

SteelConnect EX FlexVNF Basic Configuration Guide

Version 16.1R2

December 2019

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Configuring Organizations | 5 |
| 1.1 | Overview | 5 |
| 1.2 | Creating an organization | 5 |
| 1.2.1 | Adding provider organizations | 5 |
| 1.2.2 | Adding customer organizations..... | 10 |
| 1.2.3 | Deleting or decommissioning organizations | 13 |
| 1.3 | Creating FlexVNF users | 14 |
| 1.3.1 | System user attributes | 14 |
| 1.3.2 | Organization user attributes | 15 |
| 1.3.3 | Default user attributes..... | 15 |
| 2 | Configuring SteelConnect EX FlexVNF appliances..... | 17 |
| 2.1 | Configuring appliances | 17 |
| 2.2 | Configuring appliances using CLI | 19 |
| 2.3 | Certificate management in FlexVNF via SteelConnect EX Director | 19 |
| 2.3.1 | Configuring certificate server..... | 19 |
| 2.3.2 | Configuring certificate request | 22 |
| 2.4 | Applying configured certificates..... | 24 |
| 2.5 | Alarm management | 27 |
| 2.6 | Recent events | 28 |
| 3 | Creating FlexVNF appliances | 31 |
| 3.1 | Creating FlexVNF appliances on OpenStack..... | 36 |
| 3.2 | Creating FlexVNF appliances on bare metal..... | 41 |
| 3.3 | Subjugating SteelConnect EX FlexVNF appliances via SteelConnect EX Director | 45 |
| 3.4 | Alarm management..... | 46 |
| 3.5 | Recent events | 48 |
| 4 | Configuring uCPE on SteelConnect EX FlexVNF | 49 |
| 4.1 | SteelConnect EX uCPE Overview | 49 |
| 4.2 | Configuring uCPE on SteelConnect EX FlexVNF..... | 50 |
| 4.2.1 | Creating a Vendor Catalog..... | 50 |
| 4.2.2 | Creating a Service Chain Template | 53 |

| | |
|--|-----------|
| 4.2.3 Associating Service-Chaining Template with the Device Template | 54 |
| 4.2.4 Adding Devices to the Device Template..... | 55 |
| 4.2.5 Onboarding the device through Zero Touch Provisioning (ZTP) | 56 |
| 4.2.6 Verifying the uCPE Configuration | 56 |
| 4.2.7 Monitoring uCPE | 57 |
| 4.3 Viewing the uCPE on SteelConnect EX Analytics | 58 |
| 4.3.1 Troubleshooting uCPE | 60 |
| 4.3.2 Alarms generation for uCPE..... | 61 |
| 5 Verify SteelConnect EX FlexVNF Operation | 62 |

The following articles describe how to configure basic parameters for FlexVNF devices:

- [Configuring Organizations](#)(see page 5)
- [Configuring SteelConnect EX FlexVNF appliances](#)(see page 17)
- [Creating FlexVNF appliances](#)(see page 31)
- [Configuring uCPE on SteelConnect EX FlexVNF](#)(see page 49)
- [Verify SteelConnect EX FlexVNF Operation](#)(see page 62)

1 Configuring Organizations

- [Overview](#)(see page 5)
- [Creating an organization](#)(see page 5)
 - [Adding provider organizations](#)(see page 5)
 - [Adding customer organizations](#)(see page 10)
 - [Deleting or decommissioning organizations](#)(see page 13)
- [Creating FlexVNF users](#)(see page 14)
 - [System user attributes](#)(see page 14)
 - [Organization user attributes](#)(see page 15)
 - [Default user attributes](#)(see page 15)

1.1 Overview

Organizations are smaller units or departments of a network landscape. They are containers in FlexVNF to create services and resources specific to each organization or tenant. A parent organization can have a hierarchy of one or more child organizations. For example, consider a cloud provider organization, *ServiceProvider*. This provider has multiple customers, *MoneyTrans Bank* and *NextGen Computers*. In the example, *ServiceProvider* is a parent organization and its customers are the child organizations. For each organization, you can configure the required resources and services such as networks, interfaces, routers, objects, subscription plans, firewalls, servers, policies, profiles, etc. The services configured at the parent level are available to the child organizations. The parent organization is created before the child organizations. The procedure to create organizations on vCloud Director, OpenStack, and bare metal is the same.

1.2 Creating an organization


Create an organization (tenant) in SteelConnect EX Director that would connect with one or more available CMS organizations that currently exist in OpenStack.

SteelConnect EX Director supports two types of organizations:

- **Provider organizations.** Add a provider organization using the Organizations tab. Refer to [Adding provider organizations](#)(see page 5).
- **Customer organizations.** Add a customer organization using the Workflows tab. Refer to [Adding customer organizations](#)(see page 10).

1.2.1 Adding provider organizations

Steps

1. In the Director view, go to **Administration > Organizations**.
2. Click the  Add icon to open the **Add Organization** screen.

| Field | Description |
|-------------|---|
| Name | Name of the organization. Example: <i>ServiceProvider</i> |
| Description | Information about the organization. |

| Field | Description |
|--------------------------|---|
| Tags | Tags that help explain the organization. |
| Global Organization ID | Unique ID for the organization |
| Organization Label | Label to identify the organization. |
| Shared Control Plane | Enable or disable sharing of control planes with the parent organization. Organizations with an activated Shared Control Plane do not have their own MPBGP (multi-protocol Border Gateway Protocol) or control-VR routing instance and IPsec tunnels to communicate with controllers. They share the MPBGP and IPsec tunnels of their parent/predecessor organization. |
| Parent Organization | Name of the parent organization. Example: <i>ServiceProvider</i> |
| Authentication Connector | Authentication connector connects to external servers hosting users who connect with SteelConnect EX Director. The servers can be directory services like <i>LDAP</i> and <i>RADIUS</i> . |

| Field | Description |
|-------------------|--|
| Subscription Plan | <p>A subscription plan is a way to measure/price the networking services that IT provides. It contains a list of service node groups (SNG), SteelConnect EX service nodes (VSN) flavors, and elasticity settings (min and max number of VSNs available for SteelConnect EX FlexVNF). The subscription options are:</p> <ul style="list-style-type: none"> ▪ <i>Default NextGen FW NextGen VPN Plan.</i> Configure next generation firewall and next generation VPN. ▪ <i>Default NextGen VPN-Plan.</i> Configure next generation VPN. ▪ <i>Default Stateful FW NextGen VPN Plan.</i> Configure stateful firewall and next generation VPN. ▪ <i>Default-Stateful-FW-Plan.</i> Configure stateful firewall. Default-ADC-Plan. Choose this option to configure an ADC. ▪ <i>Default-ADC-SFW-Plan.</i> Configure an ADC for a stateful firewall. ▪ <i>Default-All-Services-Plan.</i> Configure all services (ADC, CGNAT, IPsec, firewall, et al). ▪ <i>Default-CGNAT-Plan.</i> Configure CGNAT. ▪ <i>Default-CGNAT-SFW-Plan.</i> Configure stateful firewall and CGNAT. ▪ <i>Default-IPSEC-Plan.</i> Configure IPsec. ▪ <i>Default-NextGen-FW-Plan.</i> Configure next generation firewall. ▪ <i>Default-NextGenFW-CGNAT-Plan.</i> Configure next generation firewall and CGNAT. ▪ <i>Default-SFW-IPSEC-CGNAT-Plan.</i> Configure stateful firewall IPsec and CGNAT. ▪ <i>Default-SFW-IPSEC-Plan.</i> Configure stateful firewall IPsec. ▪ <i>Default-Stateful-FW-Plan.</i> Configure stateful firewall. ▪ <i>Default-DPI-Plan.</i> Configure Deep packet inspection. |

- a. Click **CMS Connectors**. From the list of available connectors, select the required connector(s) for the organization.
- b. Click **CMS Organizations** and select and add the available CMS organizations for this organization.

CMS Connectors

CMS Organizations

Analytics Cluster

Routing Instance

Supported User Roles

Available

Add All

Search

rackspace

Selected

Search

OK

Cancel

c. Click **Analytics Connectors**.

CMS Connectors

CMS Organizations

Analytics Cluster

Routing Instance


Supported User Roles

☐ Analytics Cluster

☐ Analytics-1

OK

Cancel

- i. Click the  Add icon to add a cluster.
 - ii. Select a cluster from the list of available clusters.
- d. Click **Routing Instances** to define virtual routing instances for the organization.


CMS Connectors

CMS Organizations

Analytics Cluster

Routing Instance

Supported User Roles

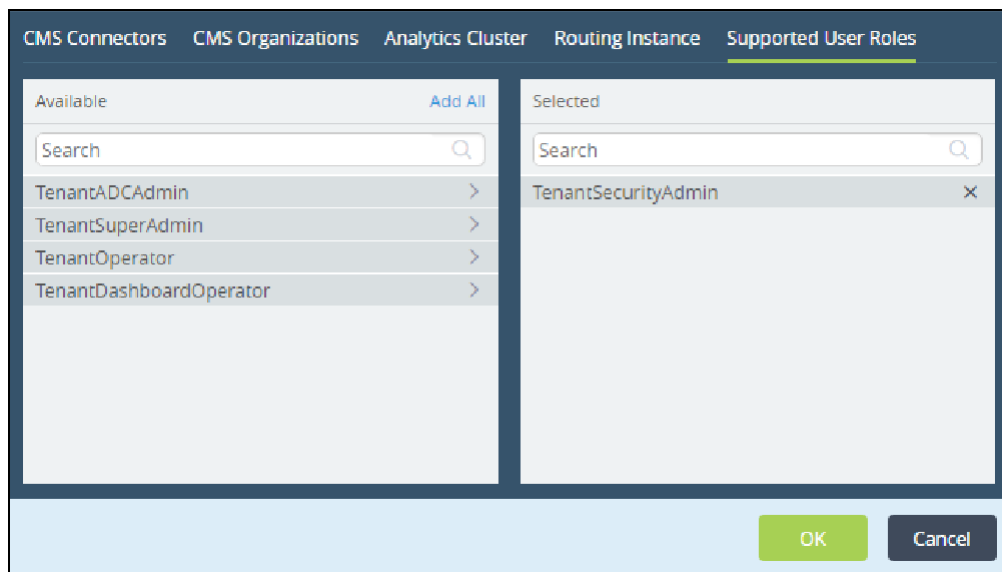
| Name  | Description | ID | VPN | |
|--|-------------|----|---|--------------|
| | | 30 | <input checked="" type="checkbox"/> VPN | <div>+</div> |
| ServiceProvider-LAN-VR | | 29 | <input checked="" type="checkbox"/> | <div></div> |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

OK

Cancel

| Field | Description |
|-------|------------------------|
| Name | Routing instance name. |
| ID | Routing instance ID. |
| VPN | Enable or disable VPN. |

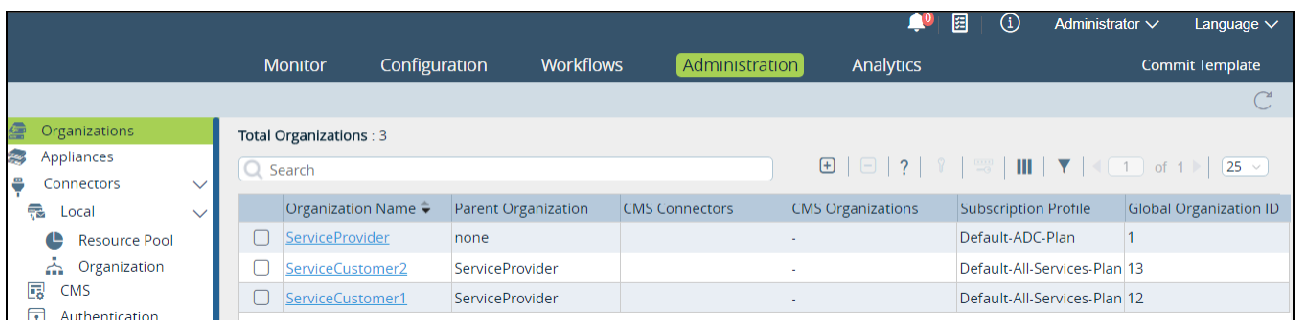
- i. Click the  Add icon.
- e. Click **Supported User Roles**.




