE"
      },
    },
    "device": [
      {
        "device_family": "juniper-srx",
        "device_name": "NGFW",
        "device_template": "SRX_Standalone_Pre_Staged_ZTP",
        "device_template_name": "SRX_Standalone_Pre_Staged_NonZTP",
        "device_details": {
          "auto_activate": true,
          "boot_image": "",
          "serial_number": "75A4A326AD0D"
        },
        "inband_management_port": "ge-0/0/0",
        "firewall_policies": "b52327c4-27ed-488c-bf23-78dcda033681",
        "nat_policies": "3812",
        "fwPolicyName": "Factory_Default_Fw_Policy",
        "natPolicyName": "Factory_Default_NAT_Policy",
        "device_role": "STANDALONE_SRX"
      }
    ],
    "access_info": {
      "wan_traffic": [
        {
          "wan_link_name": "WAN_0",
          "tunnel_type": "NONE",
          "wan_link_type": "Internet"
        }
      ]
    },
    "region": "regional"
  }
}

```

Sample Response

```
{
  "output": {
    "status": "success",
    "reason": null,
    "job_id": "e25d588c-166b-4d11-94d7-c226f7bc8059"
  }
}
```

4. Service Assurance

This section gives an overview of CSO service assurance architecture and a description of alerts, alarms and metrics collected and provided by CSO system.

4.1. Overview

CPE devices are monitored using device and cloud agent depending on the device type

- In case of device agent, an agent runs in the device and periodically sends messages to CSO FMPM microservice, device is declared down when N consecutive messages from the device are not received.
- In case of cloud agent, CSO cloud agent microservice remotely polls the device using ssh connection between device and CSO DCS microservice, device is declared down if DCS reports error/timeout.

Note – one device is monitored using only one of the agents, either device or cloud.

CSO also uses certain syslogs for monitoring overlay tunnels.

Appropriate alarms (Up or Down) are generated based on the syslogs received from the device indicating state change in the tunnel status.

Note that agents also monitor same overlay tunnels but using syslogs allows faster detection of the state change (agents executes checks with pre-defined intervals so any fault will be detected at the end of that cycle) however agent monitoring provides robustness in case syslogs are missed/not-processed.

As a result of periodic status checks using above methods, CSO generates alarms for various elements. Every monitored entity (e.g. device, interface, BGP session etc.) is represented as monitored element and monitored by various CSO microservices and agents. Main components involved in generating alarm are FMPM microservices along with on-box or cloud agent. Agents use Netconf or CLI for getting the status of the

monitored element. These “CHECKS” are then used to determine state transitions. Every time a state change in the monitored element is observed, CSO creates (or updates) following objects –

1. `alert_object` - to capture the state-change of the monitored element
2. `alert_status_object` – to capture the latest state of the monitored element

These two types of objects can be used to get the latest state of the monitored element and the history of state-change transitions. For example – if a device goes down, CSO creates an `alert_object` and creates (or updates) an `alert_status_object` with “severity” as “critical”. When this device comes back up, CSO creates another `alert_object` and updates the same `alert_status_object` with “severity” as “normal” (indicating clear).

If an external sub-system or admin-portal wants to show the status of the device, it can query `alert_status_object` for that device and use “severity” field to show whether device is up or down. Additionally, if it wants to show the history of device’s status, it can query `alert_objects` for that device. [These queries are regular HAPI APIs with filters.]

CSO uses both Alarms and Alerts for various use cases e.g. SDWAN, Security Director etc. In CSO, alerts are generated as a result of user configured events (e.g. Security Director alerts) whereas alarms are generated by the system without explicit configuration from the user. Given this definition, SDWAN/SDLAN generate alarms and Security Director generates Alerts.

Important Note - From the implementation perspective, both alarms & alerts are stored as the same `alert_object/alert_status_object` which can confuse but “category” field in the object clearly indicates whether it’s an alarm or alert.

4.2. Glossary

- Agent refers to telemetry or cloud agent that periodically collects monitoring and performance data from the device and sends it to a centralized collector.
- Alarm is generated in CSO when a monitored element changes state
- Alarm Status Object keeps the current state (up OR down) of a monitored element.
- Alarm History Object captures a particular instance of state change of the monitored element.
- Cluster here refers to the cluster formed during provisioning of Dual CPE sites
- Microservice are an architectural style for web applications, where the functionality is divided up across small web services.
- REST API is a documented method of interacting with services that implement REST architectural style.
- Service Metrics refers to the metrics such as cpu, memory and interface stats. In CSO, these metrics are collected via an agent.
- Traffic Metrics refers to the metrics such as traffic volume, rtt, jitter, packet loss etc. In CSO, these metrics are collected via device syslogs.

4.3. Alarm Life Cycle

Here are couple of examples of `alert_object` and `alert_status_object` (both are similar, main difference is that `alert_objects` are never modified after creation whereas `alert_status_object` will be modified every time a state change for that element occurs.

4.3.1. Device Goes Down

```
{
  "alert_type": "host",
  "site_name": "Site-01",
  "parent_uuid": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "tenant_name": "DemoTenant",
  "start_time": 1598349477,
  "object_type": "SRX_CLUSTER",
  "parent_type": "project",
  "site": "e68ff330-bc19-4190-ad9d-fcc74a93ee65",
  "pop": "68517ed4-dd5d-4605-bdc6-8b62ef5bf66a",
  "reason": "Host is Down",
  "display_name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "server": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "id": "d0094816-cb13-40d2-a603-d193e1645377",
  "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "uuid": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "category": "alarm",
  "name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "sub_system": "CSO",
  "region": "9e8d52c9-34c7-40dc-b26a-ba458db62fad",
  "uri": "/fmpm-provider/alert_object/ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "object_id": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "severity": "critical",
  "source": "device",
  "attributes": {
    "region_display_name": "regional",
    "pop_display_name": "regional",
    "opco_display_name": "default-domain"
  },
  "type": "alert_object",
  "parent_uri": "/fmpm-provider/project/3a35363e-0928-46d2-bd1c-d1d2a91cec8f"
}
```

Figure – alert_object for Device Down

```

{
  "alert_type": "host",
  "site_name": "Site-01",
  "parent_uuid": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "tenant_name": "DemoTenant",
  "start_time": 1598349490,
  "object_type": "SRX_CLUSTER",
  "parent_type": "project",
  "site": "e68ff330-bc19-4190-ad9d-fcc74a93ee65",
  "pop": "68517ed4-dd5d-4605-bdc6-8b62ef5bf66a",
  "reason": "Host is Down",
  "display_name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "server": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "id": "d0094816-cb13-40d2-a603-d193e1645377",
  "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "uuid": "a892ac92-22d5-4836-9f56-400997cfb215",
  "category": "alarm",
  "name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "sub_system": "CSO",
  "region": "9e8d52c9-34c7-40dc-b26a-ba458db62fad",
  "uri": "/fmpm-provider/alert_status_object/a892ac92-22d5-4836-9f56-400997cfb215",
  "object_id": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "severity": "critical",
  "source": "device",
  "attributes": {
    "region_display_name": "regional",
    "pop_display_name": "regional",
    "opco_display_name": "default-domain"
  },
  "type": "alert_status_object",
  "parent_uri": "/fmpm-provider/project/3a35363e-0928-46d2-bd1c-d1d2a91cec8f"
}

```

Figure – alert_status_object for Device Down

4.3.2. Device Restarts Successfully

```

{
  "alert_type": "host",
  "site_name": "Site-01",
  "parent_uuid": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "tenant_name": "DemoTenant",
  "start_time": 1598349990,
  "object_type": "SRX_CLUSTER",
  "parent_type": "project",
  "site": "e68ff330-bc19-4190-ad9d-fcc74a93ee65",
  "pop": "68517ed4-dd5d-4605-bdc6-8b62ef5bf66a",
  "reason": "Host is UP",
  "display_name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "server": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "id": "d0094816-cb13-40d2-a603-d193e1645377",
  "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "uuid": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "category": "alarm",
  "name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "sub_system": "CSO",
  "region": "9e8d52c9-34c7-40dc-b26a-ba458db62fad",
  "uri": "/fmpm-provider/alert_object/ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "object_id": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "severity": "normal",
  "source": "device",
  "attributes": {
    "region_display_name": "regional",
    "pop_display_name": "regional",
    "opco_display_name": "default-domain"
  },
  "type": "alert_object",
  "parent_uri": "/fmpm-provider/project/3a35363e-0928-46d2-bd1c-d1d2a91cec8f"
}

```

Figure – alert_object for Device Up