- i. From the list of available roles, select the role(s) supported in the organization.


3. Click **OK** to save the settings.


This creates a provider organization. Now, you can create its child organizations.



| Organization Name | Parent Organization | CMS Connectors | CMS Organizations | Subscription Profile | Global Organization ID |
|---|---------------------|----------------|-------------------|---------------------------|------------------------|
| <input type="checkbox"/> ServiceProvider | none | - | - | Default-ADC-Plan | 1 |
| <input type="checkbox"/> ServiceCustomer2 | ServiceProvider | - | - | Default-All-Services-Plan | 13 |
| <input type="checkbox"/> ServiceCustomer1 | ServiceProvider | - | - | Default-All-Services-Plan | 12 |


To remove an organization, select the check box next to the organization name, and click the  Delete icon.

After adding an organization, you can monitor the organization creation process in the Tasks dashboard. In case the organization creation is unsuccessful, view the error messages for possible debug information. To view the Tasks dashboard, click the  Tasks icon seen on the right corner of the top menu bar.

| Tasks | | | | | | | |
|--------------------------|---|------------------------|---------------|-----------------------|---------------------|---------------------|--|
| Failed 0 | | Pending 0 | | Total 1 | | | |
| <input type="checkbox"/> | | ID | User | Activity | Time | | Progress |
| | | | | | Start Time | End Time | |
| <input type="checkbox"/> | > | 1 | Administrator | Create-Baremetal A... | 2016-05-23 15:05:32 | 2016-05-23 15:05:46 | createAppliance: ap...  |

1.2.2 Adding customer organizations

Steps

1. In the Director view, go to **Workflows > Infrastructure > Organizations**.
2. Click the  Add icon to onboard an organization.

Create Organization

Organization

Name*

ServiceCustomer

Global Organization ID

2

Parent

ServiceProvider

IKE Authentication

PSK

SCP

Shared Control Plane

Controllers

CMS Connectors

Analytics Cluster

Routing Instances

Supported User Roles

Controllers

Available

Add All

Search

Selected

Remove All

Search

Cancel

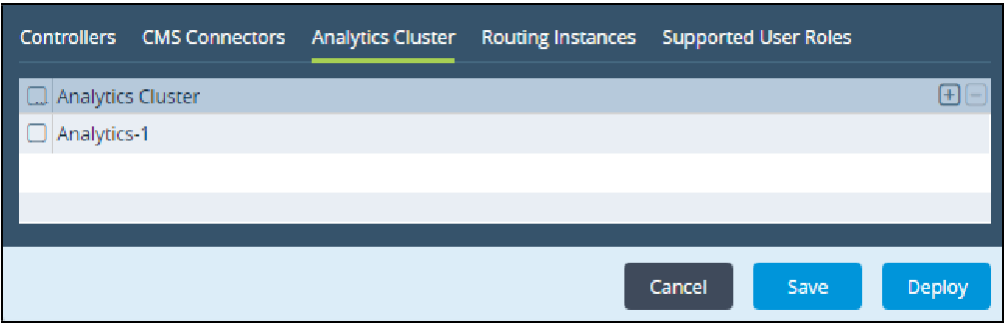
Save


Deploy

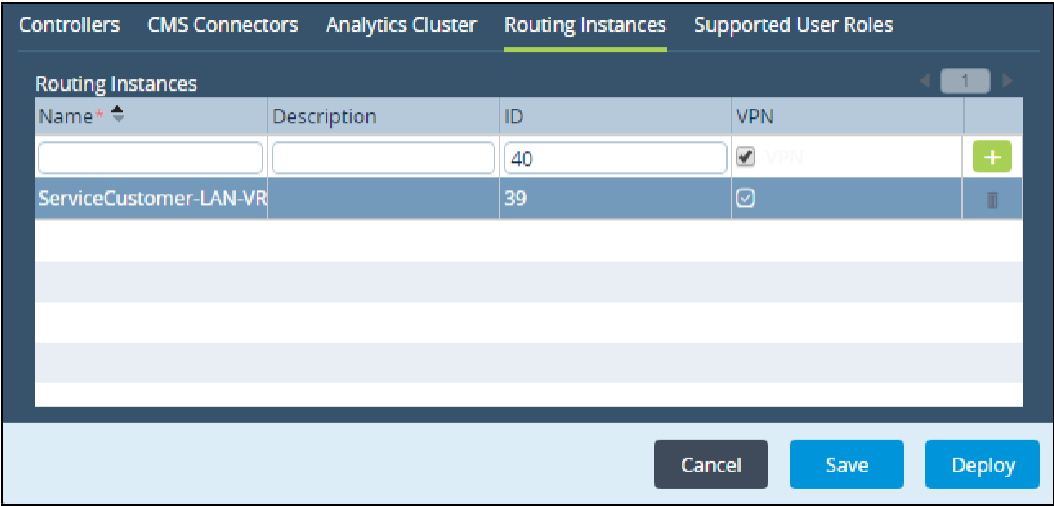
| Field | Description |
|------------------------|--|
| Name | Name of the organization. Example: <i>ServiceProvider</i> |
| Global Organization ID | ID assigned to the organization. The system populates the value automatically with the next available ID. You can change it to a different available value between 1 and 31. |
| Parent | Parent organization of the organization created. |
| IKE Authentication | Type of authentication: <i>PSK</i> (Pre Shared Key) |
| SCP | Shared Control Panel Enable or disable sharing of control or management panels with the parent or predecessor organization. This implies that the organization does not have its own control-VR routing instance and IPSec tunnels to controllers. The organization would be sharing the routing instance and IPSec tunnels of the parent or predecessor organization. Branches deployed with a single organization cannot have a shared control plane as there is no predecessor organization to provide control plane. |

- a. In **Controllers**, select the controller that you want to associate with the organization.
- b. Click **CMS Connectors** and select and add the available CMS organizations for this organization.

- c. Click **Analytics Cluster**.



- i. Click the  Add icon to add a cluster.
 - ii. Select a cluster from the list of available clusters.
- d. Click **Routing Instances** to define virtual routing instances for the organization.



| Field | Description |
|-------------|---------------------------------|
| Name | Routing instance name. |
| Description | Information about the instance. |
| ID | Routing instance ID. |
| VPN | Enable or disable VPN. |

- i. Click the  Add icon.
- e. Click **Supported User Roles**.

i. From the list of available roles, select the role(s) supported in the organization.

3. Click **Save**.

4. Click **Deploy** to onboard the organization.

This associates an organization with the selected controller(s).

| Name | Global Organization ID | Status | Last Modified Time | Last Modified By |
|---|------------------------|----------|-------------------------|------------------|
| <input type="checkbox"/> ServiceCustomer | 1 | Failed | Fri, Mar 24 2017, 11:37 | Administrator |
| <input type="checkbox"/> ServiceCustomer1 | 12 | Deployed | Wed, Mar 22 2017, 10:56 | Administrator |
| <input type="checkbox"/> ServiceCustomer2 | 13 | Deployed | Thu, Dec 22 2016, 01:09 | Administrator |
| <input type="checkbox"/> ServiceCustomer3 | 14 | Saved | Fri, Jan 06 2017, 08:40 | Administrator |

To further build the organization configuration, refer to [Adding organizations](#)

You can modify the configuration of an organization. During modification, you can deselect associated controllers or associate new controllers. After making the changes, you need to redeploy the organization.

1.2.3 Deleting or decommissioning organizations

To delete or decommission an organization, select the check box and click the  Delete icon.

Deleting or decommissioning an organization does the following:

- Disassociates the organization from all the appliances
- Deletes the hardware inventory and device groups associated with the organization
- Deletes all the templates associated with the organization

1.3 Creating FlexVNF users

SteelConnect EX FlexVNF supports the following users:

- System users
- Organization users
- Default users

1.3.1 System user attributes

- A system user can log in to SteelConnect EX FlexVNF host OS and CLI.
- A system user is created in Linux when the user is configured.
- Can assume the role of an administrator or operator. As an administrator, a system user can modify any part of configuration, while as an operator, the system user can only view the configuration.
- The allowed login is shell or CLI. If shell is selected, the system user lands on Bash mode. When CLI is selected, the user lands on the CLI prompt.
- Can SSH to port 22 and port 2024. When port 2024 is passed to SSH, the user always lands on CLI, irrespective of the login configured. System users can launch a shell from CLI.
- SteelConnect EX FlexVNF supports password-less authentication for system users using the SSH public key. This enhances security, protecting the system against the brute force password attacks of SSH.
- Can configure multiple SSH keys.

```
root@gothamcli(config)% set system users john password john123 login shell role admin
root@gothamcli(config)% show | compare
system {
    users john {
        password $1$GYdCkdSz$yiukA.B95.M8vbF3j1lpp0;
        sshpublickey laptop {
            "sshrsa
AAAAB3NzaC1yc2EAAAADAQABAAQCYhCqGWaZmpji
xaKVqjK2Ij4QUaJuiA1T+pSTveaJxrNSiCWzfKibY+
y/QV0a3+0Y4SQ5W9gkyMbL6Mrklafqnznp5y20gMIbt
ul58aJ/Q09Ygu2qg4ULb7iUgHBzwunk2hViKez06yMD
jbsE3JGvk5chffSbWXWrkObgwcHkn6KPLiYSW0cEbVS
Qa1bbF7GSJhIX6QWR17IWjp7MiD569aYxf6rI/WdjSI
St01p7mm01Y93sXnYn7hLs+8mmgV7aF18ZLtMy6x6of
b7yoyov/UQZA9L7+Wy0YtHJ+BF5oM1reG7FwxBHdwbq
p/ZqKF3R9kisxDAEWbsQBcVTSYl mmehra@quake";
        }
        login shell;
        role admin;
    }
}
```

1.3.2 Organization user attributes

An organization user can only log in to SteelConnect EX FlexVNF CLI. SteelConnect EX FlexVNF provides various predefined RBAC (Role- based access control) roles. An organization user can be assigned the following roles:

| Role | Description |
|---------------|---|
| adcadmin | Can view/modify the ADC configuration. |
| cgnatadmin | Can view/modify the CGNAT configuration. |
| sdwanadmin | Can view/modify the SD-WAN configuration. |
| securityadmin | Can view/modify the security configuration. |
| tenantadmin | Can view/modify the tenant configuration. |
| oper | Can only view the tenant configuration. |

- An organization user can log into only CLI.
- Can SSH to only port 2024. Port 22 is disallowed.
- Cannot launch “shell” from the CLI.
- Password-less authentication is currently not supported.
- While creating an organization user, @Org is appended to the user name, to create unique user names. For instance, in the following example, the user name would be john@kayak. Here, the user can SSH as:

```
ssh 'john@kayak'@77.1.1.1 p 2024      (or)
ssh 77.1.1.1 l john@kayak p 2024
root@gothamcli(config)% set orgs org Customer1 users john role tenantadmin
root@gothamcli(config)% show | compare
orgs {
  org Kayak {
    users john {
      password $1$atCDHNyk$aahOaHcP76UXyCKV7ymoz/i;
      role tenantadmin;
    }
  }
}
```

1.3.3 Default user attributes

- By default, SteelConnect EX FlexVNF has two system users — admin and versa. You cannot delete these users.
- The default password for these users is versa123.
- Admin is a super user with sudo privileges. Admin can SSH to the box on port 22 and port 2024.

- Versa is a console user. Versa can only log in via the physical or virtual console.
- The password for admin and versa can be modified or deleted via CLI. Password-less authentication can be set for admin via SSH public keys. For example:

```
root@gothamcli(config)% show system users
admin {
    login shell;
    role admin;
}
users versa {
    login shell;
    role admin;
}
```

[Return to Top](#)(see page 0)

2 Configuring SteelConnect EX FlexVNF appliances

- [Configuring appliances](#)(see page 17)
- [Configuring appliances using CLI](#)(see page 19)
- [Certificate management in FlexVNF via SteelConnect EX Director](#)(see page 19)
 - [Configuring certificate server](#)(see page 19)
 - [Configuring certificate request](#)(see page 22)
- [Applying configured certificates](#)(see page 24)
- [Alarm management](#)(see page 27)
- [Recent events](#)(see page 28)

You can configure appliances for different organizations. For example, you can configure the vCloud Director appliance for the service provider.

2.1 Configuring appliances

Steps

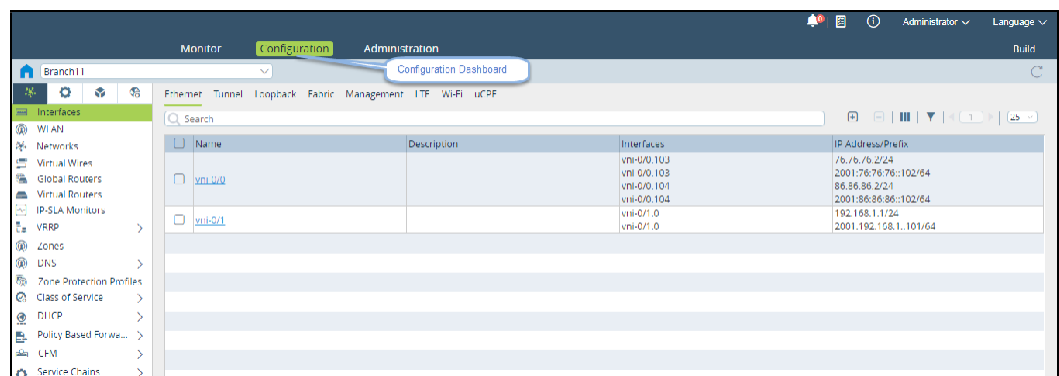
1. In the Director view, go to **Configuration > Device/s > Devices**. Select an organization in the left navigation panel and a device (branch, controller, hub) from the dashboard.
2. In the Appliance view, go to **Configuration**.

The left panel of the screen has the following tabs:

- **Networking.**

This tab is used to configure the following elements:

- **Interfaces** (Ethernet, Tunnel, Loopback, Fabric, Management). Define interfaces, their IP address, and prefix.
- **Routers** (Global, Virtual). Define global and virtual routers.
- **Virtual Wires**. Define virtual wires.
- **VRRP**. Define virtual router redundancy protocols.
- **Zones**. Define zones in the network.
- **Zone Protection Profiles**. Define profiles to protect the configured zones.
- **DHCP**. Define the DHCP protocol.
- **Policy Based Forwarding Profiles**. Define policy forwarding profiles for the network.
- **QoS**. Define the Quality of Service.



- **Services.**

This tab is used to configure services based on the subscription plan:

- **IPsec**
- **SDWAN**

The screenshot shows the 'Configuration' tab in the SteelConnect EX FlexVNF interface. The left sidebar has 'IPsec' selected. The main area displays a table with configuration details for a branch-dwan.

| VPN Profile | VPN Type | Local IP/Interface/Hostname | Peer IP/POD/Hostname | Auth Type | Local Auth Info |
|-------------------|-------------|-----------------------------|----------------------|-----------|--|
| Controller1-IPsec | branch-dwan | 10.0/24.0 | 10.12.0.1 | psk | Auth Info: id-type = email, key = 1234, id-string = Branch11@Se... |

- **Objects & Connectors.**

Objects are common network functions or service instances. Objects are created exclusively for an organization, but are reusable across network services and organizations. Objects are visible as optional, while configuring organizations, appliances, or services.

This tab is used to configure the following objects:

- **Connectors**
- **Objects**

The screenshot shows the 'Configuration' tab in the SteelConnect EX FlexVNF interface. The left sidebar has 'Objects' selected. The main area displays a table with configuration details for an object named Addressgroup1.

| Name | Members |
|---------------|---------|
| Addressgroup1 | |

- **Others.**

This tab is used to configure the following elements:


- **Organization**
- **System**
- **Elasticity**
- **Server Node Groups**
- **Syslog Server**
- **Alarms**
- **High Availability**

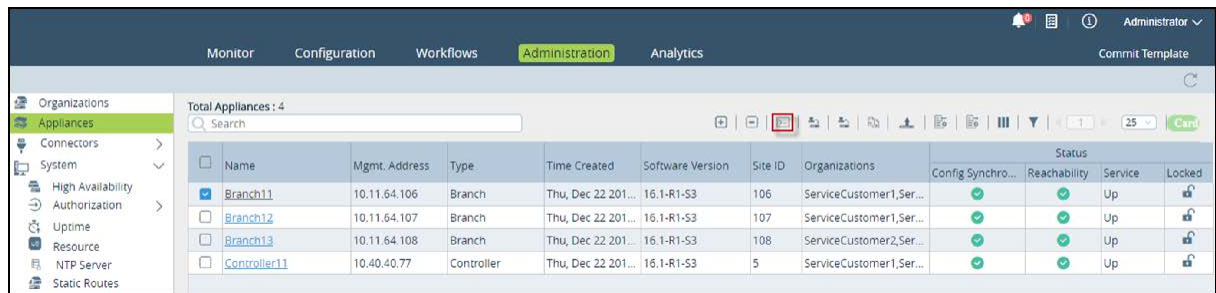
The screenshot shows the 'Configuration' tab in the SteelConnect EX FlexVNF interface. The left sidebar has 'Profiles' selected. The main area displays a table with configuration details for a profile named profile1.

| Profile Name | Max Clients | Max Servers | Max Relays | Max Rate (pps) |
|--------------|-------------|-------------|------------|----------------|
| profile1 | 8192 | 100 | 100 | |

2.2 Configuring appliances using CLI

Steps

1. Select the check box of the appliance to be configured.
2. Click the  **Appliance CLI** icon (on the top menu).



This takes you to the command line shell from where you can configure the appliances as required.

2.3 Certificate management in FlexVNF via SteelConnect EX Director

Certificates enable setting up a secure communication channel between a branch and controller. When a branch and controller need to communicate, they send a request for a certificate to the certificate authority (CA), which issues the certificates. Both the branch and the controller request the third-party CA for authentication. After the CA validates the certificate, a secure tunnel connection between a branch and controller is set up.


To configure a certificate, you need to configure the server that hosts the certificate. The branch or controller that requires a certificate sends a certificate request to the server. So, configuring a certificate comprises the following two tasks:

1. [Configuring certificate server](#)(see page 19)
2. [Configuring certificate request](#)(see page 22)

2.3.1 Configuring certificate server

You must configure the server details for the certificate authority (CA).

Steps

1. In the Director view, go to **Configuration > Devices > Devices**. Select an organization in the left navigation panel and a device from the dashboard.
2. In the Appliance view, go to **Configuration > Objects & Connectors > Connectors > Certificate Manager**.
3. On the **Servers** tab, click the  Add icon to configure a server.

Add Server

Name *

Description

Tags

Server Type *

CA Identity

URL

Routing Instance

Interface Name

Retry Interval

☐ Default CSR

OCSP

Responder Url

☐ Sign Request

☐ Verify Signature

Hash Algorithm

Response Cache Period

Monitor Interval

OK

Cancel

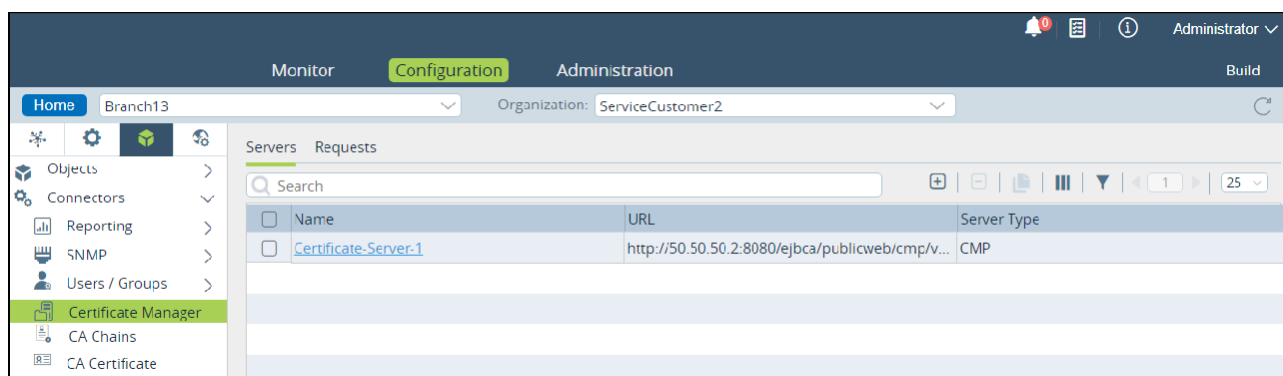
| Field | Description |
|------------------|---|
| Name | Name of the server. |
| Description | Description of the server. |
| Tags | Tags to identify the server. |
| Server Type | Type of the server. Example: <i>CMP</i> |
| CA Identity | Name of the certificate authority. |
| URL | URL of the server hosting the certificate authority. |
| Routing Instance | Routing instance used by the branch or controller to communicate with the server. This is not mandatory if you specify the interface as eth0. |
| Interface Name | Interface used for communication with the server. |
| Monitor Interval | Monitoring interval (in seconds). This is the interval at which a branch or a controller can retry to get the certificate. |



| Field | Description |
|-----------------------|--|
| Default CSR | This is the option to use the device serial number as the common name in the CSR. When selected, additional certificate signing request configuration is not required. |
| Responder URL | OCSP responder's URL. The OCSP responder reports the status of a certificate. |
| Sign Request | Enable to sign the OCSP request. The OCSP responder verifies the signature before responding. |
| Verify Signature | Enable this to verify the OCSP response signature. FlexVNF verifies the signature of OCSP responder. |
| Hash Algorithm | Algorithm to be used in preparing the OCSP request. |
| Response Cache Period | Time period to cache an OCSP response. |
| Monitor Interval | Monitoring interval (in seconds) |

OCSP is supported in the version 16.1R1 and higher.

4. Click **OK**.

This configures the server hosting the CA.