```
{
  "alert_type": "host",
  "site_name": "Site-01",
  "parent_uuid": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "tenant_name": "DemoTenant",
  "start_time": 1598349993,
  "object_type": "SRX_CLUSTER",
  "parent_type": "project",
  "site": "e68ff330-bc19-4190-ad9d-fcc74a93ee65",
  "pop": "68517ed4-dd5d-4605-bdc6-8b62ef5bf66a",
  "reason": "Host is UP",
  "display_name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "server": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "id": "d0094816-cb13-40d2-a603-d193e1645377",
  "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
  "uuid": "a892ac92-22d5-4836-9f56-400997cfb215",
  "category": "alarm",
  "name": "ef3a95f9-9c13-4d6a-b479-7c7689d222d1",
  "sub_system": "CSO",
  "region": "9e8d52c9-34c7-40dc-b26a-ba458db62fad",
  "uri": "/fmpm-provider/alert_status_object/a892ac92-22d5-4836-9f56-400997cfb215",
  "object_id": "d805adaf-e7c5-487b-9775-054c9f0b404b",
  "severity": "normal",
  "source": "device",
  "attributes": {
    "region_display_name": "regional",
    "pop_display_name": "regional",
    "opco_display_name": "default-domain"
  },
  "type": "alert_status_object",
  "parent_uri": "/fmpm-provider/project/3a35363e-0928-46d2-bd1c-d1d2a91cec8f"
}
```

Figure – alert_status_object for Device Down

Note that same alert_status_object is modified (same uri) when device comes back up.

4.4. Supported Alarms in CSO

CSO supports following alarm types –

4.4.1. Device Down/Unreachable

This alarm is generated when device is down or not reachable from CSO. Severity of this alarm is “critical”, it is “cleared” when connectivity between Device and CSO is restored.

4.4.2. Cluster Down

This alarm is applicable for Dual CPE. An alarm is raised with “major” severity if either “Primary” or “Secondary” node is down. If both nodes are down then same alarm is raised with “critical” severity. Alarm with “major” severity is cleared when both nodes are up. Alarm with “critical” may move to “clear” or “major” depending on whether one or both nodes are up.

4.4.3. DHCP Address Change Notification

This alarm is generated when IP address change is detected for a WAN link as a result of DHCP address assignment/re-assignment. Severity of this alarm is “major”, it is “cleared” when IP Address remains same across two consecutive checks.

4.4.4. WAN Interface Down

This alarm is generated when WAN link disconnection is detected. Severity of this alarm is “Major”, it is cleared when WAN connectivity is restored.

4.4.5. OAM IPSec Tunnel down

This alarm is generated when IPSec link between a site and OAM hub goes down. Severity of this alarm is “critical”, it is cleared when IPSec tunnel between site and OAM hub is re-established.

4.4.6. Overlay Tunnel Down

This alarm is generated when GRE/GRE_Over_IPSec data tunnel goes down, it can be between a spoke to hub, enterprise-hub or another spoke. Severity of this alarm is “critical”, it is cleared when the tunnels is re-established.

4.4.7. Underlay BGP Session Down

This alarm is generated when BGP association between a spoke and next hop router goes down. In case of dual homed connections, alarms for individual associations are raised. Severity of this alarm is “critical”, it is cleared when BGP association with the peer is restored.

4.4.8. Dual homed Underlay BGP Session Down

This alarm is generated when or both BGP associations between a spoke and next hop router are down. If one of the association is down then severity of the alarm is “minor”, for both associations down, severity is “critical”. Alarm with “critical” may move to “clear” or “minor” depending on whether one or both associations are up.

4.4.9. Site Monitoring Stopped

This alarm is generated when a site is recalled Or deleted. Severity of this alarm is “normal”, it is not required to “clear” this alarm.

4.4.10. VRR Down

This alarm is generated when a VRR is down or unreachable from CSO. Severity of this alarm is “critical”, it is cleared when connectivity between VRR and CSO is restored. This alarm is only visible to CSO administrator.

4.4.11. Combined Alarm for “alarms present in the device”

This alarm is generated when device shows any alarms (via cli/netconf), CSO raises an alarm with “major” severity if there are any alarms listed as a result of device cli/netconf command, it is cleared when no alarms are listed in the device.

4.4.12. Site-Edit Failure Alarm

This alarm is generated when any site-edit operation fails. Severity of this alarm is “major”, it is cleared

4.4.13. Site-Edit Alarm for “DHCP Update”

This alarm is generated when TSSM microservice starts a workflow after receiving “DHCP Address change” alarm. Severity of this alarm is “major”, it is cleared after workflow is completed.

4.4.14. DVPN tenant tunnel threshold exceeded Alarm

This alarm is generated when tenant threshold for number of DVPN tunnels is exceeded. Severity of this alarm is “major”, it is cleared when number of DVPN tunnels for a tenant falls below the threshold.

4.4.15. Provider-HUB Alarms

CSO generates Device Up/Down and WAN Link Up/Down alarms for Provider-HUBs. Payloads of these alarms are similar to corresponding spoke alarms but these alarms are visible only to the owner of the Provider-HUB (SRE or OpCo), these are not shared with tenants that connect spokes to this HUB.

Summary table for CSO alarms with JSON references

Alarm Types	Severity	Reference
Device Down	Critical	Device Down/Unreachable
Cluster Down (one or both nodes)	Critical/Major	Cluster Down
DHCP Address Change Notification	Major	DHCP Address Change Notification
WAN Interface Down	Major	WAN Interface Down
OAM IPsec Tunnel Down	Critical	OAM IPsec Tunnel down
Overlay Tunnel Down (GRE, GRE_Over_IPsec etc.)	Critical	Overlay Tunnel Down (GRE)
Underlay BGP Session Down	Critical	Underlay BGP Session Down
Dual Homed Underlay BGP Session Down	Critical/Minor	Dual homed Underlay BGP Session Down
Site Monitoring Stopped	Normal	Site Monitoring Stopped
VRR Down	Critical	VRR Down
Combined Alarm for “alarms present in the device”	Major	Combined Alarm for “alarms present in the device”
Site-Edit Failure Alarm	Major	Site-Edit Failure Alarm

Alarm Types	Severity	Reference
Site-Edit Alarm for “DHCP Update”	Major	Site-Edit Alarm for “DHCP Update”
DVPN tenant tunnel threshold exceeded Alarm	Major	DVPN tenant tunnel threshold exceeded Alarm

4.5. Main attributes of alarms payload

Field	Description	Example Value
device	Device <uuid>. In case of host up/down alarms, it is same as object_id field.	<b9a0de2b-1472-4516-89ee-7faec9249972>
severity	“normal” represents alarm is cleared, other values indicate alarm severity – major, critical, info, event.	“critical”
start_time	Epoch timestamp when alarm was raised/cleared.	1598362317
sub_system	Set to CSO for SDWAN/SDLAN alarms and to SD for alarms raised by Security Director.	“CSO”

Field	Description	Example Value
object_type	Set to device type where alarm is raised – UCPE_DEVICE, CPE_DEVICE, HUB, NFX_CLUSTER_NODE, NFX_CLUSTER, SRX_CLUSTER & VRR.	“SRX_CLUSTER”
object_id	Identifies the element, it could be set to the device <uuid> or element.	* device < b9a0de2b-1472-4516-89ee-7faec9249972> * interface < /SRX/interface/WAN_1 > ...
reason	Set to brief description about the alarms.	* "GRE_OVER_IPSEC DOWN" * "BGP Session state to VRR vrr-10.219.98.28 is Established"
source	Set to identify which functional component raised the alarm. Possible values are - SECURITY, DEVICE, ROUTING, & TENANT	* Device Critical - Device Down Major - DHCP Address Change Notification * Underlay Major - Physical Interface Down * Overlay Critical - GRE/IPSec Tunnels Down * Routing Critical - Underlay BGP Session Down Critical - VRR Down (*these alarms are only visible to SP-Admin)

Field	Description	Example Value
tenant	<uuid> of the tenant.	3a35363e-0928-46d2-bd1c-d1d2a91cec8f
tenant_name	<name> of the tenant.	"tenant_1"
site	<uuid> of the site.	9cfa61fb-87bf-45cf-ab03-af0f42f3d448
site_name	<name> of the site	"site_1"
uri	<uri> to fetch this particular HAPI object	* /fmpm-provider/alert_object/41c95609-c919-4ea6-a88f-1ebd81c07a20 * /fmpm-provider/alert_status_object/2c620575-bad8-4181-8cd1-98db9fd41780
attributes	Additional information about the alarm, varies for different types of alarms.	<pre>{ "region_display_name": "regional", "src": { "site_name": "SiteB-01", "role": "gateway", "wan_name": "WAN_1", "overlay_interface": "gr-0/0/0.4019", "underlay_interface": "ge-0/0/1" }, "opco_display_name": "default-domain", "underlay_link_name": "WAN_1", "dst": { "site_name": "Site-01", "role": "gateway", "wan_name": "WAN_1", "overlay_interface": null, "underlay_interface": "reth1" } }</pre>

4.6. Few Examples for fetching alarm objects

4.6.1. Get all active alarms for a tenant

GET `https://{central_ip}/fmpm-provider/alert_status_object?detail=true&filter=(severity!=normal)`

```

{
  "total": 1,
  "alert_status_object": [
    {
      "last_update_time": 1598372083,
      "alert_type": "host",
      "site_name": "Site-01",
      "parent_uuid": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
      "tenant_name": "DemoTenant",
      "object_type": "SRX_CLUSTER",
      "parent_type": "project",
      "site": "e68ff330-bc19-4190-ad9d-fcc74a93ee65",
      "pop": "68517ed4-dd5d-4605-bdc6-8b62ef5bf66a",
      "id": "d805adaf-e7c5-487b-9775-054c9f0b404b",
      "category": "alarm",
      "fq_name": [
        "default-domain",
        "DemoTenant",
        "d805adaf-e7c5-487b-9775-054c9f0b404b"
      ],
      "uuid": "64e7987c-e377-4ea1-bb0d-d4a2da13e53e",
      "sub_system": "CSO",
      "object_id": "d805adaf-e7c5-487b-9775-054c9f0b404b",
      "source": "device",
      "id_perms": {
        "enable": true,
        "uuid": {
          "uuid_mslong": 7270947785572568737,
          "uuid_lslong": 13478663055698289982
        },
        "created": "2020-08-25T09:21:53.694893",
        "description": null,
        "creator": "admin",
        "user_visible": true,
        "last_modified": "2020-08-25T16:14:43.704588",
        "modifier": "admin",
        "permissions": {
          "owner": "admin",
          "owner_access": 7,
          "other_access": 7,
          "group": "admin",
          "group_access": 7
        }
      },
      "type": "alert_status_object",
      "parent_uri": "/fmpm-provider/project/3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
      "region_name": null,
      "start_time": 1598347313,
      "reason": "Host is UP",
      "perms2": {

```

```

    "owner": "3a35363e092846d2bd1cd1d2a91cec8f",
    "owner_access": 7,
    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "f07884c8f7994eb49af0828031d7e247"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ],
    "device": "d805adaf-e7c5-487b-9775-054c9f0b404b",
    "display_name": "d805adaf-e7c5-487b-9775-054c9f0b404b",
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "severity": "normal",
    "name": "d805adaf-e7c5-487b-9775-054c9f0b404b",
    "region": "9e8d52c9-34c7-40dc-b26a-ba458db62fad",
    "counter": 4,
    "uri": "/fmpm-provider/alert_status_object/64e7987c-e377-4ea1-bb0d-d4a2da13e53e",
    "server": "d805adaf-e7c5-487b-9775-054c9f0b404b",
    "pop_name": null,
    "attributes": {
      "region_display_name": "regional",
      "pop_display_name": "regional",
      "opco_display_name": "default-domain"
    },
    "opco_name": null
  }
]
}

```

4.6.2. Get all active alarms for a site

GET

/fmpm-provider/alert_status_object?detail=true&filter=(site=e68ff330-bc19-4190-ad9d-fcc74a93ee65
and severity!=normal)

Response format is same as above.

4.6.3. Get history of alarms for a tenant

```
GET /fmpm-provider/alert_object?detail=true
```

Response format is same as above.

4.6.4. Get history of alarms for a site

```
GET
```

```
/fmpm-provider/alert_object?detail=true&filter=(site=e68ff330-bc19-4190-ad9d-fcc74a93ee65)
```

Response format is same as above.

4.6.5. Filters Based on Alarm Attributes

Based on other fields, e.g. alert_type, source etc. RPC below will fetch history of all device down alarms for a given site.

```
GET
```

```
/fmpm-provider/alert_object?from=0&size=200&detail=true&filter=(site=e68ff330-bc19-4190-ad9d-fcc74a93ee65  
and alert_type=host)
```

Response format is same as above.

4.6.6. API Result Pagination

```
GET /fmpm-provider/alert_object?detail=True&from=0&size=20
```

Response format is same as above.

Similarly, next 20 objects can be fetched as

```
GET
```

```
https://{{central_ip}}/fmpm-provider/alert_object?detail=True&from=20&size=20
```

Response format is same as above.

Note – “from” is zero based index.

4.7. Alarm Payloads (JSON)

4.7.1. Device Down/Unreachable

```

{
  "alert_status_object": {
    "last_update_time": 1598539848,
    "alert_type": "host",
    "site_name": "enthub2",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "CPE_DEVICE",
    "parent_type": "project",
    "site": "ae6e48d9-3cc3-467d-ab58-22fca1562aa8",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "id": "16e98901-adf2-443b-9f47-dd9d3cabed4b",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "16e98901-adf2-443b-9f47-dd9d3cabed4b"
    ],
    "uuid": "b3229593-a9a4-477b-a181-78064d8ab53c",
    "sub_system": "CSO",
    "object_id": "16e98901-adf2-443b-9f47-dd9d3cabed4b",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 12908043943436109691,
        "uuid_lslong": 11637714880568145212
      },
      "created": "2020-08-13T10:48:31.113346",
      "description": null,
      "creator": "admin",
      "user_visible": true,
      "last_modified": "2020-08-27T14:50:48.957985",
      "modifier": "admin",
      "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
    "region_name": null,
    "start_time": 1597315710,
    "reason": "Device is down",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",
      "owner_access": 7,
      "global_access": 0,

```

```

    "share": [
      {
        "tenant_access": 7,
        "tenant": "45f1033764954b899cee9f6ea25a667f"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ],
    "device": "16e98901-adf2-443b-9f47-dd9d3cabed4b",
    "display_name": "16e98901-adf2-443b-9f47-dd9d3cabed4b",
    "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "severity": "critical",
    "name": "16e98901-adf2-443b-9f47-dd9d3cabed4b",
    "region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
    "counter": 4,
    "uri": "/fmpm-provider/alert_status_object/b3229593-a9a4-477b-a181-78064d8ab53c",
    "server": "16e98901-adf2-443b-9f47-dd9d3cabed4b",
    "pop_name": null,
    "attributes": {
      "region_display_name": "regional",
      "pop_display_name": "regional",
      "opco_display_name": "default-domain"
    },
    "opco_name": null
  }
}

```

4.7.2. Cluster Down

```

{
  "alert_status_object": {
    "last_update_time": 1602854135,
    "alert_type": "service",
    "site_name": "SRXDUAL",
    "parent_uuid": "ab6df30b-970f-4e1a-9c28-a557ea056512",
    "tenant_name": "DemoTenant",
    "object_type": "SRX_CLUSTER",
    "parent_type": "project",
    "site": "66856085-f42c-4eb8-9c12-5496992e7447",
    "pop": "61a4c7dd-51b0-444f-a0c6-366c8442eeb6",
    "opco": "c9e32dacb40e4f9e9416b615e2913c89",
    "id": "5a963031-c17f-4fc0-a7a4-1c252265fc32##/SRX/cluster/status",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "DemoTenant",
      "5a963031-c17f-4fc0-a7a4-1c252265fc32##/SRX/cluster/status"
    ],
    "uuid": "431473f2-97e1-4cb9-9645-de8b2fe7bbd0",
    "sub_system": "CSO",
    "object_id": "/SRX/cluster/status",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 4833615785842789561,
        "uuid_lslong": 10828305568467762128
      },
      "created": "2020-10-16T13:15:35.515887",
      "description": null,
      "creator": "admin",
      "user_visible": true,
      "last_modified": "2020-10-16T13:15:35.515887",
      "modifier": "admin",
      "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/ab6df30b-970f-4e1a-9c28-a557ea056512",
    "start_time": 1602854135,
    "reason": "MEMBER ROLE - CLUSTER UNSTABLE",
    "perms2": {
      "owner": "ab6df30b970f4e1a9c28a557ea056512",
      "owner_access": 7,
      "global_access": 0,

```

```

    "share": [
      {
        "tenant_access": 7,
        "tenant": "c9e32dacb40e4f9e9416b615e2913c89"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ],
    "device": "5a963031-c17f-4fc0-a7a4-1c252265fc32",
    "display_name": "/SRX/cluster/status",
    "tenant": "ab6df30b-970f-4e1a-9c28-a557ea056512",
    "severity": "major",
    "name": "5a963031-c17f-4fc0-a7a4-1c252265fc32##/SRX/cluster/status",
    "region": "b2af2887-a3c0-44f8-b569-57e9d8f20d19",
    "counter": 1,
    "uri": "/fmpm-provider/alert_status_object/431473f2-97e1-4cb9-9645-de8b2fe7bbd0",
    "server": "5a963031-c17f-4fc0-a7a4-1c252265fc32",
    "attributes": {
      "region_display_name": "regional",
      "pop_display_name": "regional",
      "opco_display_name": "default-domain"
    }
  }
}

```

4.7.3. DHCP Address Change Notification