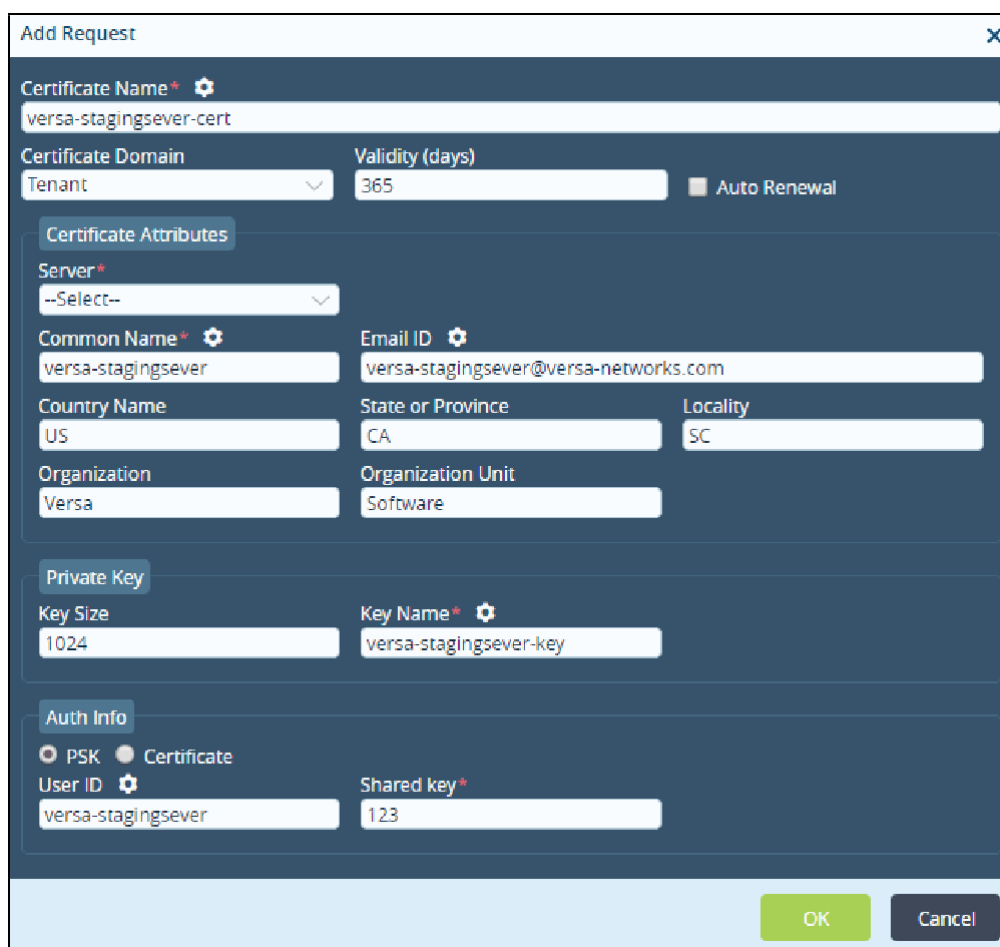
- To delete an existing server, select the check box corresponding to the server and click the  Delete icon on the top right corner.
- To filter the configuration screen table information, click  on the top right corner.

Next, configure the request sent by a branch or controller to the certificate authority.


2.3.2 Configuring certificate request

Steps

1. In the Director view, go to **Configuration > Devices > Devices**. Select an organization in the left navigation panel and a device from the dashboard.
2. In the Appliance view, go to **Configuration > Objects & Connectors > Connectors > Certificate Manager**. Click the **Requests** tab.
3. Click the  Add icon to configure a request for the certificate.





Add Request

Certificate Name * 
versa-stagingsever-cert

Certificate Domain: Tenant Validity (days): 365 ☐ Auto Renewal

Certificate Attributes


Server *

Common Name * : versa-stagingsever Email ID : versa-stagingsever@versa-networks.com

Country Name: US State or Province: CA Locality: SC



Organization: Versa Organization Unit: Software

Private Key

Key Size: 1024 Key Name * : versa-stagingsever-key

Auth Info

☒ PSK ☐ Certificate

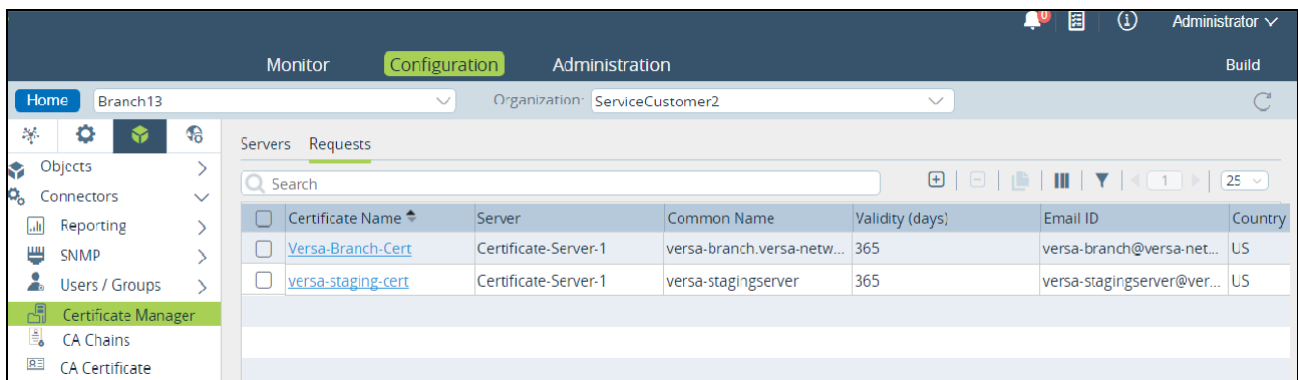
User ID : versa-stagingsever Shared key * : 123

| Field | Description |
|--------------------|---|
| Certificate Name | Name of the branch certificate. |
| Certificate Domain | Domain of the certificate. |
| Validity | Number of days for which this certificate is valid. |
| Auto Renewal | Enable or disable the renewal of the certificate. |
| Server | Name of the server. |

| Field | Description |
|--|---|
| Common Name | Name of the certificate. This is also an identity, which needs to be configured in the Certificate Authority server as well. Both the names should match. Only then does the CA server issue the certificate. |
| Email ID | Email ID of the user who wants to download the certificate. The email ID must be registered in the CA server. |
| Country Name | Name of the country from where the FlexVNF is operated from. |
| State or Province | State or province from where the FlexVNF is operated from. |
| Locality | Locality from where the FlexVNF is operated. |
| Organization | Name of the organization. |
| Key Size | Size of the key. The standard size is 1024 MB. |
| Key Name | Name in which the key is generated. |
| PSK Certificate | Mode to authenticate the certificate request: <ul style="list-style-type: none"> • <i>PSK(PreSharedKey)</i> • <i>Certificate</i> |
| User ID Shared Key | Applicable when <i>PSK</i> is the authentication mode. <ul style="list-style-type: none"> • <i>UserID</i> • <i>SharedKey</i>. Password should be identical to the shared key of the server. |
| <ul style="list-style-type: none"> • Certificate Name • CA Chain • Certificate Domain | Applicable when <i>Certificate</i> is the authentication mode. <ul style="list-style-type: none"> • <i>CertificateName</i>. Name of the certificate. • <i>CACchain</i>. Name of the certificate chain. • <i>CertificateDomain</i>. |

4. Click **OK**.

This configures a certificate.



2.4 Applying configured certificates

After configuring a certificate, you must apply the certificate to use it. For the same, associate the certificate with a VPN profile.

Steps

1. In the Director view, go to **Configuration > Devices > Devices**. Select an organization in the left navigation panel and a device from the dashboard.
2. In the Appliance view, go to **Configuration > Services > IPsec > VPN Profiles**.
3. Click the **+** Add icon to create a VPN profile. In the **General** tab, select the required **VPN Type** and enter the related information.

The 'Add IPsec VPN' dialog box is shown with the 'General' tab selected. The fields are as follows:

- VPN Profile Name***: Control11-Profile
- General** | Address Pool
- VPN Type***: Branch SDWAN
- Tunnel Initiate**: Automatic
- Peer FQDN**: --Select--
- Peer IP**: ☐ Peer IP, ☐ 10.13.0.5
- Peer Hostname**:
- Hardware Accelerator**: Any
- Routing Instance***: ServiceCustomer2-Control-VR
- Branch SDWAN Profile**: --Select--
- Local IP**:
- Local Interface**: tvl-0/26.0
- Route Based** | **Policy Based**
- Tunnel Routing Instance**: ServiceCustomer2-Control-VR
- Tunnel Interface***: tvl-0/26.0

Buttons: OK, Cancel

| Field | Description |
|---|---|
| VPN Profile Name | Name of the VPN profile. |
| VPN Type | Type of VPN. |
| Tunnel Initiate | Mode to initiate the child SA creation. For rule-based VPN, a tunnel can be initiated only when traffic is seen for that rule. <ul style="list-style-type: none"> • <i>Traffic</i> • <i>Automatic</i> |
| <ul style="list-style-type: none"> • Peer FQDN • Peer IP • Peer Hostname | Type of identification to be used for the peer identity. |
| Routing Instance | Routing instance to be used. |
| Branch SDWAN Profile | Type of branch profile. |
| <ul style="list-style-type: none"> • Local IP • Local Interface • Hostname | Local IP address or local interface or name of the host server to be used. |
| Route Based | Refers to a VPN type where traffic is tunneled by doing a route lookup where a route points to a tunnel interface. SA is associated with this interface. |
| Tunnel Routing Instance | Tunnel routing instance to be used. |
| Tunnel Interface | Tunnel interface to be used. |
| Policy Based | VPN type where traffic is tunneled based on rules or policies negotiated with a peer. SA is created as per the rule or policy. |

- Under the **IKE** tab, enter the required information.

Add IPsec VPN

General | **IKE** | IPsec

Version: --Select-- Transform: --Select-- DH Group: Diffie-Hellman Group 2 - 1024-1

Rekey Time: Hours 8 DPD Timeout: 10 Auth Domain:

Local Auth

Authentication Type*: psk Shared Key*: 1234

Identity Type*: Email Identity*: Branch13@ServiceCustomer2.co

Peer Auth

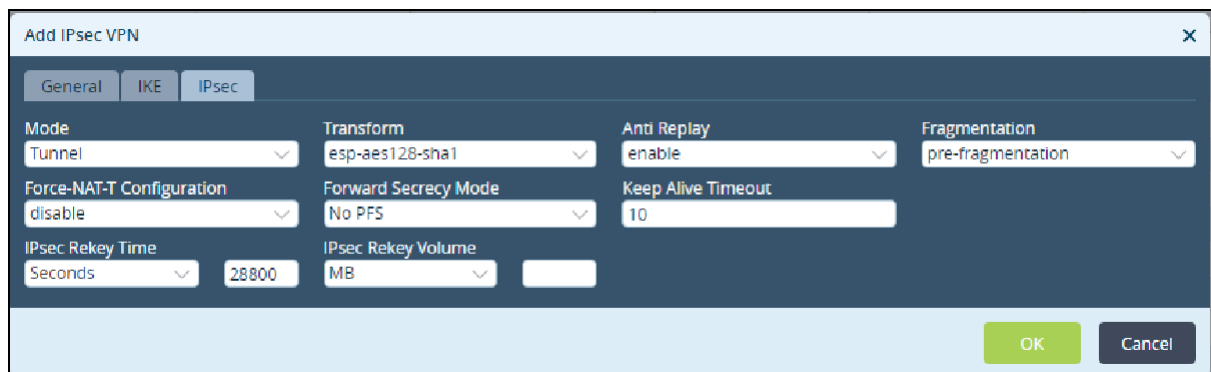
Authentication Type*: psk Shared Key*: 1234

Identity Type*: Email Identity*: Controller11@ServiceCustomer2.

OK Cancel

| Field | Description |
|---------------------|--|
| Rekey Time | Time duration in which another key is generated. |
| Local Auth | |
| Authentication Type | Mode of authentication: <ul style="list-style-type: none"> • <i>PSK</i>(Pre Shared Key) • <i>Certificate</i> |
| Shared Key | Key for access. (Applicable when <i>PSK</i> is selected) |
| Identity Type | Type of identity proof to be given: <ul style="list-style-type: none"> • <i>Email</i> • <i>FQDN</i> (Applicable when <i>PSK</i> is selected) |
| Identity | Email ID. (Applicable when Identity Type is <i>Email</i>) |

5. In the **IPsec** tab, enter the required information. Refer to [Configuring IPsec profiles](#) in the *SteelConnect EX SD-WAN Configuration Guide*.



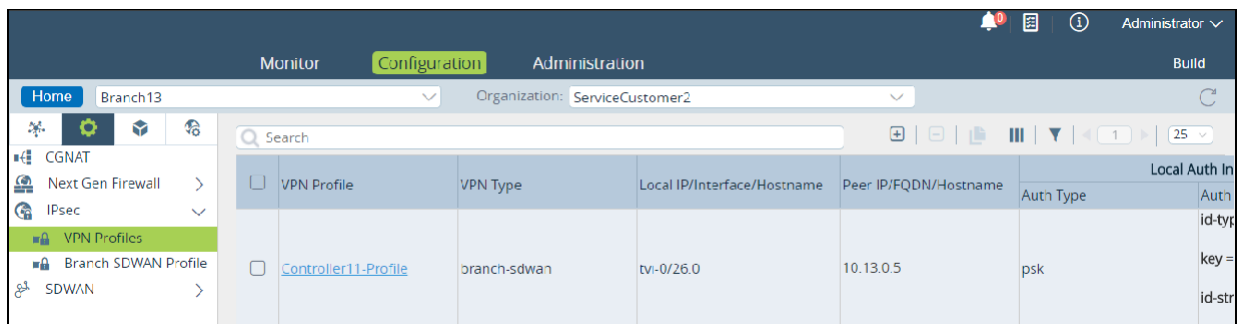
The 'Add IPsec VPN' window has three tabs: General, IKE, and IPsec. The IPsec tab is active, showing the following settings:

- Mode:** Tunnel
- Transform:** esp-aes128-sha1
- Anti Replay:** enable
- Fragmentation:** pre-fragmentation
- Force-NAT-T Configuration:** disable
- Forward Secrecy Mode:** No PFS
- Keep Alive Timeout:** 10
- IPsec Rekey Time:** Seconds, 28800
- IPsec Rekey Volume:** MB, [empty]

Buttons: OK, Cancel

6. Click **OK**.

This completes applying the certificate information for the VPN.



The Configuration page shows the VPN Profiles table. The left sidebar has a tree view with 'VPN Profiles' selected. The top navigation bar includes Monitor, Configuration, and Administration. The top right shows the user as Administrator.

| VPN Profile | VPN Type | Local IP/Interface/Hostname | Peer IP/FQDN/Hostname | Auth Type | Local Auth In |
|---|--------------|-----------------------------|-----------------------|-----------|---------------------------|
| <input type="checkbox"/> Controller11-Profile | branch-sdwan | tv-0/26.0 | 10.13.0.5 | psk | id-type key= id-str |

2.5 Alarm management

Providers can monitor organizations, child organizations, appliances, and devices using the Monitor module, which provides a top down view all the events and alarms generated by SteelConnect EX FlexVNF. Administrators can create events and assign a status to each event.

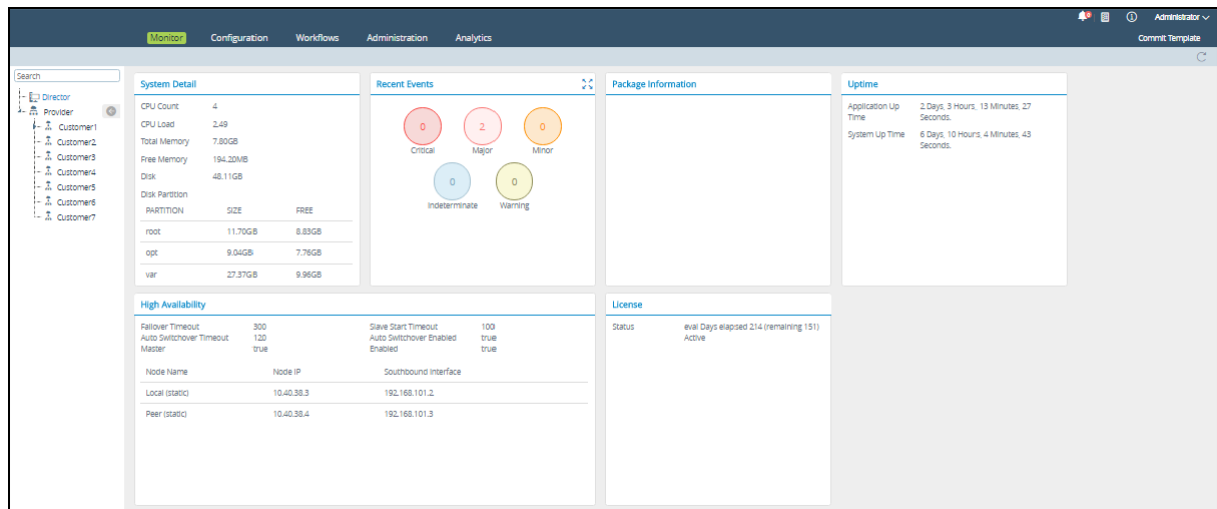
Steps

1. In the Director view, go to **Monitor**.

This screen displays the following:

- **System Detail**
- **Recent Events**
- **Package Information**
- **Uptime**
- **High Availability**
- **License**

2. Click on the provider organization in the left panel to view its monitor dashboard.

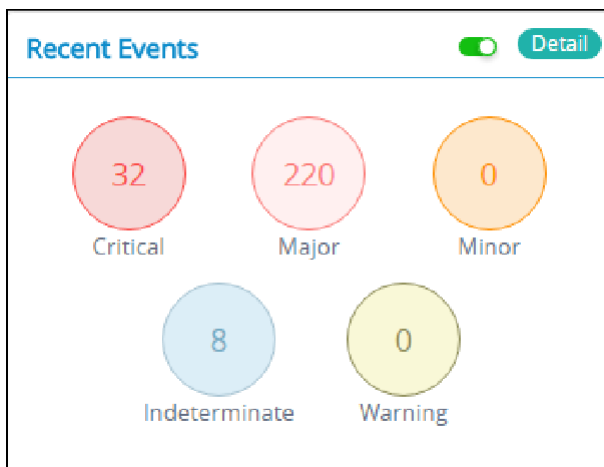


The screen displays the following sections:

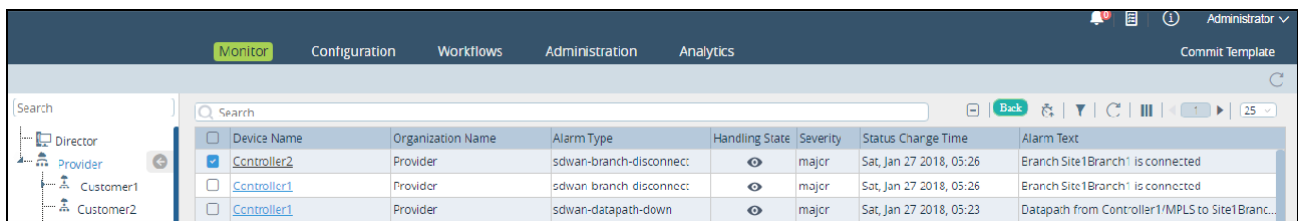
- **Asset Inventory.** Number of tenants, directors, SDWAN controllers, vCPEs.
- **Recent Events.** Number of events of different categories (critical, major, minor, indeterminate, warnings)
- **Firmware Summary.** Number of CPUs, system version, etc.
- **Provider Health.** Health of the different elements such interfaces, services, etc.
- **Application Activity.** Top applications installed on the system.
- **Services.** Number of services running (SD-WAN, CGNAT, etc.)

2.6 Recent events

Go to **Monitor > Provider Organization > Recent Events**. This tile provides a summary of all the alarms of customer organizations and system alarms with respect to the associated devices. Alarms include multiple levels—critical, major, minor, indeterminate, and warning. All event alarms can be drilled down to view the alarm details for each category.



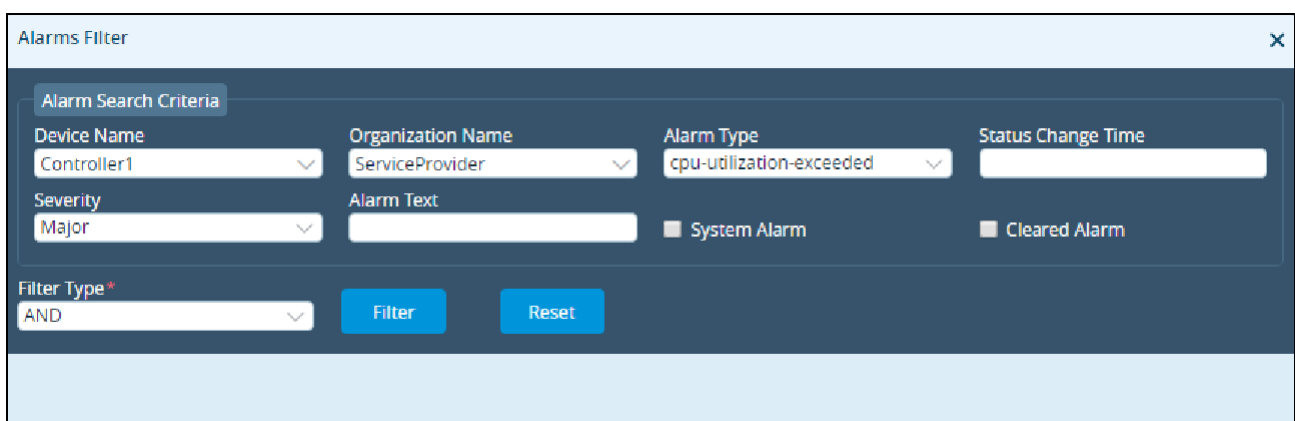
Click the **Detail** button on **Recent Events** to view the information of all the alarms in relation to the associated devices.



| Device Name | Organization Name | Alarm Type | Handling State | Severity | Status Change Time | Alarm Text |
|---|-------------------|-------------------------|----------------|----------|-------------------------|--|
| <input checked="" type="checkbox"/> Controller2 | Provider | sdwan-branch-disconnect | | major | Sat, Jan 27 2018, 05:26 | Branch Site1Branch1 is connected |
| <input type="checkbox"/> Controller1 | Provider | sdwan-branch-disconnect | | major | Sat, Jan 27 2018, 05:26 | Branch Site1Branch1 is connected |
| <input type="checkbox"/> Controller1 | Provider | sdwan-datapath-down | | major | Sat, Jan 27 2018, 05:23 | Datapath from Controller1/MPLS to Site1Branch1 is down |

Click **Back** to go back to the tile view of this screen.
 Click **Column Filter** to select the columns to be displayed.