```

{
  "alert_status_object": {
    "last_update_time": 1597919188,
    "alert_type": "host",
    "site_name": "nfx-site",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "start_time": 1597652305.530225,
    "parent_type": "project",
    "site": "17312cf8-617b-4780-b97f-678746881d18",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "reason": "interface address changed",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",
      "owner_access": 7,
      "global_access": 0,
      "share": [
        {
          "tenant_access": 7,
          "tenant": "45f1033764954b899cee9f6ea25a667f"
        },
        {
          "tenant_access": 4,
          "tenant": "share.child_projects"
        }
      ]
    },
    "device": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "display_name": "/SRX/interface/WAN_3.DATA/dhcp_status",
    "server": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "id": "/SRX/interface/WAN_3.DATA/dhcp_status",
    "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "name": "/SRX/interface/WAN_3.DATA/dhcp_status",
    "fq_name": [
      "default-domain",
      "tenant",
      "/SRX/interface/WAN_3.DATA/dhcp_status"
    ],
    "uuid": "05c10e99-2fb7-44ed-b906-1855bfe4addb",
    "sub_system": "CSO",
    "region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
    "counter": 3,
    "uri": "/fmpm-provider/alert_status_object/05c10e99-2fb7-44ed-b906-1855bfe4addb",
    "object_id": "/SRX/interface/WAN_3.DATA/dhcp_status",
    "severity": "critical",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 414628691788121325,

```

```
    "uuid_lslong": 13332370503447653851
  },
  "created": "2020-08-17T08:18:25.679507",
  "description": null,
  "creator": "admin",
  "user_visible": true,
  "last_modified": "2020-08-20T10:26:29.072935",
  "modifier": "admin",
  "permissions": {
    "owner": "admin",
    "owner_access": 7,
    "other_access": 7,
    "group": "admin",
    "group_access": 7
  }
},
"parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9"
}
```

4.7.4. WAN Interface Down

```

{
  "alert_status_object": {
    "last_update_time": 1598259119,
    "alert_type": "service",
    "site_name": "nfx-site",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "UCPE_DEVICE",
    "parent_type": "project",
    "site": "17312cf8-617b-4780-b97f-678746881d18",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "id": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/SRX/interface/WAN_3.PPPOE",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/SRX/interface/WAN_3.PPPOE"
    ],
    "uuid": "7b7fc709-e30a-4688-865a-3d57e1956ce6",
    "sub_system": "CSO",
    "object_id": "/SRX/interface/WAN_3.PPPOE",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 8899050233985123976,
        "uuid_lslong": 9681117796642417894
      },
      "created": "2020-08-17T07:20:02.679454",
      "description": null,
      "creator": "admin",
      "user_visible": true,
      "last_modified": "2020-08-24T08:51:59.298907",
      "modifier": "admin",
      "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
    "start_time": 1597648796,
    "reason": "Monitor object deleted",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",
      "owner_access": 7,
      "global_access": 0,
      "share": [

```

```

    {
      "tenant_access": 7,
      "tenant": "45f1033764954b899cee9f6ea25a667f"
    },
    {
      "tenant_access": 4,
      "tenant": "share.child_projects"
    }
  ]
},
"device": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
"display_name": "/SRX/interface/WAN_3.PPPOE",
"tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
"severity": "normal",
"name": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/SRX/interface/WAN_3.PPPOE",
"region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
"counter": 1,
"uri": "/fmpm-provider/alert_status_object/7b7fc709-e30a-4688-865a-3d57e1956ce6",
"server": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
"attributes": {
  "region_display_name": "regional",
  "local_breakout": "shared",
  "map_e_support": false,
  "alert_name": "/SRX/interface/WAN_3.PPPOE",
  "pop_display_name": "regional",
  "service_value": "WAN_3",
  "opco_display_name": "default-domain",
  "service_category": "underlay",
  "interface_name": "pp0.0",
  "component_name": "JUNOS"
}
}
}

```

4.7.5. OAM IPSec Tunnel down

```

{
  "alert_status_object": {
    "last_update_time": 1597730938,
    "alert_type": "service",
    "site_name": "enthub-1",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "CPE_DEVICE",
    "parent_type": "project",
    "site": "824b4c08-a745-4521-ae2b-60279db0e8e6",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "id": "6861d066-623b-4a85-8558-
19341bfd3699##/SRX/ipsec/vpn/344de8aebbd7802747013406e6c6369",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "6861d066-623b-4a85-8558-
19341bfd3699##/SRX/ipsec/vpn/344de8aebbd7802747013406e6c6369"
    ],
    "uuid": "d6466b92-ca5d-44de-b6a4-25e52a24c40e",
    "sub_system": "CSO",
    "object_id": "/SRX/ipsec/vpn/344de8aebbd7802747013406e6c6369",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 15440146650690831582,
        "uuid_lslong": 13160685677268222990
      },
      "created": "2020-08-13T12:39:12.861251",
      "description": null,
      "creator": "admin",
      "user_visible": true,
      "last_modified": "2020-08-18T06:08:59.308402",
      "modifier": "admin",
      "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
    "region_name": null,
    "start_time": 1597322352,
    "reason": "IPSEC DOWN : Local: E14:WAN_0, Remote: H0:WAN_1",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",

```

```

    "owner_access": 7,
    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "45f1033764954b899cee9f6ea25a667f"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ]
  },
  "device": "6861d066-623b-4a85-8558-19341bfd3699",
  "display_name": "/SRX/ipsec/vpn/344de8aebbd7802747013406e6c6369",
  "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
  "severity": "critical",
  "name": "6861d066-623b-4a85-8558-19341bfd3699##/SRX/ipsec/vpn/344de8aebbd7802747013406e6c6369",
  "region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
  "counter": 4,
  "uri": "/fmpm-provider/alert_status_object/d6466b92-ca5d-44de-b6a4-25e52a24c40e",
  "server": "6861d066-623b-4a85-8558-19341bfd3699",
  "pop_name": null,
  "attributes": {
    "region_display_name": "regional",
    "src": {
      "site_name": "E14",
      "role": "spoke",
      "wan_name": "WAN_0",
      "overlay_interface": "st0.4000",
      "underlay_interface": "ge-0/0/1"
    },
    "opco_display_name": "default-domain",
    "underlay_link_name": "WAN_0",
    "dst": {
      "site_name": "H0",
      "role": "hub",
      "wan_name": "WAN_1",
      "overlay_interface": "st0.4005",
      "underlay_interface": "ge-0/0/2"
    }
  },
  "link_encapsulation": "IPSEC",
  "alert_name": "/SRX/ipsec/vpn/344de8aebbd7802747013406e6c6369",
  "pop_display_name": "regional",
  "service_value": "344de8aebbd7802747013406e6c6369",
  "service_category": "overlay",
  "device_id": "6861d066-623b-4a85-8558-19341bfd3699",
  "peer_id": "d6297ef0-3ab9-4a2e-8158-526453ef43f1",
  "overlay_link_name": "OAM-E14_WAN_0_H0_WAN_1_IPSEC_1",

```

```
        "interface_name": "st0.4000",  
        "component_name": "SRX"  
    },  
    "opco_name": null  
}
```

4.7.6. Overlay Tunnel Down (GRE)

```

{
  "alert_status_object": {
    "last_update_time": 1598259132,
    "alert_type": "service",
    "site_name": "nfx-site",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "UCPE_DEVICE",
    "parent_type": "project",
    "site": "17312cf8-617b-4780-b97f-678746881d18",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "id": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/SRX/gre/vpn/86eedc8d1178f3c5a609dacb9b59ecd7",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/SRX/gre/vpn/86eedc8d1178f3c5a609dacb9b59ecd7"
    ],
    "uuid": "b02923dd-34d2-42b4-995b-21b5dad3d04a",
    "sub_system": "CSO",
    "object_id": "/SRX/gre/vpn/86eedc8d1178f3c5a609dacb9b59ecd7",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 12693716457701393076,
        "uuid_lslong": 11050463175627755594
      }
    },
    "created": "2020-08-18T06:45:24.266997",
    "description": null,
    "creator": "admin",
    "user_visible": true,
    "last_modified": "2020-08-24T08:52:12.838616",
    "modifier": "admin",
    "permissions": {
      "owner": "admin",
      "owner_access": 7,
      "other_access": 7,
      "group": "admin",
      "group_access": 7
    }
  },
  "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
  "start_time": 1597733123,
  "reason": "Interface Down",
  "perms2": {
    "owner": "1462d2272131478e8f78a4995f73b8e9",
    "owner_access": 7,
  }
}

```

```

    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "45f1033764954b899cee9f6ea25a667f"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ]
  },
  "device": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
  "display_name": "/SRX/gre/vpn/86eedc8d1178f3c5a609dacb9b59ecd7",
  "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
  "severity": "critical",
  "name": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/SRX/gre/vpn/86eedc8d1178f3c5a609dacb9b59ecd7",
  "region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
  "counter": 9,
  "uri": "/fmpm-provider/alert_status_object/b02923dd-34d2-42b4-995b-21b5dad3d04a",
  "server": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
  "attributes": {
    "region_display_name": "regional",
    "src": {
      "site_name": "S7",
      "role": "spoke",
      "wan_name": "WAN_0",
      "overlay_interface": "gr-1/0/0.4026",
      "underlay_interface": "ge-1/0/1"
    },
    "opco_display_name": "default-domain",
    "underlay_link_name": "WAN_0",
    "dst": {
      "site_name": "H1",
      "role": "hub",
      "wan_name": "WAN_2",
      "overlay_interface": null,
      "underlay_interface": "ge-0/0/3"
    },
    "link_encapsulation": "GRE",
    "alert_name": "/SRX/gre/vpn/86eedc8d1178f3c5a609dacb9b59ecd7",
    "pop_display_name": "regional",
    "service_value": "86eedc8d1178f3c5a609dacb9b59ecd7",
    "service_category": "overlay",
    "peer_id": "7109fb14-fd1f-44a9-b0f5-ebcd289d8bf8",
    "overlay_link_name": "S7_WAN_0_H1_WAN_2_GRE_0",
    "interface_name": "gr-1/0/0.4026",
    "component_name": "SRX"
  }
}

```

```
}  
}
```

4.7.7. Overlay Tunnel Down (GRE_Over_IPSec)

```

{
  "alert_status_object": {
    "last_update_time": 1597669115,
    "alert_type": "service",
    "site_name": "enthub-1",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "CPE_DEVICE",
    "parent_type": "project",
    "site": "824b4c08-a745-4521-ae2b-60279db0e8e6",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "id": "6861d066-623b-4a85-8558-19341bfd3699##/SRX/gre-
ipsec/vpn/81755f0595d2bf5a8e11c09208bdcf87",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "6861d066-623b-4a85-8558-19341bfd3699##/SRX/gre-
ipsec/vpn/81755f0595d2bf5a8e11c09208bdcf87"
    ],
    "uuid": "28eca8b8-0d1e-4412-af3c-1856d4c642e4",
    "sub_system": "CSO",
    "object_id": "/SRX/gre-ipsec/vpn/81755f0595d2bf5a8e11c09208bdcf87",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 2948917364468368402,
        "uuid_lslong": 12626994216456045284
      },
    },
    "created": "2020-08-17T10:19:05.687569",
    "description": null,
    "creator": "admin",
    "user_visible": true,
    "last_modified": "2020-08-17T12:58:35.291587",
    "modifier": "admin",
    "permissions": {
      "owner": "admin",
      "owner_access": 7,
      "other_access": 7,
      "group": "admin",
      "group_access": 7
    }
  },
  "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
  "region_name": null,
  "start_time": 1597659545,
  "reason": "Interface Down",
  "perms2": {
    "owner": "1462d2272131478e8f78a4995f73b8e9",
  }
}

```

```

    "owner_access": 7,
    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "45f1033764954b899cee9f6ea25a667f"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ]
  },
  "device": "6861d066-623b-4a85-8558-19341bfd3699",
  "display_name": "/SRX/gre-ipsec/vpn/81755f0595d2bf5a8e11c09208bdcf87",
  "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
  "severity": "critical",
  "name": "6861d066-623b-4a85-8558-19341bfd3699##/SRX/gre-
ipsec/vpn/81755f0595d2bf5a8e11c09208bdcf87",
  "region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
  "counter": 2,
  "uri": "/fmpm-provider/alert_status_object/28eca8b8-0d1e-4412-af3c-1856d4c642e4",
  "server": "6861d066-623b-4a85-8558-19341bfd3699",
  "pop_name": null,
  "attributes": {
    "region_display_name": "regional",
    "src": {
      "site_name": "E14",
      "role": "gateway",
      "wan_name": "WAN_0",
      "overlay_interface": "gr-0/0/0.4020",
      "underlay_interface": "ge-0/0/1"
    },
    "opco_display_name": "default-domain",
    "underlay_link_name": "WAN_0",
    "dst": {
      "site_name": "S7",
      "role": "spoke",
      "wan_name": "WAN_2",
      "overlay_interface": null,
      "underlay_interface": "ge-1/0/3"
    }
  },
  "link_encapsulation": "GRE_OVER_IPSEC",
  "alert_name": "/SRX/gre-ipsec/vpn/81755f0595d2bf5a8e11c09208bdcf87",
  "pop_display_name": "regional",
  "service_value": "81755f0595d2bf5a8e11c09208bdcf87",
  "service_category": "overlay",
  "peer_id": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
  "overlay_link_name": "E14_WAN_0_S7_WAN_2_GRE_IPSEC_0",
  "interface_name": "gr-0/0/0.4020",

```