Click **Alarms Filter** on the top right menu bar to filter the alarms.



Alarms Filter

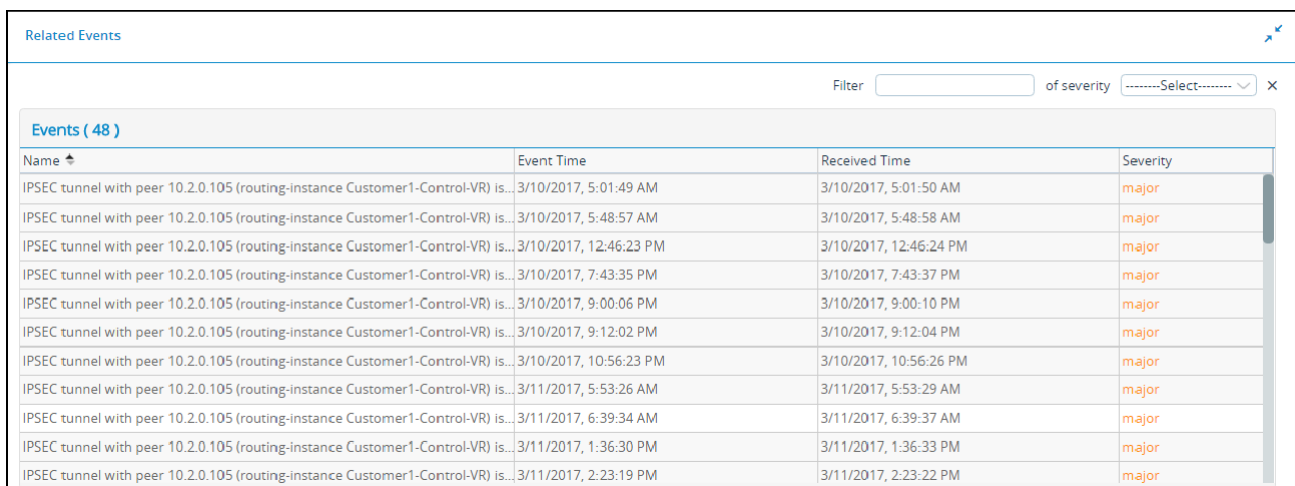
Alarm Search Criteria

Device Name: Organization Name: Alarm Type: Status Change Time:

Severity: Alarm Text: ☐ System Alarm ☐ Cleared Alarm

Filter Type*:

Click on a device to view its alarm (raised and cleared) history.



Related Events

Filter: of severity:

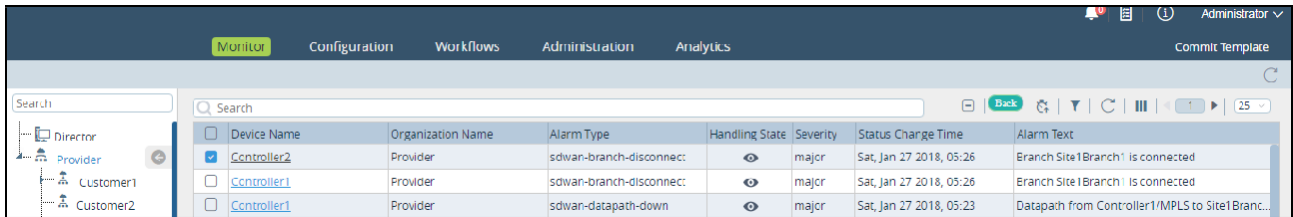
Events (48)

| Name | Event Time | Received Time | Severity |
|---|------------------------|------------------------|----------|
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 5:01:49 AM | 3/10/2017, 5:01:50 AM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 5:48:57 AM | 3/10/2017, 5:48:58 AM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 12:46:23 PM | 3/10/2017, 12:46:24 PM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 7:43:35 PM | 3/10/2017, 7:43:37 PM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 9:00:06 PM | 3/10/2017, 9:00:10 PM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 9:12:02 PM | 3/10/2017, 9:12:04 PM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/10/2017, 10:56:23 PM | 3/10/2017, 10:56:26 PM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/11/2017, 5:53:26 AM | 3/11/2017, 5:53:29 AM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/11/2017, 6:39:34 AM | 3/11/2017, 6:39:37 AM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/11/2017, 1:36:30 PM | 3/11/2017, 1:36:33 PM | major |
| IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is... | 3/11/2017, 2:23:19 PM | 3/11/2017, 2:23:22 PM | major |

You can filter events per severity level.

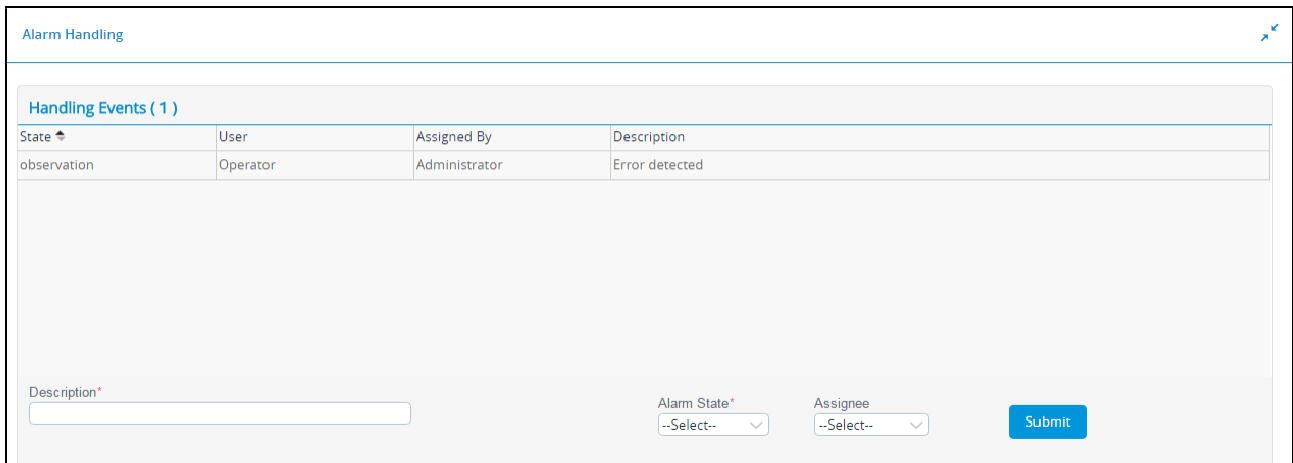
Click **Eye** in the **Handling State** column of the **Events** screen to assign tasks. Alternatively, select the check box

corresponding to a device record and click the  **Handle/Assign** icon on the top right menu bar to assign tasks.



| Device Name | Organization Name | Alarm Type | Handling State | Severity | Status Change Time | Alarm Text |
|---|-------------------|-------------------------|----------------|----------|-------------------------|--|
| <input checked="" type="checkbox"/> Controller2 | Provider | sdwan-branch-disconnect | | major | Sat, Jan 27 2018, 05:26 | Branch Site1Branch1 is connected |
| <input type="checkbox"/> Controller1 | Provider | sdwan-branch-disconnect | | major | Sat, Jan 27 2018, 05:26 | Branch Site1Branch1 is connected |
| <input type="checkbox"/> Controller1 | Provider | sdwan-datapath-down | | major | Sat, Jan 27 2018, 05:23 | Datapath from Controller1/MPLS to Site1 Branc... |

The **Alarm Handling** screen appears. The screen displays the tasks assigned by the operator or the administrator.



Alarm Handling

Handling Events (1)

| State | User | Assigned By | Description |
|-------------|----------|---------------|----------------|
| observation | Operator | Administrator | Error detected |

Description*

Alarm State* --Select--

Assignee --Select--

Submit

To enable Alarm Management in Monitor dashboard, you must configure the VNMS properties in SteelConnect EX Director. Refer to *Configuring variables in VNMS properties files* in the [SteelConnect EX Director Installation and Basic Configuration Guide](#)³.

Steps

1. Enter the event description.
2. Select the **Alarm State**. The values are:
 - *Acknowledge*
 - *Close*
 - *Investigation*
 - *None*
 - *Observation*
3. Select the **Assignee**.
4. Click **Submit**.

| Field | Description |
|-----------------------|--|
| Type | Appliance type: <ul style="list-style-type: none"> ▪ <i>Controller</i> • <i>Branch</i> • <i>Hub</i> • <i>Others</i> • <i>ServiceVNF</i> |
| Solution Tier | Network service to be configured. |
| Service Bandwidth | Allocated bandwidth for the subscribed service. |
| Primary | Identifies the selected service or solution tier as the subscribed service. |
| Analytics Enabled | Enable or disable generation of logs on SteelConnect EX Analytics. |
| Custom Parameters | |
| Name | Name of the parameter. |
| Value | Value assigned to the parameter. |
| Resource Attributes | |
| CMS Organization Name | Name of the CMS organization. |
| Availability Zone | Zone of the CMS organization. |
| Image | Image of the CMS organization. |
| Optimized For | <ul style="list-style-type: none"> ▪ Density. This mode decreases the CPU percentage of the VM since SteelConnect EX's data path process 'vsmd' polls the IO ports and goes to sleep for few microseconds. Consequently, the overall CPU percentage of the VM decreases resulting into lower data path performance. ▪ Performance. This mode increases the CPU percentage of the VM since SteelConnect EX's data path process 'vsmd' consumes heavy CPU cycles to poll the IO ports for incoming traffic. This consequently leads to high data path performance. However, the density of VMs is less. ▪ Hyper Performance. This mode increases the rate at which a data packet is processed. It optimizes the lifetime of a data packet. |

- a. Click the **Network** tab.

| Field | Description |
|---------------|--|
| Connectivity | <ul style="list-style-type: none"> ▪ Automatic. Connect the FlexVNF appliance to all the networks existing on vCloud Director. • Manually add multiple external networks to connect the appliance. |
| IP Assignment | Mode of allocating IP addresses: <ul style="list-style-type: none"> ▪ <i>POOL</i> • <i>DHCP</i> • <i>NONE</i> |

IP address pool can be added under **Administration > System > IP address pool** in the Director view.

- i. In the **Advanced** option, manually add multiple external networks to connect the appliance by selecting the **External** network entity and related **IP Assignment** method.

Add Appliance

☒ Virtual ☐ Baremetal

Name* SFWApp Organization* Pepsi Type Controller

Subscription

Solution Tier* Advanced SDWAN Service Bandwidth* 500 Mbps Aggregate Bandwidth* 500 Mbps

☒ Primary ☒ Analytics Enabled

Resource Attributes **Network** Services

Connectivity

☐ Automatic ☒ Advanced


Management Fabric Auto Create Data Fabric Auto Create

| External | IP Assignment | |
|------------|---------------|---|
| client-net | POOL | + |

NO NETWORKS ADDED

OK Cancel

| Field | Description |
|-------------------|---|
| Management Fabric | Internal network. |
| Data Fabric | External network. |
| External | Name of the external network. |
| IP Assignment | Method of IP address allocation: <ul style="list-style-type: none"> POOL DHCP NONE |

- ii. Click the  Add icon. Repeat this step to add multiple external networks.
- b. Click the **Services** tab.

Add Appliance

Virtual

Baremetal

Name*

Organization*

Type

SFWApp

Pepsi

Controller

Subscription

Solution Tier*

Service Bandwidth*

Aggregate Bandwidth*

Advanced SDWAN

500 Mbps

500 Mbps

☒ Primary

☒ Analytics Enabled

Resource Attributes

Network

Services

VCSN Flavor

DefaultVcsnFlavorTemplate


1

25

| <input type="checkbox"/> | Service Node Group | Flavor Template | VCSN Included | Services |
|--------------------------|----------------------|------------------|-------------------------------------|----------|
| <input type="checkbox"/> | Default All Services | DefaultVsnFlavor | <input checked="" type="checkbox"/> | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

OK

Cancel

- i. Click the  Add icon to add a service node group.

Add Service Node Group

Service Node Group*

Flavor Template*

Default All Services

DefaultVsnFlavor

☒ VCSN Included

☐ Services

☐ stateful-firewall

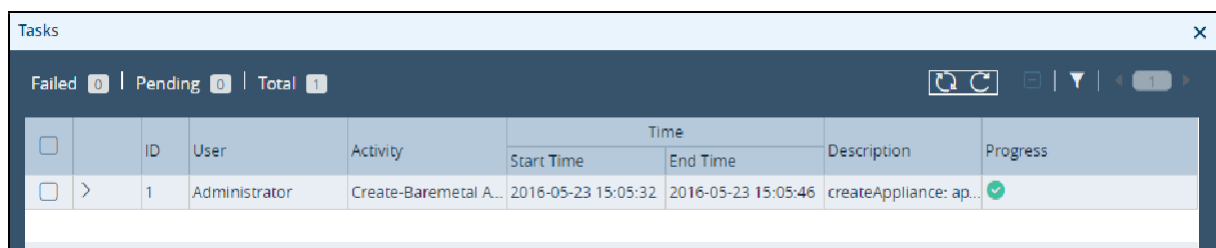
OK

Cancel

| Field | Description |
|--------------------|------------------------------|
| Service Node Group | Name of the service group. |
| Flavor Template | Name of the flavor template. |
| VCSN | Enable or disable VCSN. |
| Services | Service to be added. |


ii. Click **OK**.

2. Click **OK** on the **Add Appliance** screen to save the settings.



The screenshot shows a 'Tasks' window with a dark blue header. Below the header, there are status indicators: 'Failed 0', 'Pending 0', and 'Total 1'. To the right of these indicators are icons for refresh, expand, filter, and a page indicator showing '1'. Below this is a table with columns: ID, User, Activity, Time (subdivided into Start Time and End Time), Description, and Progress. A single task is listed with ID 1, User Administrator, Activity Create-Baremetal A..., Start Time 2016-05-23 15:05:32, End Time 2016-05-23 15:05:46, Description createAppliance: ap..., and a green checkmark in the Progress column.


| | ID | User | Activity | Time | | Description | Progress |
|--------------------------|----|---------------|-----------------------|---------------------|---------------------|------------------------|----------|
| | | | | Start Time | End Time | | |
| <input type="checkbox"/> | 1 | Administrator | Create-Baremetal A... | 2016-05-23 15:05:32 | 2016-05-23 15:05:46 | createAppliance: ap... | ✓ |

3. Click the  Tasks icon on the top right menu to view the activity details.

Appliances can be also configured using the CLI.

3.1 Creating FlexVNF appliances on OpenStack

Steps

1. In the Director view, go to **Administration > Appliances**.
2. Click the  Add icon to open the **Add Appliances** screen.

| Field | Description |
|--|---|
| <ul style="list-style-type: none"> Virtual Baremetal | Type of underlying platform. |
| Name | Name of the SteelConnect EX FlexVNF. Example: <i>SFWApp</i> |
| Organization | Name of the organization. Example: <i>Pepsi</i> |
| Type | Appliance type: <ul style="list-style-type: none"> Controller Branch Hub Others ServiceVNF |
| Solution Tier | Network service to be configured. |
| Service Bandwidth | Allocated bandwidth for the subscribed service. |
| Primary | Identifies the selected service or solution tier as the subscribed service. |
| Analytics Enabled | Enable or disable generation of logs on SteelConnect EX Analytics. |
| Custom Parameters | |
| Name | Name of the parameter. |

| Field | Description |
|-----------------------|--|
| Value | Value assigned to the parameter. |
| Resource Attributes | |
| CMS Organization Name | Name of the CMS organization. |
| Availability Zone | Zone of the CMS organization. |
| Image | Image of the CMS organization. |
| Optimized For | <ul style="list-style-type: none"> ▪ Density. This mode decreases the CPU percentage of the VM since SteelConnect EX's data path process 'vsmd' polls the IO ports and goes to sleep for few microseconds. Consequently, the overall CPU percentage of the VM decreases resulting into lower data path performance. ▪ Performance. This mode increases the CPU percentage of the VM since SteelConnect EX's data path process 'vsmd' consumes heavy CPU cycles to poll the IO ports for incoming traffic. This consequently leads to high data path performance. However, the density of VMs is less. ▪ Hyper Performance. This mode increases the rate at which a data packet is processed. It optimizes the lifetime of a data packet. |

- a. Click the **Network** tab.

The screenshot shows the 'Add Appliance' dialog box with the 'Network' tab selected. The dialog has a title bar with a close button. Below the title bar, there are two radio buttons: 'Virtual' (selected) and 'Baremetal'. The 'Name*' field contains 'SFWApp'. The 'Organization*' dropdown is set to 'Pepsi'. The 'Type' dropdown is set to 'Controller'. Below these, there is a 'Subscription' section with three dropdowns: 'Solution Tier*' set to 'Advanced SDWAN', 'Service Bandwidth*' set to '500 Mbps', and 'Aggregate Bandwidth*' set to '500 Mbps'. There are two checkboxes: 'Primary' (checked) and 'Analytics Enabled' (checked). Below this, there are three tabs: 'Resource Attributes', 'Network' (selected), and 'Services'. Under the 'Network' tab, there is a 'Connectivity' section with two radio buttons: 'Automatic' (selected) and 'Advanced'. Below that is an 'IP Assignment' dropdown set to 'POOL'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

| Field | Description |
|---------------|--|
| Connectivity | <ul style="list-style-type: none"> ▪ Automatic. connects the FlexVNF appliance to all the networks existing on vCloud Director. • Advanced |
| IP Assignment | Mode of allocating IP addresses: <ul style="list-style-type: none"> ▪ <i>POOL</i> • <i>DHCP</i> • <i>NONE</i> |


IP address pool can be added under Administration > System > IP address pool in the Director context.


- i. In the **Advanced** option, manually add multiple external networks to connect the appliance by selecting the **External** network entity and related **IP Assignment** method.

The screenshot shows the 'Add Appliance' configuration window. The 'Virtual' radio button is selected. The 'Name' field contains 'SFWApp', 'Organization' is 'Pepsi', and 'Type' is 'Controller'. Under the 'Subscription' section, 'Solution Tier' is 'Advanced SDWAN', 'Service Bandwidth' is '500 Mbps', and 'Aggregate Bandwidth' is '500 Mbps'. The 'Primary' and 'Analytics Enabled' checkboxes are checked. The 'Network' tab is active, showing 'Connectivity' set to 'Advanced'. 'Management Fabric' is 'Auto Create' and 'Data Fabric' is 'Auto Create'. Below, a table lists the selected network entity 'client-net' and the IP assignment method 'POOL'. A green '+' button is next to the table. At the bottom, it says 'NO NETWORKS ADDED'. 'OK' and 'Cancel' buttons are at the bottom right.

| Field | Description |
|-------------------|-------------------------------|
| Management Fabric | Internal network. |
| Data Fabric | External network. |
| External | Name of the external network. |

| Field | Description |
|---------------|--|
| IP Assignment | Method of IP address allocation: <ul style="list-style-type: none"> ▪ <i>POOL</i> • <i>DHCP</i> • <i>NONE</i> |

- ii. Click the  Add icon. Repeat this step to add multiple external networks.
- b. Click the **Services** tab.

- i. Click the  Add icon to add a service node group.

| Field | Description |
|--------------------|------------------------------|
| Service Node Group | Name of the service group. |
| Flavor Template | Name of the flavor template. |
| VCSN | Enable or disable VCSN. |
| Services | Service to be added. |

ii. Click **OK**.


2. Click **OK** on the **Add Appliance** screen to save the settings.

This creates an appliance on OpenStack.

3.2 Creating FlexVNF appliances on bare metal

Prior to defining a FlexVNF appliance within SteelConnect EX Director, a FlexVNF image must be installed and started on bare metal. Whether the image is running with no hypervisor, or running over KVM or VMware without a dynamic CMS connector, these appliances are considered “Bare Metal” from a SteelConnect EX Director management perspective. Contact Riverbed Support for assistance with ISO or OVA installation in bare metal scenarios.

Steps

1. In the Director view, go to **Administration > Appliances**.
2. Click the  Add icon. The Add Appliance screen displays.

Add Appliance

☒ Virtual ☐ Baremetal

Name*

VersaLV

Organization*

Provider

Type

Controller

Subscription

Solution Tier*

Advanced SDWAN

Service Bandwidth

500 Mbps

Aggregate Bandwidth*

500 Mbps

☒ Primary

☒ Analytics Enabled

Custom Parameters

| Name | Value | |
|----------|-------------|---|
| Location | NYC | + |
| Name | Controller1 | ⌵ |

Resource Attributes
Network
Services

CMS Organization Name*

SDWAN-CMS-ORG

Server

appliance1

OK
Cancel

| Field | Description |
|-------------------|--|
| Virtual Baremetal | Type of underlying platform. |
| Name | Name of the SteelConnect EX FlexVNF. Example: <i>SFWApp</i> |
| Organization | Name of the organization. Example: <i>Pepsi</i> |
| Type | Appliance type: <ul style="list-style-type: none"> ▪ <i>Controller</i> • <i>Branch</i> • <i>Hub</i> • <i>Others</i> • <i>ServiceVNF</i> |
| Solution Tier | Network service to be configured. |
| Service Bandwidth | Allocated bandwidth for the subscribed service. |
| Primary | Identifies the selected service or solution tier as the subscribed service. |
| Analytics Enabled | Enable or disable generation of logs on SteelConnect EX Analytics. |
| Custom Parameters | |
| Name | Name of the parameter. |

| Field | Description |
|-----------------------|--|
| Value | Value assigned to the parameter. |
| Resource Attributes | |
| CMS Organization Name | Name of the CMS organization. |
| Availability Zone | Zone of the CMS organization. |
| Image | Image of the CMS organization. |
| Optimized For | <ul style="list-style-type: none"> ▪ Density. This mode decreases the CPU percentage of the VM since SteelConnect EX's data path process 'vsmd' polls the IO ports and goes to sleep for few microseconds. Consequently, the overall CPU percentage of the VM decreases resulting into lower data path performance. ▪ Performance. This mode increases the CPU percentage of the VM since SteelConnect EX's data path process 'vsmd' consumes heavy CPU cycles to poll the IO ports for incoming traffic. This consequently leads to high data path performance. However, the density of VMs is less. ▪ Hyper Performance. This mode increases the rate at which a data packet is processed. It optimizes the lifetime of a data packet. |

- a. Click the **Network** tab. This displays the networks, if any, associated with the organization. The network information automatically derives from the host interfaces.