```
        "component_name": "SRX"  
      },  
      "opco_name": null  
    }  
  }
```

4.7.8. Underlay BGP Session Down

```

{
  "alert_status_object": {
    "last_update_time": 1598281508,
    "alert_type": "service",
    "site_name": "nfx-site",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "UCPE_DEVICE",
    "parent_type": "project",
    "site": "2735c7ab-31a4-4f49-82f0-a58558711dee",
    "pop": "0be374b0-df72-4d2b-8f83-dbd3ac426c2a",
    "id": "e793f2e9-a357-4920-af2d-2b56868a2b4b##/juniper-nfx3/BGP/vrr-10.213.5.102",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "e793f2e9-a357-4920-af2d-2b56868a2b4b##/juniper-nfx3/BGP/vrr-10.213.5.102"
    ],
    "uuid": "e4a8cfca-ad5d-4fe4-bcca-0a30c7fecf44",
    "sub_system": "CSO",
    "object_id": "/juniper-nfx3/BGP/vrr-10.213.5.102",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 16476647706133876708,
        "uuid_lslong": 13603696829056077636
      },
      "created": "2020-08-24T15:00:21.140323",
      "description": null,
      "creator": "admin",
      "user_visible": true,
      "last_modified": "2020-08-24T15:05:08.971535",
      "modifier": "admin",
      "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
    "start_time": 1598281218,
    "reason": "Monitor object deleted",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",
      "owner_access": 7,
      "global_access": 0,
      "share": [

```

```

    {
      "tenant_access": 7,
      "tenant": "45f1033764954b899cee9f6ea25a667f"
    },
    {
      "tenant_access": 4,
      "tenant": "share.child_projects"
    }
  ]
},
"device": "e793f2e9-a357-4920-af2d-2b56868a2b4b",
"display_name": "/juniper-nfx3/BGP/vrr-10.213.5.102",
"tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
"severity": "critical",
"name": "e793f2e9-a357-4920-af2d-2b56868a2b4b##/juniper-nfx3/BGP/vrr-10.213.5.102",
"region": "328ca06a-02da-4fa2-b19f-e37e6bd248b0",
"counter": 1,
"uri": "/fmpm-provider/alert_status_object/e4a8cfca-ad5d-4fe4-bcca-0a30c7fecf44",
"server": "e793f2e9-a357-4920-af2d-2b56868a2b4b",
"attributes": {
  "region_display_name": "regional",
  "neighbour_ip": "10.213.5.102",
  "service_name": "vrr",
  "pop_display_name": "regional",
  "opco_display_name": "default-domain",
  "component_name": "JUNOS"
}
}
}

```

4.7.9. Dual Homed Underlay BGP Session Down

```

{
  "last_update_time": 1599056212,
  "alert_type": "service",
  "site_name": "GW-Site-2",
  "parent_uuid": "939144e4-325f-41c5-9330-87ff84b88d89",
  "tenant_name": "mssb_tenant",
  "object_type": "CPE_DEVICE",
  "parent_type": "project",
  "site": "5e9cb5f2-ad5a-4110-a5cf-259ba319882c",
  "pop": "1be5b5a9-5846-429e-ae46-9a151c792b26",
  "id": "ed9f457a-ecb8-4d60-b5f6-f43057c17252##/juniper-
srx/BGP/composite/WAN_0",
  "category": "alarm",
  "fq_name": [
    "default-domain",
    "mssb_tenant",
    "ed9f457a-ecb8-4d60-b5f6-f43057c17252##/juniper-srx/BGP/composite/WAN_0"
  ],
  "uuid": "69eead34-84bc-48eb-b38c-c5f89fca689d",
  "sub_system": "CSO",
  "object_id": "/juniper-srx/BGP/composite/WAN_0",
  "source": "device",
  "id_perms": {
    "enable": true,
    "uuid": {
      "uuid_mslong": 7633228859516405995,
      "uuid_lslong": 12937933501151996061
    },
    "created": "2020-09-02T14:14:57.119525",
    "description": null,
    "creator": "admin",
    "user_visible": true,
    "last_modified": "2020-09-02T14:17:00.549530",
    "modifier": "admin",
    "permissions": {
      "owner": "admin",
      "owner_access": 7,
      "other_access": 7,
      "group": "admin",
      "group_access": 7
    }
  },
  "type": "alert_status_object",
  "parent_uri": "/fmpm-provider/project/939144e4-325f-41c5-9330-87ff84b88d89",
  "region_name": null,
  "start_time": 1599056092,
  "reason": "BGP Peers info on WAN_0 `Neighbor : 40.2.20.254, State: DOWN`
`Neighbor : 40.2.20.253, State: DOWN`",
  "perms2": {
    "owner": "939144e4325f41c5933087ff84b88d89",

```

```

    "owner_access": 7,
    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "fdb64c37d7924a49a8200d586f4edab6"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ],
    "device": "ed9f457a-ecb8-4d60-b5f6-f43057c17252",
    "display_name": "/juniper-srx/BGP/composite/WAN_0",
    "tenant": "939144e4-325f-41c5-9330-87ff84b88d89",
    "severity": "critical",
    "name": "ed9f457a-ecb8-4d60-b5f6-f43057c17252##/juniper-
srx/BGP/composite/WAN_0",
    "region": "8d582d73-5791-4461-9f18-d7aff4d203d8",
    "counter": 2,
    "uri": "/fmpm-provider/alert_status_object/69eead34-84bc-48eb-b38c-
c5f89fca689d",
    "server": "ed9f457a-ecb8-4d60-b5f6-f43057c17252",
    "pop_name": null,
    "attributes": {
      "region_display_name": "regional",
      "pop_display_name": "regional",
      "opco_display_name": "default-domain",
      "role": "composite_alarm",
      "component_name": "JUNOS"
    },
    "opco_name": null
  }
}

```

4.7.10. Monitored Object Deleted

```

{
  "alert_status_object": {
    "last_update_time": 1603130398,
    "alert_type": "host",
    "site_name": "CaptainAmerica",
    "parent_uuid": "d3adabb6-00d4-4e5c-81f1-3f752c4a9b76",
    "tenant_name": "DemoTenant",
    "object_type": "CPE_DEVICE",
    "parent_type": "project",
    "site": "c991ff63-13cf-4796-a073-bd3e6899b632",
    "pop": "f1f0cc96-6c20-40f0-b5e4-be4fc6b763c9",
    "opco": "adb27982758643f891d0a2c9e5c626bf",
    "id": "0fef2031-7c54-4dde-9397-6feb15d56c0b",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "DemoTenant",
      "0fef2031-7c54-4dde-9397-6feb15d56c0b"
    ],
    "uuid": "8b6c2286-ebd2-41cb-9b52-26185919db5e",
    "sub_system": "CSO",
    "object_id": "0fef2031-7c54-4dde-9397-6feb15d56c0b",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 10046442831634121163,
        "uuid_lslong": 11192049909985041246
      },
      "created": "2020-10-19T17:49:51.356827",
      "description": null,
      "creator": "admin",
      "user_visible": true,
      "last_modified": "2020-10-19T17:59:58.169060",
      "modifier": "admin",
      "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/d3adabb6-00d4-4e5c-81f1-3f752c4a9b76",
    "start_time": 1603129789,
    "reason": "Monitor object deleted",
    "perms2": {
      "owner": "d3adabb600d44e5c81f13f752c4a9b76",
      "owner_access": 7,

```

```

    "global_access": 0,
    "share": [{
        "tenant_access": 7,
        "tenant": "adb27982758643f891d0a2c9e5c626bf"
    },
    {
        "tenant_access": 4,
        "tenant": "share.child_projects"
    }
    ],
    "device": "0fef2031-7c54-4dde-9397-6feb15d56c0b",
    "display_name": "0fef2031-7c54-4dde-9397-6feb15d56c0b",
    "tenant": "d3adabb6-00d4-4e5c-81f1-3f752c4a9b76",
    "severity": "normal",
    "name": "0fef2031-7c54-4dde-9397-6feb15d56c0b",
    "region": "8e230830-d5bc-4df2-8c17-23a20c6e5c41",
    "counter": 1,
    "uri": "/fmpm-provider/alert_status_object/8b6c2286-ebd2-41cb-9b52-26185919db5e",
    "server": "0fef2031-7c54-4dde-9397-6feb15d56c0b",
    "attributes": {
        "region_display_name": "regional",
        "pop_display_name": "regional",
        "opco_display_name": "default-domain"
    }
}

```

4.7.11. VRR Down

```

{
  "last_update_time": 1548171584,
  "alert_type": "host",
  "parent_uuid": "d2bbfbdf-11b4-48f0-84be-405730df9685",
  "severity": "critical",
  "start_time": 1548171584,
  "object_type": "VRR",
  "parent_type": "project",
  "site": "NA",
  "reason": "CRITICAL - Host Unreachable (10.213.21.138)",
  "perms2": {
    "owner": "d2bbfbdf11b448f084be405730df9685",
    "owner_access": 7,
    "global_access": 0,
    "share": [{
      "tenant_access": 4,
      "tenant": "share.child_projects"
    }]
  },
  "device": "10.213.21.138",
  "display_name": "10.213.21.138",
  "id": "10.213.21.138",
  "tenant": "d2bbfbdf-11b4-48f0-84be-405730df9685",
  "uuid": "6ef9c27b-42c5-40e9-a8db-42aa28d54918",
  "category": "alarm",
  "fq_name": ["default-domain", "default-project", "10.213.21.138"],
  "name": "10.213.21.138",
  "sub_system": "CSO",
  "counter": 1,
  "uri": "/fmpm-provider/alert_status_object/6ef9c27b-42c5-40e9-a8db-42aa28d54918",
  "object_id": "10.213.21.138",
  "source": "device",
  "id_perms": {
    "enable": true,
    "uuid": {
      "uuid_mslong": 7996636448030015721,
      "uuid_lslong": 12167392116868466968
    },
    "created": "2019-01-22T15:39:44.880616",
    "description": null,
    "creator": "admin",
    "user_visible": true,
    "last_modified": "2019-01-22T15:39:44.880616",
    "modifier": "admin",
    "permissions": {
      "owner": "admin",
      "owner_access": 7,
      "other_access": 7,
      "group": "admin",
      "group_access": 7
    }
  }
}

```

```
    }  
  },  
  "attributes": {  
    "opco_display_name": "default-domain"  
  },  
  "type": "alert_status_object",  
  "parent_uri": "/fmpm-provider/project/d2bbfbdf-11b4-48f0-84be-405730df9685"  
}
```

4.7.12. Combined Alarm For “alarms present in the device”

```

{
  "alert_status_object": {
    "last_update_time": "1595488924",
    "alert_type": "service",
    "site_name": "SiteB-01",
    "parent_uuid": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "severity": "minor",
    "start_time": "1595488924",
    "object_type": "CPE_DEVICE",
    "parent_type": "project",
    "site": "42d58b31-3b0e-4b08-837d-7df5bd25252e",
    "reason": "Rescue configuration is not set",
    "perms2": {
      "owner": "3a35363e092846d2bd1cd1d2a91cec8f",
      "owner_access": 7,
      "global_access": 0,
      "share": [
        {
          "tenant_access": 7,
          "tenant": "f07884c8f7994eb49af0828031d7e247"
        },
        {
          "tenant_access": 4,
          "tenant": "share.child_projects"
        }
      ]
    },
    "device": "1bdc3b73-804b-4e43-b49f-3b624bf57d54",
    "display_name": "3fd84e7e-a6bf-48f2-a855-8e82173445dd",
    "id": "1bdc3b73-804b-4e43-b49f-3b624bf57d54##3fd84e7e-a6bf-48f2-a855-8e82173445dd",
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "name": "1bdc3b73-804b-4e43-b49f-3b624bf57d54##3fd84e7e-a6bf-48f2-a855-8e82173445dd",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "DemoTenant",
      "1bdc3b73-804b-4e43-b49f-3b624bf57d54##3fd84e7e-a6bf-48f2-a855-8e82173445dd"
    ],
    "uuid": "ed5505d8-cb5a-449a-8bb9-527f28049c99",
    "sub_system": "CSO",
    "region": "9e8d52c9-34c7-40dc-b26a-ba458db62fad",
    "counter": 1,
    "uri": "/fmpm-provider/alert_status_object/ed5505d8-cb5a-449a-8bb9-527f28049c99",
    "object_id": "3fd84e7e-a6bf-48f2-a855-8e82173445dd",
    "source": "device",
    "id_perms": {
      "enable": true,
      "uuid": {

```

```
        "uuid_mslong": 17101581588692092058,
        "uuid_lslong": 10068169148049169561
    },
    "created": "2020-07-23T07:46:00.211786",
    "description": null,
    "creator": "admin",
    "user_visible": true,
    "last_modified": "2020-07-23T07:46:00.211786",
    "modifier": "admin",
    "permissions": {
        "owner": "admin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
    }
},
"attributes": {
    "system_alarm": "True"
},
"parent_uri": "/fmpm-provider/project/3a35363e-0928-46d2-bd1c-d1d2a91cec8f"
}
```

4.7.13. Site-Edit Failure Alarm

```

{
  "alert_status_object": {
    "last_update_time": 1598604318,
    "alert_type": "service",
    "site_name": "nfx-site",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "object_type": "UCPE_DEVICE",
    "parent_type": "project",
    "site": "9312648b-f964-4a14-a66e-7305f5a10efd",
    "id": "6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0##/6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0/hub_edit_to_site/E15_edited_property",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0##/6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0/hub_edit_to_site/E15_edited_property"
    ],
    "uuid": "ba23ea81-76c5-42f3-9ee0-b68de3580c1f",
    "sub_system": "CSO",
    "object_id": "/6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0/hub_edit_to_site/E15_edited_property",
    "source": "DEVICE",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 13412821957003789043,
        "uuid_lslong": 11448350973296643103
      }
    },
    "created": "2020-08-27T14:42:49.104126",
    "description": null,
    "creator": "cspadmin",
    "user_visible": true,
    "last_modified": "2020-08-28T08:45:31.270113",
    "modifier": "cspadmin",
    "permissions": {
      "owner": "cspadmin",
      "owner_access": 7,
      "other_access": 7,
      "group": "_member_",
      "group_access": 7
    }
  },
  "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9",
  "region_name": null,
  "start_time": 1598539366.902576,
  "reason": "E15_edited_property changed status to Adding E-hub E15 to site S31 failed",
  "perms2": {

```

```

    "owner": "1462d2272131478e8f78a4995f73b8e9",
    "owner_access": 7,
    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "45f1033764954b899cee9f6ea25a667f"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ],
    "device": "6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0",
    "display_name": "/6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0/hub_edit_to_site/E15_edited_property",
    "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "severity": "major",
    "name": "6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0##/6d8cb4a7-1a52-437d-a66d-c2b8ea8ec1f0/hub_edit_to_site/E15_edited_property",
    "counter": 4,
    "uri": "/fmpm-provider/alert_status_object/ba23ea81-76c5-42f3-9ee0-b68de3580c1f",
    "pop_name": null,
    "opco_name": null
  }
}

```

4.7.14. Site-Edit Alarm for “DHCP Update”

```

{
  "alert_status_object": {
    "last_update_time": 1598259132,
    "alert_type": "service",
    "site_name": "nfx-site",
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "tenant_name": "tenant",
    "start_time": 1597306412.92613,
    "object_type": "UCPE_DEVICE",
    "parent_type": "project",
    "site": "17312cf8-617b-4780-b97f-678746881d18",
    "reason": "Workflow started on Address change",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",
      "owner_access": 7,
      "global_access": 0,
      "share": [
        {
          "tenant_access": 7,
          "tenant": "45f1033764954b899cee9f6ea25a667f"
        },
        {
          "tenant_access": 4,
          "tenant": "share.child_projects"
        }
      ]
    },
    "device": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "display_name": "/site_edit/dhcp_update_WAN_1/a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "id": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/site_edit/dhcp_update_WAN_1/a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "tenant": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "name": "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/site_edit/dhcp_update_WAN_1/a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "tenant",
      "a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb##/site_edit/dhcp_update_WAN_1/a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb"
    ],
    "uuid": "669c6e14-b8d6-4bcf-811d-71c7a75e1f00",
    "sub_system": "CSO",
    "counter": 17,
    "uri": "/fmpm-provider/alert_status_object/669c6e14-b8d6-4bcf-811d-71c7a75e1f00",
    "object_id": "/site_edit/dhcp_update_WAN_1/a526f629-67ad-44ec-9bcc-a3f3c0ba5ccb",
    "severity": "major",
    "source": "DEVICE",
    "id_perms": {

```

```
"enable": true,
"uuid": {
  "uuid_mslong": 7393905723514964943,
  "uuid_lslong": 9303717507537706752
},
"created": "2020-08-13T08:13:36.611165",
"description": null,
"creator": "cspadmin",
"user_visible": true,
"last_modified": "2020-08-24T08:52:12.337142",
"modifier": "admin",
"permissions": {
  "owner": "cspadmin",
  "owner_access": 7,
  "other_access": 7,
  "group": "_member_",
  "group_access": 7
}
},
"parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9"
}
```

4.7.15. DVPN Tenant Tunnel Threshold Exceeded Alarm

```

{
  "alert_status_object": {
    "last_update_time": 1599648668,
    "alert_type": "service",
    "site_name": "SPOAM",
    "parent_uuid": "00ff0f57-b9df-4149-9928-77d5009238cd",
    "tenant_name": "default-project",
    "object_type": "UCPE_DEVICE",
    "parent_type": "project",
    "site": "all",
    "id": "/oam/tunnel_threshold/H0_IPSEC_tunnels_count",
    "category": "alarm",
    "fq_name": [
      "default-domain",
      "default-project",
      "/oam/tunnel_threshold/H0_IPSEC_tunnels_count"
    ],
    "uuid": "d031753c-5ad9-4aa1-8b57-60d85fd60a86",
    "sub_system": "CSO",
    "object_id": "/oam/tunnel_threshold/H0_IPSEC_tunnels_count",
    "source": "TENANT",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 15001900735830510241,
        "uuid_lslong": 10040600376682875526
      },
      "created": "2020-08-11T09:07:15.455439",
      "description": null,
      "creator": "cspadmin",
      "user_visible": true,
      "last_modified": "2020-09-09T10:51:09.689780",
      "modifier": "cspadmin",
      "permissions": {
        "owner": "cspadmin",
        "owner_access": 7,
        "other_access": 7,
        "group": "admin",
        "group_access": 7
      }
    },
    "parent_uri": "/fmpm-provider/project/00ff0f57-b9df-4149-9928-77d5009238cd",
    "region_name": null,
    "start_time": 1597136834.346286,
    "reason": "H0_IPSEC_tunnels_count changed status to 3% of the max allowed value 300 for the hub device H0 ",
    "perms2": {
      "owner": "00ff0f57b9df4149992877d5009238cd",
      "owner_access": 7,
      "global_access": 0,

```

```

        "share": [
            {
                "tenant_access": 4,
                "tenant": "share.child_projects"
            }
        ],
        "device": "d6297ef0-3ab9-4a2e-8158-526453ef43f1",
        "display_name": "/oam/tunnel_threshold/H0_IPSEC_tunnels_count",
        "tenant": "00ff0f57-b9df-4149-9928-77d5009238cd",
        "severity": "major",
        "name": "/oam/tunnel_threshold/H0_IPSEC_tunnels_count",
        "counter": 68,
        "uri": "/fmpm-provider/alert_status_object/d031753c-5ad9-4aa1-8b57-60d85fd60a86",
        "pop_name": null,
        "opco_name": null
    }
}

```

4.8. Performance Management

4.8.1. Overview

In addition to monitoring various elements, CSO collects and stores various statistical counters related to resource, interface, traffic and SLA. These counters are collected using agents (device or cloud) and syslogs. These counters are stored as a time-series which can be accessed using CSO API using filters and time-range.

4.8.2. Service Metrics

Get Service Metrics for a Site

POST /fmpm-provider/get_service_metrics

```

{"input": {
    "period": "1d",
    "site": "183364ab-00ce-4956-8745-55724e8e8d44",
    "tenant": "b444a895-b7e1-43bc-a4aa-2bfdc269c0cc"
}}

```

JSON

```

{
  "output":{
    "status":"success",
    "input_time":{
      "period":"1d"
    },
    "metric":null,
    "group_by":"DEVICE",
    "metrics_ts":[
      {
        "DEVICE":"526bbe9d-4f43-4bd3-ad72-5a1449436692",
        "metrics_list":[
          {
            "timestamp":"1527256412645580",
            "/SRX/interfaces/ge-0/0/2/stats/input-rate":46750431,
            "/SRX/system/resources/load-average":0,
            "COMPONENT":"SRX",
            "/SRX/system/resources/load-average-15":0,
            "/SRX/interfaces/ge-0/0/2/stats/output-rate":45225581,
            "/SRX/system/failed-sessions":425913641,
            "/SRX/system/resources/load-average-5":0,
            "/SRX/system/active-sessions":5,
            "/SRX/system/alarm-count":1,
            "/SRX/system/resources/used-memory":52,
            "/SRX/system/resources/total-memory":977
          },
          {
            "/SRX/system/resources/load-average":0,
            "timestamp":"1527173601477120",
            "/SRX/interfaces/ge-0/0/2/stats/input-rate":4228,
            "/SRX/system/failed-sessions":425913641,
            "COMPONENT":"SRX",
            "/SRX/system/resources/load-average-15":0,
            "/SRX/interfaces/ge-0/0/2/stats/output-rate":8963,
            "/SRX/system/resources/load-average-5":0,
            "/SRX/system/active-sessions":2,
            "/SRX/system/alarm-count":1,
            "/SRX/system/resources/used-memory":51,
            "/SRX/system/resources/total-memory":977
          },
          {
            "timestamp":"1527227608654620",
            "/SRX/interfaces/ge-0/0/2/stats/input-rate":4220,
            "/SRX/system/resources/load-average":0,
            "/SRX/system/alarm-count":1,
            "COMPONENT":"SRX",
            "/SRX/system/resources/load-average-15":0,
            "/SRX/interfaces/ge-0/0/2/stats/output-rate":8995,
            "/SRX/system/resources/load-average-5":0,

```

```

    "/SRX/system/active-sessions":2,
    "/SRX/system/failed-sessions":425913641,
    "/SRX/system/resources/used-memory":51,
    "/SRX/system/resources/total-memory":977
  }
]
}
}
}

```

4.8.3. Traffic Metrics

Get Traffic Metrics for a Site

POST /fmpm-provider/get_sdwan_metrics

```

{
  "input": {
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "0427622f-9893-424b-8d93-7a2077e10266",
    "metric": [
      "APP_TX_BYTES",
      "APP_RX_BYTES",
      "APP_TOTAL_BYTES",
      "APP_SESSIONS"
    ],
    "period": "2h"
  }
}

```

JSON

```
{
  "output": {
    "status": "success",
    "data": {
      "default_grouping": {
        "metric_ts": [
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 1,
            "APP_TX_BYTES": 144,
            "timestamp": 1599647940000000,
            "APP_TOTAL_BYTES": 144
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 1,
            "APP_TX_BYTES": 144,
            "timestamp": 1599649020000000,
            "APP_TOTAL_BYTES": 144
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599646860000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 14,
            "APP_TX_BYTES": 2368,
            "timestamp": 1599648840000000,
            "APP_TOTAL_BYTES": 2368
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 6,
            "APP_TX_BYTES": 976,
            "timestamp": 1599647040000000,
            "APP_TOTAL_BYTES": 976
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599648660000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
```

```
"APP_SESSIONS": 2,
"APP_TX_BYTES": 416,
"timestamp": 1599646500000000,
"APP_TOTAL_BYTES": 416
},
{
  "APP_RX_BYTES": 0,
  "APP_SESSIONS": 2,
  "APP_TX_BYTES": 240,
  "timestamp": 1599647760000000,
  "APP_TOTAL_BYTES": 240
},
{
  "APP_RX_BYTES": 1498,
  "APP_SESSIONS": 1,
  "APP_TX_BYTES": 0,
  "timestamp": 1599643800000000,
  "APP_TOTAL_BYTES": 1498
},
{
  "APP_RX_BYTES": 0,
  "APP_SESSIONS": 2,
  "APP_TX_BYTES": 240,
  "timestamp": 1599645600000000,
  "APP_TOTAL_BYTES": 240
},
{
  "APP_RX_BYTES": 0,
  "APP_SESSIONS": 2,
  "APP_TX_BYTES": 416,
  "timestamp": 1599649200000000,
  "APP_TOTAL_BYTES": 416
},
{
  "APP_RX_BYTES": 0,
  "APP_SESSIONS": 2,
  "APP_TX_BYTES": 416,
  "timestamp": 1599645060000000,
  "APP_TOTAL_BYTES": 416
},
{
  "APP_RX_BYTES": 0,
  "APP_SESSIONS": 2,
  "APP_TX_BYTES": 240,
  "timestamp": 1599649740000000,
  "APP_TOTAL_BYTES": 240
},
{
  "APP_RX_BYTES": 0,
  "APP_SESSIONS": 2,
```

```

        "APP_TX_BYTES": 416,
        "timestamp": 1599647220000000,
        "APP_TOTAL_BYTES": 416
      }
    ]
  }
}

```

Get Traffic Metrics for a Site, Group-By Links (Overlay + Local Breakout)

POST /fmppm-provider/get_sdwan_metrics

```

{
  "input": {
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "0427622f-9893-424b-8d93-7a2077e10266",
    "metric": [
      "LINK_TX_BYTES",
      "LINK_RX_BYTES",
      "LINK_TOTAL_BYTES",
      "LINK_SESSIONS"
    ],
    "period": "2h",
    "groupby": ["LINK"]
  }
}

```

JSON

```
{
  "output": {
    "status": "success",
    "data": {
      "default_grouping": {
        "metric_ts": [
          {
            "LINK_SESSIONS": 1,
            "LINK_TX_BYTES": 144,
            "LINK_TOTAL_BYTES": 144,
            "timestamp": 1599649020000000,
            "LINK_RX_BYTES": 0
          },
          {
            "LINK_SESSIONS": 2,
            "LINK_TX_BYTES": 240,
            "LINK_TOTAL_BYTES": 240,
            "timestamp": 1599649740000000,
            "LINK_RX_BYTES": 0
          },
          {
            "LINK_SESSIONS": 2,
            "LINK_TX_BYTES": 416,
            "LINK_TOTAL_BYTES": 416,
            "timestamp": 1599646860000000,
            "LINK_RX_BYTES": 0
          },
          {
            "LINK_SESSIONS": 1,
            "LINK_TX_BYTES": 144,
            "LINK_TOTAL_BYTES": 144,
            "timestamp": 1599647940000000,
            "LINK_RX_BYTES": 0
          },
          {
            "LINK_SESSIONS": 6,
            "LINK_TX_BYTES": 976,
            "LINK_TOTAL_BYTES": 976,
            "timestamp": 1599647040000000,
            "LINK_RX_BYTES": 0
          },
          {
            "LINK_SESSIONS": 2,
            "LINK_TX_BYTES": 240,
            "LINK_TOTAL_BYTES": 240,
            "timestamp": 1599647760000000,
            "LINK_RX_BYTES": 0
          },
          {
            "LINK_SESSIONS": 2,
```

```

        "LINK_TX_BYTES": 416,
        "LINK_TOTAL_BYTES": 416,
        "timestamp": 1599646500000000,
        "LINK_RX_BYTES": 0
    },
    {
        "LINK_SESSIONS": 2,
        "LINK_TX_BYTES": 416,
        "LINK_TOTAL_BYTES": 416,
        "timestamp": 1599648660000000,
        "LINK_RX_BYTES": 0
    },
    {
        "LINK_SESSIONS": 2,
        "LINK_TX_BYTES": 240,
        "LINK_TOTAL_BYTES": 240,
        "timestamp": 1599645600000000,
        "LINK_RX_BYTES": 0
    },
    {
        "LINK_SESSIONS": 2,
        "LINK_TX_BYTES": 416,
        "LINK_TOTAL_BYTES": 416,
        "timestamp": 1599649200000000,
        "LINK_RX_BYTES": 0
    },
    {
        "LINK_SESSIONS": 2,
        "LINK_TX_BYTES": 416,
        "LINK_TOTAL_BYTES": 416,
        "timestamp": 1599645060000000,
        "LINK_RX_BYTES": 0
    },
    {
        "LINK_SESSIONS": 14,
        "LINK_TX_BYTES": 2368,
        "LINK_TOTAL_BYTES": 2368,
        "timestamp": 1599648840000000,
        "LINK_RX_BYTES": 0
    },
    {
        "LINK_SESSIONS": 2,
        "LINK_TX_BYTES": 416,
        "LINK_TOTAL_BYTES": 416,
        "timestamp": 1599647220000000,
        "LINK_RX_BYTES": 0
    }
}
]
}
}

```

```
}  
}
```

Get Traffic Metrics for a Site, Group-By SLA profiles

POST /fmpm-provider/get_sdwan_metrics

JSON

```
{  
  "input": {  
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",  
    "site": "0427622f-9893-424b-8d93-7a2077e10266",  
    "metric": [  
      "APP_TX_BYTES",  
      "APP_RX_BYTES",  
      "APP_TOTAL_BYTES",  
      "APP_SESSIONS"  
    ],  
    "period": "2h",  
    "group_by": ["SLA_PROFILE"]  
  }  
}
```

```

{
  "output": {
    "status": "success",
    "data": {
      "DEFAULT": {
        "metric_ts": [
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599649200000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599648660000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 6,
            "APP_TX_BYTES": 976,
            "timestamp": 1599647040000000,
            "APP_TOTAL_BYTES": 976
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 240,
            "timestamp": 1599649740000000,
            "APP_TOTAL_BYTES": 240
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 240,
            "timestamp": 1599645600000000,
            "APP_TOTAL_BYTES": 240
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 240,
            "timestamp": 1599651900000000,
            "APP_TOTAL_BYTES": 240
          },
          {
            "APP_RX_BYTES": 0,

```

```
"APP_SESSIONS": 14,  
"APP_TX_BYTES": 2368,  
"timestamp": 1599648840000000,  
"APP_TOTAL_BYTES": 2368  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 2,  
  "APP_TX_BYTES": 416,  
  "timestamp": 1599645060000000,  
  "APP_TOTAL_BYTES": 416  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 2,  
  "APP_TX_BYTES": 240,  
  "timestamp": 1599647760000000,  
  "APP_TOTAL_BYTES": 240  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 2,  
  "APP_TX_BYTES": 416,  
  "timestamp": 1599646860000000,  
  "APP_TOTAL_BYTES": 416  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 2,  
  "APP_TX_BYTES": 416,  
  "timestamp": 1599646500000000,  
  "APP_TOTAL_BYTES": 416  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 1,  
  "APP_TX_BYTES": 144,  
  "timestamp": 1599647940000000,  
  "APP_TOTAL_BYTES": 144  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 1,  
  "APP_TX_BYTES": 144,  
  "timestamp": 1599649020000000,  
  "APP_TOTAL_BYTES": 144  
},  
{  
  "APP_RX_BYTES": 0,  
  "APP_SESSIONS": 2,
```

```

        "APP_TX_BYTES": 416,
        "timestamp": 1599647220000000,
        "APP_TOTAL_BYTES": 416
      }
    ]
  }
}

```

Get Traffic Metrics for a Site, filtered for an Overlay link

POST /fmpm-provider/get_sdwan_metrics

JSON

```

{
  "input": {
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "0427622f-9893-424b-8d93-7a2077e10266",
    "input_filters": {
      "filters": [
        {
          "entity": "LINK",
          "entity_id": [
            "5fba9e59b1177003c9245d16a8ef44c9",
            "fb1a3ed3215fb1857f4f53db4b3c9455"
          ]
        }
      ]
    },
    "metric": [
      "APP_RX_BYTES",
      "APP_TX_BYTES",
      "APP_TOTAL_BYTES",
      "APP_SESSIONS"
    ],
    "period": "2h"
  }
}

```

```
{
  "output": {
    "status": "success",
    "data": {
      "default_grouping": {
        "metric_ts": [
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599645060000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 1,
            "APP_TX_BYTES": 144,
            "timestamp": 1599649020000000,
            "APP_TOTAL_BYTES": 144
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599646860000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 14,
            "APP_TX_BYTES": 2368,
            "timestamp": 1599648840000000,
            "APP_TOTAL_BYTES": 2368
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 6,
            "APP_TX_BYTES": 976,
            "timestamp": 1599647040000000,
            "APP_TOTAL_BYTES": 976
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599648660000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
```

```

        "APP_SESSIONS": 2,
        "APP_TX_BYTES": 416,
        "timestamp": 1599646500000000,
        "APP_TOTAL_BYTES": 416
    },
    {
        "APP_RX_BYTES": 0,
        "APP_SESSIONS": 2,
        "APP_TX_BYTES": 240,
        "timestamp": 1599647760000000,
        "APP_TOTAL_BYTES": 240
    },
    {
        "APP_RX_BYTES": 0,
        "APP_SESSIONS": 1,
        "APP_TX_BYTES": 144,
        "timestamp": 1599647940000000,
        "APP_TOTAL_BYTES": 144
    },
    {
        "APP_RX_BYTES": 0,
        "APP_SESSIONS": 2,
        "APP_TX_BYTES": 240,
        "timestamp": 1599645600000000,
        "APP_TOTAL_BYTES": 240
    },
    {
        "APP_RX_BYTES": 0,
        "APP_SESSIONS": 2,
        "APP_TX_BYTES": 416,
        "timestamp": 1599649200000000,
        "APP_TOTAL_BYTES": 416
    },
    {
        "APP_RX_BYTES": 0,
        "APP_SESSIONS": 2,
        "APP_TX_BYTES": 240,
        "timestamp": 1599649740000000,
        "APP_TOTAL_BYTES": 240
    },
    {
        "APP_RX_BYTES": 0,
        "APP_SESSIONS": 2,
        "APP_TX_BYTES": 416,
        "timestamp": 1599647220000000,
        "APP_TOTAL_BYTES": 416
    }
}
]
}
}

```

```
}  
}
```

Get Traffic Metrics for a Site, filtered for an Application

POST /fmpm-provider/get_sdwan_metrics

JSON

```
{  
  "input": {  
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",  
    "site": "0427622f-9893-424b-8d93-7a2077e10266",  
    "input_filters": {  
      "filters": [  
        {  
          "entity": "APP",  
          "entity_id": [  
            "DNS"  
          ]  
        }  
      ]  
    },  
    "metric": [  
      "APP_RX_BYTES",  
      "APP_TX_BYTES",  
      "APP_TOTAL_BYTES",  
      "APP_SESSIONS"  
    ],  
    "period": "2h"  
  }  
}
```

```
{
  "output": {
    "status": "success",
    "data": {
      "default_grouping": {
        "metric_ts": [
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599645060000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 1,
            "APP_TX_BYTES": 144,
            "timestamp": 1599649020000000,
            "APP_TOTAL_BYTES": 144
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 240,
            "timestamp": 1599649740000000,
            "APP_TOTAL_BYTES": 240
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 2,
            "APP_TX_BYTES": 416,
            "timestamp": 1599646860000000,
            "APP_TOTAL_BYTES": 416
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 14,
            "APP_TX_BYTES": 2368,
            "timestamp": 1599648840000000,
            "APP_TOTAL_BYTES": 2368
          },
          {
            "APP_RX_BYTES": 0,
            "APP_SESSIONS": 6,
            "APP_TX_BYTES": 976,
            "timestamp": 1599647040000000,
            "APP_TOTAL_BYTES": 976
          },
          {
            "APP_RX_BYTES": 0,
```

```
    "APP_SESSIONS": 2,  
    "APP_TX_BYTES": 416,  
    "timestamp": 1599648660000000,  
    "APP_TOTAL_BYTES": 416  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 2,  
    "APP_TX_BYTES": 416,  
    "timestamp": 1599646500000000,  
    "APP_TOTAL_BYTES": 416  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 2,  
    "APP_TX_BYTES": 240,  
    "timestamp": 1599647760000000,  
    "APP_TOTAL_BYTES": 240  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 1,  
    "APP_TX_BYTES": 144,  
    "timestamp": 1599647940000000,  
    "APP_TOTAL_BYTES": 144  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 2,  
    "APP_TX_BYTES": 240,  
    "timestamp": 1599645600000000,  
    "APP_TOTAL_BYTES": 240  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 2,  
    "APP_TX_BYTES": 416,  
    "timestamp": 1599649200000000,  
    "APP_TOTAL_BYTES": 416  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 2,  
    "APP_TX_BYTES": 240,  
    "timestamp": 1599651900000000,  
    "APP_TOTAL_BYTES": 240  
  },  
  {  
    "APP_RX_BYTES": 0,  
    "APP_SESSIONS": 2,
```

```

        "APP_TX_BYTES": 416,
        "timestamp": 1599647220000000,
        "APP_TOTAL_BYTES": 416
      }
    ]
  }
}

```

4.8.4. SLA Metrics

Get SLA Metrics for a Site, Group-By Links (Overlay)

POST /fmpm-provider/get_sdwan_metrics

JSON

```

{
  "input": {
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "42d58b31-3b0e-4b08-837d-7df5bd25252e",
    "metric": [
      "LINK_RTT",
      "LINK_JITTER",
      "LINK_PACKET_LOSS"
    ],
    "period": "2h",
    "group_by": [
      "LINK"
    ]
  }
}

```

```
{
  "output": {
    "status": "success",
    "data": {
      "515a611ab75aa9b4d51c6a675654f229": {
        "metric_ts": [
          {
            "LINK_RTT": 469,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 108,
            "LINK_PACKET_LOSS": 0
          },
          {
            "LINK_RTT": 411,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 120,
            "LINK_PACKET_LOSS": 0
          }
        ]
      },
      "b93ab16b991c13434c3b9af791637a65": {
        "metric_ts": [
          {
            "LINK_RTT": 659,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 280,
            "LINK_PACKET_LOSS": 0
          },
          {
            "LINK_RTT": 466,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 64,
            "LINK_PACKET_LOSS": 0
          }
        ]
      },
      "9900ccf6811e9ea3f2ba9efcd851781f": {
        "metric_ts": [
          {
            "LINK_RTT": 687,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 389,
            "LINK_PACKET_LOSS": 0
          },
          {
            "LINK_RTT": 416,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 65,
            "LINK_PACKET_LOSS": 0
          }
        ]
      }
    }
  }
}
```

```

    ]
  },
  "01981b2278b0fd7bc8bbff29d5956007": {
    "metric_ts": [
      {
        "LINK_RTT": 431,
        "timestamp": 1599652080000000,
        "LINK_JITTER": 106,
        "LINK_PACKET_LOSS": 0
      },
      {
        "LINK_RTT": 424,
        "timestamp": 1599652260000000,
        "LINK_JITTER": 70,
        "LINK_PACKET_LOSS": 0
      }
    ]
  },
  "f5a69441478b54db34773cc11e459eab": {
    "metric_ts": [
      {
        "LINK_RTT": 511,
        "timestamp": 1599652260000000,
        "LINK_JITTER": 174,
        "LINK_PACKET_LOSS": 0
      },
      {
        "LINK_RTT": 472,
        "timestamp": 1599652080000000,
        "LINK_JITTER": 104,
        "LINK_PACKET_LOSS": 0
      }
    ]
  },
  "b74576ba053c7fb03915e1044eb9052f": {
    "metric_ts": [
      {
        "LINK_RTT": 503,
        "timestamp": 1599652260000000,
        "LINK_JITTER": 162,
        "LINK_PACKET_LOSS": 0
      },
      {
        "LINK_RTT": 490,
        "timestamp": 1599652080000000,
        "LINK_JITTER": 101,
        "LINK_PACKET_LOSS": 0
      }
    ]
  },
  ]
},

```

```
"d9b517a07ba4afdf5f5b80806177849c": {
  "metric_ts": [
    {
      "LINK_RTT": 514,
      "timestamp": 1599652260000000,
      "LINK_JITTER": 94,
      "LINK_PACKET_LOSS": 0
    },
    {
      "LINK_RTT": 552,
      "timestamp": 1599652080000000,
      "LINK_JITTER": 62,
      "LINK_PACKET_LOSS": 0
    }
  ]
},
"63ea619390546721250db4d5f60c3131": {
  "metric_ts": [
    {
      "LINK_RTT": 840,
      "timestamp": 1599652080000000,
      "LINK_JITTER": 896,
      "LINK_PACKET_LOSS": 0
    },
    {
      "LINK_RTT": 640,
      "timestamp": 1599652260000000,
      "LINK_JITTER": 190,
      "LINK_PACKET_LOSS": 0
    }
  ]
},
"4663e658eecb62979a3a287120024114": {
  "metric_ts": [
    {
      "LINK_RTT": 528,
      "timestamp": 1599652080000000,
      "LINK_JITTER": 58,
      "LINK_PACKET_LOSS": 0
    },
    {
      "LINK_RTT": 448,
      "timestamp": 1599652260000000,
      "LINK_JITTER": 70,
      "LINK_PACKET_LOSS": 0
    }
  ]
},
"0c153317147b661dce58c4ba7ce6e802": {
  "metric_ts": [
```

```

    {
      "LINK_RTT": 797,
      "timestamp": 1599652080000000,
      "LINK_JITTER": 499,
      "LINK_PACKET_LOSS": 0
    },
    {
      "LINK_RTT": 532,
      "timestamp": 1599652260000000,
      "LINK_JITTER": 146,
      "LINK_PACKET_LOSS": 0
    }
  ]
},
"21b886a07254b7382060aa586db78432": {
  "metric_ts": [
    {
      "LINK_RTT": 440,
      "timestamp": 1599652080000000,
      "LINK_JITTER": 82,
      "LINK_PACKET_LOSS": 0
    },
    {
      "LINK_RTT": 657,
      "timestamp": 1599652260000000,
      "LINK_JITTER": 359,
      "LINK_PACKET_LOSS": 0
    }
  ]
},
"0fb836ff4fc3b7352b7d7970c82be2c0": {
  "metric_ts": [
    {
      "LINK_RTT": 610,
      "timestamp": 1599652260000000,
      "LINK_JITTER": 190,
      "LINK_PACKET_LOSS": 0
    },
    {
      "LINK_RTT": 835,
      "timestamp": 1599652080000000,
      "LINK_JITTER": 905,
      "LINK_PACKET_LOSS": 0
    }
  ]
},
"93ca977505d8653ac3c72e6b75a04983": {
  "metric_ts": [
    {
      "LINK_RTT": 809,

```

```

        "timestamp": 1599652080000000,
        "LINK_JITTER": 871,
        "LINK_PACKET_LOSS": 0
    },
    {
        "LINK_RTT": 567,
        "timestamp": 1599652260000000,
        "LINK_JITTER": 160,
        "LINK_PACKET_LOSS": 0
    }
]
},
"78e04a6af92ddee2da92a8af3adc0126": {
    "metric_ts": [
        {
            "LINK_RTT": 511,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 71,
            "LINK_PACKET_LOSS": 0
        },
        {
            "LINK_RTT": 786,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 892,
            "LINK_PACKET_LOSS": 0
        }
    ]
},
"2097c061847473b3aff30fbe44d94f4f": {
    "metric_ts": [
        {
            "LINK_RTT": 622,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 334,
            "LINK_PACKET_LOSS": 0
        },
        {
            "LINK_RTT": 596,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 117,
            "LINK_PACKET_LOSS": 0
        }
    ]
},
"2a8aed9074a3951f06c574040793424a": {
    "metric_ts": [
        {
            "LINK_RTT": 568,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 96,

```

```

        "LINK_PACKET_LOSS": 0
      },
      {
        "LINK_RTT": 599,
        "timestamp": 1599652080000000,
        "LINK_JITTER": 97,
        "LINK_PACKET_LOSS": 0
      }
    ]
  }
}

```

Get SLA Metrics for a Site, filtered for an Overlay link

JSON

```

{
  "input": {
    "input_filters": {
      "filters": [
        {
          "entity": "LINK",
          "entity_id": [
            "f5a69441478b54db34773cc11e459eab",
            "0c153317147b661dce58c4ba7ce6e802"
          ]
        }
      ]
    },
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "42d58b31-3b0e-4b08-837d-7df5bd25252e",
    "metric": [
      "LINK_RTT",
      "LINK_JITTER",
      "LINK_PACKET_LOSS"
    ],
    "period": "5m",
    "group_by": [
      "LINK"
    ]
  }
}

```

```

{
  "output": {
    "status": "success",
    "data": {
      "f5a69441478b54db34773cc11e459eab": {
        "metric_ts": [
          {
            "LINK_RTT": 472,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 104,
            "LINK_PACKET_LOSS": 0
          },
          {
            "LINK_RTT": 511,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 174,
            "LINK_PACKET_LOSS": 0
          }
        ]
      },
      "0c153317147b661dce58c4ba7ce6e802": {
        "metric_ts": [
          {
            "LINK_RTT": 797,
            "timestamp": 1599652080000000,
            "LINK_JITTER": 499,
            "LINK_PACKET_LOSS": 0
          },
          {
            "LINK_RTT": 532,
            "timestamp": 1599652260000000,
            "LINK_JITTER": 146,
            "LINK_PACKET_LOSS": 0
          }
        ]
      }
    }
  }
}

```

Get Application SLA Metrics for a Site, Group-By SLA profiles

POST /fmpm-provider/get_sdwan_metrics

```
{
  "input": {
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "42d58b31-3b0e-4b08-837d-7df5bd25252e",
    "metric": [
      "APP_RTT",
      "APP_JITTER",
      "APP_PACKET_LOSS"
    ],
    "period": "5d",
    "group_by": [
      "SLA-PROFILE"
    ]
  }
}
```

```
{
  "output": {
    "status": "success",
    "data": {
      "CNN": {
        "metric_ts": [
          {
            "APP_JITTER": 0,
            "timestamp": 1602852840000000,
            "APP_RTT": 833,
            "APP_PACKET_LOSS": 0
          },
          {
            "APP_JITTER": 115,
            "timestamp": 1602852840000000,
            "APP_RTT": 800,
            "APP_PACKET_LOSS": 0
          }
        ]
      },
      "Wikipedia": {
        "metric_ts": [
          {
            "APP_JITTER": 161,
            "timestamp": 1602852840000000,
            "APP_RTT": 839,
            "APP_PACKET_LOSS": 0
          }
        ]
      },
      "Salesforce": {
        "metric_ts": [
          {
            "APP_JITTER": 140,
            "timestamp": 1602852840000000,
            "APP_RTT": 833,
            "APP_PACKET_LOSS": 0
          },
          {
            "APP_JITTER": 99,
            "timestamp": 1602852840000000,
            "APP_RTT": 762,
            "APP_PACKET_LOSS": 0
          }
        ]
      },
      "WebEx": {
        "metric_ts": [
          {
            "APP_JITTER": 0,
```

```

        "timestamp": 1602852840000000,
        "APP_RTT": 838,
        "APP_PACKET_LOSS": 0
      },
      {
        "APP_JITTER": 195,
        "timestamp": 1602852840000000,
        "APP_RTT": 797,
        "APP_PACKET_LOSS": 0
      }
    ]
  }
}
}
}

```

Get Application SLA Metrics for a Site, filtered for an SLA profile

POST /fmpm-provider/get_sdwan_metrics

JSON

```

{
  "input": {
    "input_filters": {
      "filters": [
        {
          "entity": "SLA_PROFILE",
          "entity_id": [
            "CNN"
          ]
        }
      ]
    },
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "42d58b31-3b0e-4b08-837d-7df5bd25252e",
    "metric": [
      "APP_RTT",
      "APP_JITTER",
      "APP_PACKET_LOSS"
    ],
    "period": "5m",
    "group_by": [
      "SLA_PROFILE"
    ]
  }
}

```

```
{
  "output": {
    "status": "success",
    "data": {
      "CNN": {
        "metric_ts": [
          {
            "APP_JITTER": 0,
            "timestamp": 1602852480000000,
            "APP_RTT": 826,
            "APP_PACKET_LOSS": 0
          },
          {
            "APP_JITTER": 81,
            "timestamp": 1602852480000000,
            "APP_RTT": 757,
            "APP_PACKET_LOSS": 0
          },
          {
            "APP_JITTER": 58,
            "timestamp": 1602852660000000,
            "APP_RTT": 817,
            "APP_PACKET_LOSS": 0
          },
          {
            "APP_JITTER": 3,
            "timestamp": 1602852660000000,
            "APP_RTT": 833,
            "APP_PACKET_LOSS": 0
          }
        ]
      }
    }
  }
}
```

Get Application SLA Metrics for a Site, Group-By SLA profiles and Applications

POST /fmpm-provider/get_sdwan_metrics

```
{
  "input": {
    "tenant": "3a35363e-0928-46d2-bd1c-d1d2a91cec8f",
    "site": "42d58b31-3b0e-4b08-837d-7df5bd25252e",
    "metric": [
      "APP_RTT",
      "APP_JITTER",
      "APP_PACKET_LOSS"
    ],
    "period": "5m",
    "group_by": [
      "SLA_PROFILE", "APP"
    ]
  }
}
```

```

{
  "output": {
    "status": "success",
    "data": {
      "CNN": {
        "CNN": {
          "metric_ts": [
            {
              "APP_JITTER": 3,
              "timestamp": 1602852660000000,
              "APP_RTT": 833,
              "APP_PACKET_LOSS": 0
            },
            {
              "APP_JITTER": 58,
              "timestamp": 1602852660000000,
              "APP_RTT": 817,
              "APP_PACKET_LOSS": 0
            },
            {
              "APP_JITTER": 115,
              "timestamp": 1602852840000000,
              "APP_RTT": 800,
              "APP_PACKET_LOSS": 0
            },
            {
              "APP_JITTER": 0,
              "timestamp": 1602852840000000,
              "APP_RTT": 833,
              "APP_PACKET_LOSS": 0
            }
          ]
        }
      }
    }
  }
}

```

4.9. SDWAN Events

4.9.1. Overview

Syslogs are used to generate “link-switch” events that denote events when traffic is switched due to sla-violation in the device. These “link-switch” events capture “from” and “to” tunnels, timestamp, SLA profile, applications and values of SLA parameters when violation was

detected. Note that one link-switch may be created using multiple appqoe syslogs, these syslogs are discarded after event is created however link-switch events can be retrieved using CSP API.

CSO also generates events when a DVPN tunnel is created/deleted, these events can be retrieved using CSP API.

4.9.2. Dynamic VPN

This event is created when an overlay tunnel is created after meeting a criteria defined for DVPN tunnel creation. Here is an example object –

```

{
  "dvpn_event": {
    "parent_uuid": "1462d227-2131-478e-8f78-a4995f73b8e9",
    "timestamp": 1597662871.821015,
    "vpn_name": "tenant_DefaultVPN",
    "parent_type": "project",
    "perms2": {
      "owner": "1462d2272131478e8f78a4995f73b8e9",
      "owner_access": 7,
      "global_access": 0,
      "share": [
        {
          "tenant_access": 7,
          "tenant": "45f1033764954b899cee9f6ea25a667f"
        },
        {
          "tenant_access": 4,
          "tenant": "share.child_projects"
        }
      ]
    },
    "display_name": "70b56ecd-9d91-4d12-ae1e-3374c500b268",
    "tunnel_count": 0,
    "name": "70b56ecd-9d91-4d12-ae1e-3374c500b268",
    "site2_id": "08dda429-3f0c-490a-8242-97fdd9ce2231",
    "fq_name": [
      "default-domain",
      "tenant",
      "70b56ecd-9d91-4d12-ae1e-3374c500b268"
    ],
    "uuid": "eac47984-c0da-4db0-9abd-87980a019f95",
    "vpn_id": "ed53d8f7-1052-4718-9bbf-75d675acd378",
    "tenant_id": "1462d2272131478e8f78a4995f73b8e9",
    "uri": "/fmpm-provider/dvpn_event/eac47984-c0da-4db0-9abd-87980a019f95",
    "tunnels_type": "STATIC",
    "site1_id": "75a0049a-178a-4a72-8c06-a98a68e397fc",
    "id_perms": {
      "enable": true,
      "uuid": {
        "uuid_mslong": 16916779711388601776,
        "uuid_lslong": 11150217339511873429
      }
    },
    "created": "2020-08-17T11:14:32.046671",
    "description": null,
    "creator": "cspadmin",
    "user_visible": true,
    "last_modified": "2020-08-17T11:14:32.046671",
    "modifier": "cspadmin",
    "permissions": {
      "owner": "cspadmin",

```

```
        "owner_access": 7,  
        "other_access": 7,  
        "group": "_member_",  
        "group_access": 7  
    },  
    },  
    "details": {  
        "reason": "add-wan-link"  
    },  
    "action": "UPDATE",  
    "parent_uri": "/fmpm-provider/project/1462d227-2131-478e-8f78-a4995f73b8e9"  
}  
}
```

4.9.3. Get DVPN events for a given site

GET

/fmpm-provider/dvpn_event?detail=true&filter=site2_id=08dda429-3f0c-490a-8242-97fdd9ce2231) or (site1_id=08dda429-3f0c-490a-8242-97fdd9ce2231

Response format is same as above.

4.9.4. Get DVPN events for a given time range

GET /fmpm-provider/dvpn_event?detail=true&filter=timestamp>1597662870) and (timestamp<1597662872

Response format is same as above.

4.9.5. Link switch

This event is created when application traffic in the device is switched to a link meeting a pre-defined SLA criteria (AppQoS feature). An alarm object is also created for these events that allows these events to be received asynchronously using SSE (refer here).

```

{
  "parent_uuid": "142dafe8-41fa-43bb-a67f-c68d255090fe",
  "start_time": 1602827940,
  "parent_type": "project",
  "site": "2ca64cb7-da96-43f5-9e0a-86fd7f65ed91",
  "src_link": "3368400cf13505c5c09cb8377c7a7493",
  "metrics": {
    "loss": {
      "status": "ERROR",
      "max": 2,
      "target": "1"
    },
    "jitter": {
      "status": "OK",
      "max": 878,
      "target": "30000"
    },
    "rtt": {
      "status": "OK",
      "max": 2639,
      "target": "150000"
    }
  },
  "reason": "LINK_SWITCH",
  "perms2": {
    "owner": "142dafe841fa43bba67fc68d255090fe",
    "owner_access": 7,
    "global_access": 0,
    "share": [
      {
        "tenant_access": 7,
        "tenant": "64345ae05c154dc7a9f15d219f9b0e39"
      },
      {
        "tenant_access": 4,
        "tenant": "share.child_projects"
      }
    ]
  },
  "duration": 0,
  "display_name": "eac5e22a-0937-4018-b290-3ebEFF3de800",
  "dst_link": "3368400cf13505c5c09cb8377c7a7493",
  "tenant": "142dafe8-41fa-43bb-a67f-c68d255090fe",
  "uuid": "1f06527f-f1c6-4ca3-8904-1ea23eef95bb",
  "fq_name": [
    "default-domain",
    "TEST",
    "eac5e22a-0937-4018-b290-3ebEFF3de800"
  ],
  "name": "eac5e22a-0937-4018-b290-3ebEFF3de800",

```

```

"sla_profile": "TEST-GOLD",
"apps": [
  "RTP",
  "N/A"
],
"uri": "/fmpm-provider/sla_event/1f06527f-f1c6-4ca3-8904-1ea23eef95bb",
"departments": [
  null
],
"id_perms": {
  "enable": true,
  "uuid": {
    "uuid_mslong": 2235564974506658979,
    "uuid_lslong": 9873049965292393915
  },
  "created": "2020-10-16T05:59:12.995163",
  "description": null,
  "creator": "admin",
  "user_visible": true,
  "last_modified": "2020-10-16T05:59:12.995163",
  "modifier": "admin",
  "permissions": {
    "owner": "admin",
    "owner_access": 7,
    "other_access": 7,
    "group": "_member_",
    "group_access": 7
  }
},
"end_time": 1602827940,
"type": "sla_event",
"parent_uri": "/fmpm-provider/project/142dafa8-41fa-43bb-a67f-c68d255090fe"
}

```

4.9.6. Get link switch events for a given site

GET /fmpm-provider/sla_event?detail=true&filter=(site=2ca64cb7-da96-43f5-9e0a-86fd7f65ed91)

Response format is same as above.

4.9.7. Get link switch events for a given time range

GET /fmpm-provider/sla_event?detail=true&filter=timestamp>1597662870) and (timestamp<1597662872

Response format is same as above.

4.10. Upstream Notifications From CSO

4.10.1. Server-Sent Events

Apart from retrieving various objects and metrics using API, CSO also allows upstream subsystems to receive asynchronous notifications via Server-Sent Events (SSE). An application can subscribe to these events by writing an SSE client by pointing to a well-defined url. A pre-defined set of object types are published by CSO for this subscription to allow client application to receive notifications from CSO. Alarm objects defined in this document are available via SSE notifications (Refer to the SSE notification section in CSO overview chapter).

4.10.2. Syslog forwarding

CSO does not support forwarding of raw syslogs to upstream systems. If needed, this can be achieved via configuring an external syslog server in the device directly.

5. Security Management RESTful API Reference and Logging



The API examples provided in this chapter are meant for illustrative purpose only. For more information about the specific APIs, see **Chapter 7 - API Reference**

The Juniper Contrail Service Orchestration (CSO) security management APIs allow you to manage security-related services and schedulers:

- **Security services APIs** - Allow you to create, modify, and delete security-related services (applications running on devices) in both your test and deployment environments. Domain Name System (DNS) is an example of a security service. Such services are based on protocols and ports used by applications. When services are added to a policy, a configured service or group of services can be applied across all devices associated with the policy.



Services are candidates for firewall policy endpoints. The protocols used to create a service includes: TCP, UDP, MSRPC, Sun RPC, ICMP, and ICMPv6.



In addition to the services listed in this section, CSO also includes predefined services that you cannot modify or delete.

- **Security Scheduler APIs** - Allow you to create, modify, and delete schedulers in both your test and deployment environment. The schedulers allow you to specify the duration of policies. To enable a policy for a specified time, you must either create a schedule for that policy or link the policy to an existing schedule. When a schedule times out, the associated policy is deactivated and all sessions associated with the policy expire.

Table 21 provides related information about the security management reference and logging APIs:

Table 4. Related Information

API	Description
Security management	<u>Security Management</u>

API	Description
Security management-application statistics	<u>Security Management - Application Statistics</u>
Security management-events	<u>Security Management - Events</u>
Security management-reports	<u>Security Management - Reports</u>

6. Glossary

For glossary of terms, see **Juniper Networks Glossary**

(https://www.juniper.net/documentation/en_US/release-independent/glossary/index.html).

7. API Reference

Use the Contrail Services Orchestration (CSO) APIs to orchestrate processes for developing portals, applications and automations. You can use these APIs to automate various tasks, processes and workflows as you design, deploy and monitor the services that you provide for your customers.

Two categories of CSO APIs exist:

- **Pre-staging APIs**- Cloud administrators and providers to pre-stage their customer implementation and sites. These APIs are used by network service providers to create service offerings.
- **Lifecycle management APIs**. For use by customers, offered to them through their Cloud Services provider portal, to manage the lifecycle of the Network Service that they are purchasing.

Because some complex operations don't easily lend themselves to strict RESTful (CRUD) conventions, the CSO HTTP APIs are available through endpoints to which you can send HTTP requests that map all complex operations to:

- REST CRUD.
- RPC over HTTP.

When creating your requests:

- For each operation that maps to CRUD, the parent parameter is usually a meaningful name.
- For each operation that maps to RPC, the request is always a POST, and the json object that you construct for the request body must have "input" as root.
- Each response that corresponds to a request that maps to RPC begins with the parent parameter "output".

The requests for creating and importing POPs, onboarding tenants, and creating service instances require that you assemble data into properly-formatted json files for the body (payload) of each request.

Refer to the following API documentation:

Service	Path	Description	
<u>Security Management</u>	/api/juniper/sd	Security Management service provides configuration ability for: <ul style="list-style-type: none"> - Scheduler Management - Identity Management - UTM (Unified Threat Management) - NAT Policy Configuration - SSL Proxy Profile Configuration 	
<u>Security Management - Application Statistics</u>	/api/juniper/appvisibility	Application Statistics service provides APIs for detailed application usage as detected by SRX. Detailed statistics can be based on application, user or source IP	
<u>Security Management - Events</u>	/api/juniper/ecm	Event Management service provides APIs to get events collected by the Log Collector. Using these APIs user will be able to get logs based on time range and aggregated logs etc...	
<u>Security Management - Reports</u>	/api/juniper/seci	Report Management service provides CRUD operations for Reports	
<u>activation-service-central</u>	/activation-service-central	Use these Central Activation Service APIs to control details associated with service activation in a centralized deployment.	

<u>cms-central</u>	/cms-central	Use the Central Configuration Management APIs to get information about and manage centralized deployments.	<u>Changes</u>
<u>cslm</u>	/cslm	This service provides APIs for root and trusted certificates management.	
<u>data-view-central</u>	/data-view-central	Data view server is intended to serve the northbound applications such as portals or OSS systems, read-only data with paging, sorting and rich queries. Each view handler in the server collects disparate data from multiple vertexes in one micro service or multiple micro services. This allows Administration Portal to use a relative simple query to retrieve aggregated data for operations, analysis and reporting purpose.	<u>Changes</u>

<u>dms-central</u>	/dms-central	<p>Device Management Service manages the life-cycle of all devices brought under control of CSO.</p> <p>This includes CPEs, HUBs, POP routers, as well as VNFs orchestrated via CSO. Many of the APIs provided by this service are not exposed to north-bound clients directly. Instead they are meant to be consumed by north-bound clients via abstract APIs exposed by the TSSM service.</p>	
<u>fmpm-provider</u>	/fmpm-provider	As part of fault and performance monitoring services, these APIs implement query interfaces to provide information.	<u>Changes</u>
<u>iamsvc</u>	/iamsvc	<p>iamsvc service provides management of:</p> <ul style="list-style-type: none"> - Users - User authorizations - Roles - Authentication methods 	<u>Changes</u>
<u>iamsvc-noauth</u>	/iamsvc-noauth	<p>IAM Utilities provides RPCs to:</p> <ul style="list-style-type: none"> - Change user password - Send email instructions to reset password if user forgot the password - Reset password if user forgot password 	<u>Changes</u>

<u>ims-central</u>	/ims-central	Image Management Service provides APIs using which images can be uploaded to CSO and then deployed to managed devices. These images can be software upgrade packages for managed devices, VNF images, script files to be deployed to devices, license data files, etc.	
<u>inv-central</u>	/inv-central	API of CSP inventory management service.	
<u>job-service</u>	/job-service	APIs to handle job services.	
<u>policy-mgmt</u>	/policy-mgmt	APIs for managing and deploying CSO Policies.	<u>Changes</u>
<u>pslam</u>	/pslam	Policy and SLA profile object management service to enable software-defined WAN (SD-WAN) functions.	
<u>security-objects</u>	/sd-security-objects	APIs for managing and deploying SD Design objects used in policies.	
<u>shared-object</u>	/shared-object	Service to manage Application and Address objects.	<u>Changes</u>
<u>signature-manager</u>	/signature-manager	Service to manage Application signatures.	<u>Changes</u>

<u>topology-service</u>	/topology-service	This service provides APIs for modeling topologies and working with networked elements like devices, hubs, spokes, policy enforcement points, and other objects.	<u>Changes</u>
<u>tssm</u>	/tssm	This service provides APIs for tenant, site and service management.	<u>Changes</u>

Version 6.1.0, API Documentation

Last updated 2021-09-01 06:30:18 +00:00