Add Appliance

Virtual ☒ Baremetal

Name* VersaLV Organization* CTS Type Controller

Subscription

Solution Tier* Advanced SDWAN Service Bandwidth* 500 Mbps Aggregate Bandwidth* 500 Mbps


☒ Primary ☒ Analytics Enabled

Resource Attributes **Network** Services

| Interface | Network | Member Of AE | Sub Unit | Subnet | IP Address | |
|-----------|---------|--------------------------|----------|---------------|------------|---|
| vni-0/0 | RIGHT | <input type="checkbox"/> | 0 | 12.12.12.0/24 | | + |
| vni-0/0 | LEFT | <input type="checkbox"/> | 0 | 11.11.11.0/24 | 107.40.2.1 | |

OK Cancel

| Field | Description |
|------------|----------------------------|
| Interface | Interface to be used. |
| Network | Network to be used. |
| Sub Unit | Sub Unit. |
| IP Address | IP address of the network. |

- Click the  Add icon. Repeat the steps to add multiple networks.
- Click the **Services** tab.

Add Appliance

Virtual

Baremetal

Name*

VersaLV

Organization*

CTS

Type

Controller

Subscription

Solution Tier*

Advanced SDWAN

Service Bandwidth*

500 Mbps

Aggregate Bandwidth*

500 Mbps

☒ Primary

☒ Analytics Enabled

Resource Attributes

Network

Services

+ | - ||| | 🔍 | ◀ 1 ▶ | 25

| <input type="checkbox"/> | Service Node Group | VCSN Included | Services |
|--------------------------|--------------------------------------|-------------------------------------|----------|
| <input type="checkbox"/> | Default All Services | <input checked="" type="checkbox"/> | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

OK

Cancel

- i. Click the Add icon to add a service node group.

| Field | Description |
|--------------------|------------------------------|
| Service Node Group | Name of the service group. |
| Flavor Template | Name of the flavor template. |
| VCSN | Enable or disable VCSN. |
| Services | Service to be added. |

ii. Click **OK**.


2. Click **OK** on the **Add Appliance** screen to save the settings.

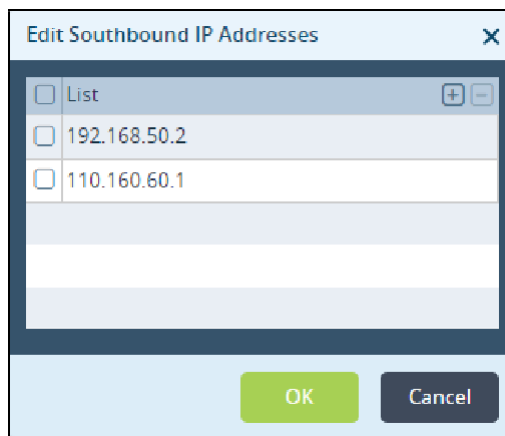
This creates an appliance on bare metal. This completes creating an appliance on OpenStack, vCloud Director, and bare metal.


3.3 Subjugating SteelConnect EX FlexVNF appliances via SteelConnect EX Director

Subjugating means controlling select FlexVNF appliances exclusively through the associated SteelConnect EX Director. Such that all network communication between appliances can happen only via SteelConnect EX Director. You might want to subjugate certain SteelConnect EX appliances in order to streamline the management of branches and network services.

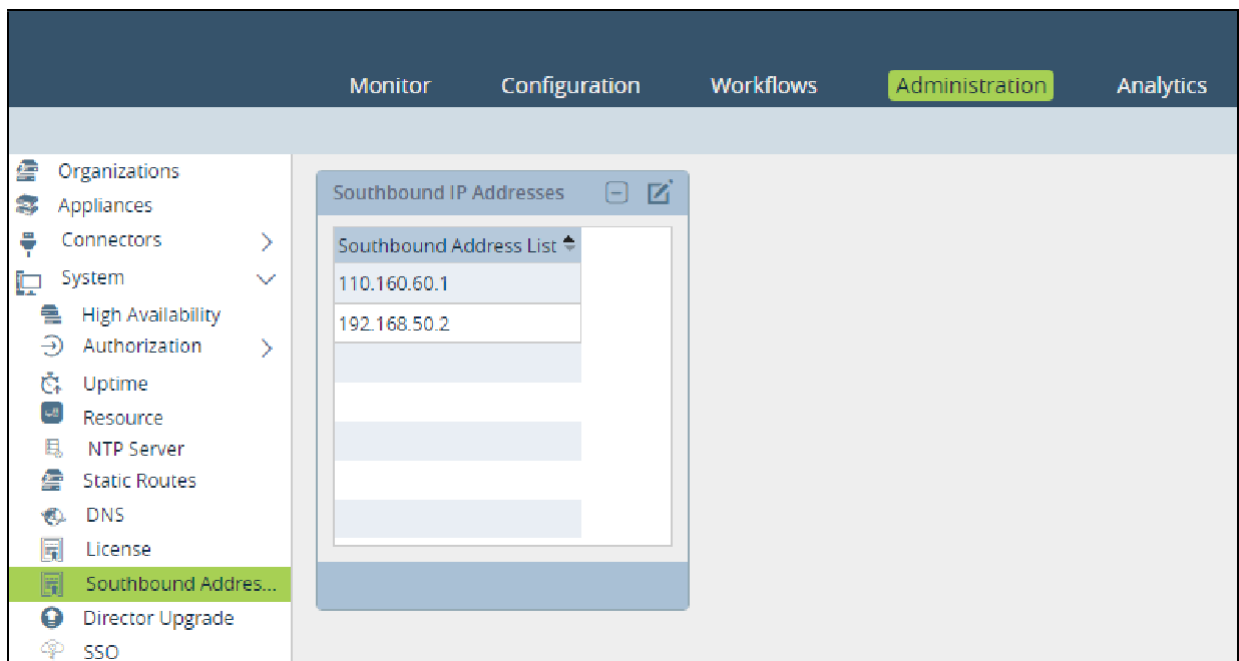
Steps

1. In the Director view, go to **Administration > System > Southbound Addresses**.
2. In the **Southbound IP Addresses** screen, click the  Edit icon to add IP addresses.



- a. Click the  Add icon to add an IP address.
- b. Click **OK**.

This enables subjugation in SteelConnect EX Director.

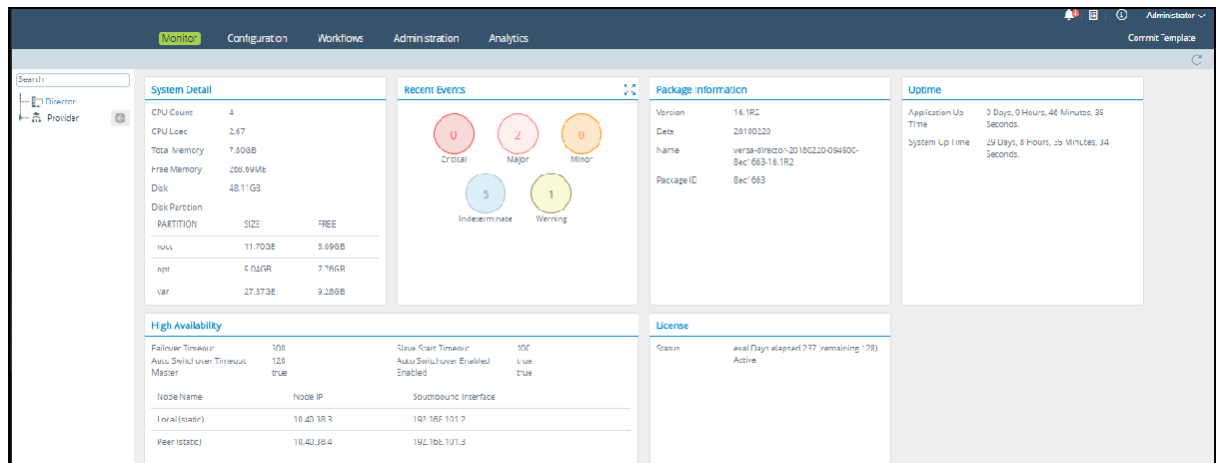


3.4 Alarm management

Providers can monitor organizations, child organizations, appliances, and devices using the Monitor module, which provides a top down view all the events and alarms generated by SteelConnect EX FlexVNF. Administrators can create events and assign a status to each event.

Steps

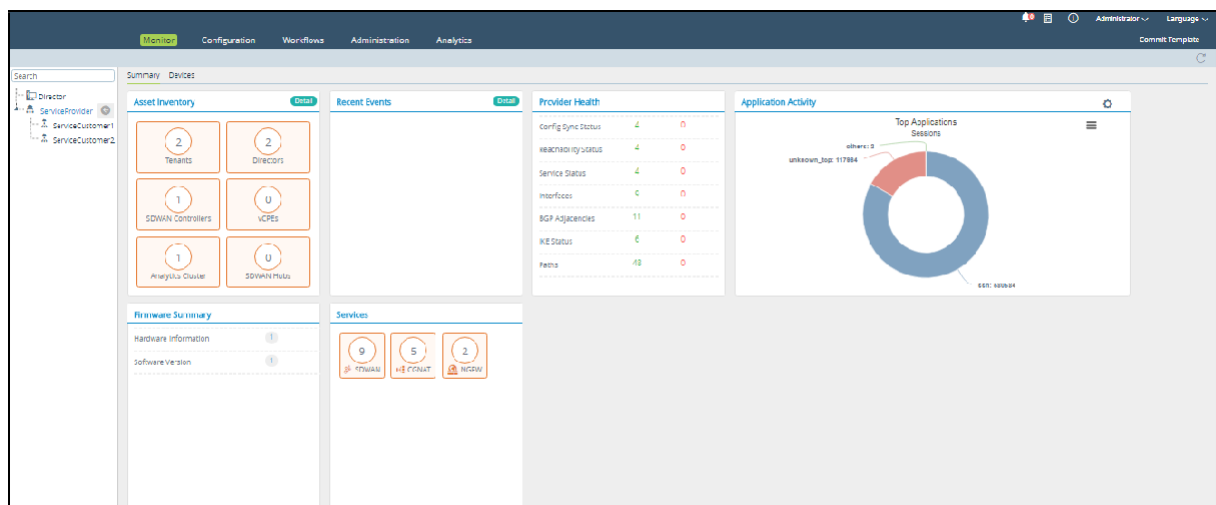
1. In the Director view, go to **Monitor**.



This screen displays the following sections at the Director level:

- **System Detail**
- **Recent Events**
- **Package Information**
- **Uptime**
- **High Availability**
- **License**

- Click on the provider organization in the left panel to view its monitor dashboard.



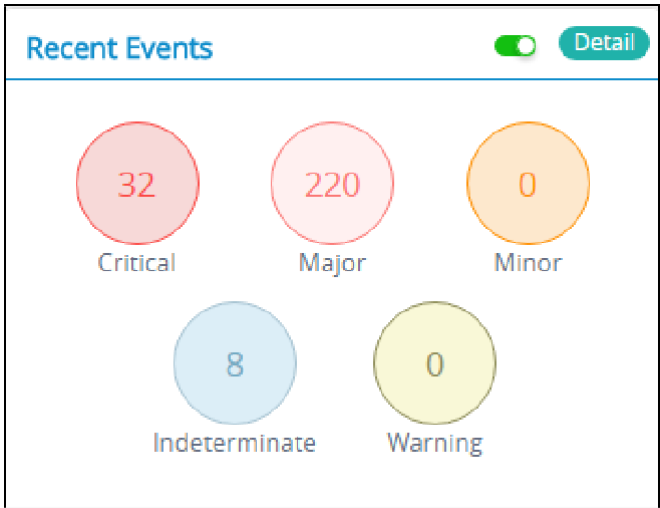
The screen displays the following sections:

- **Asset Inventory.** Number of tenants, directors, SDWAN controllers, vCPUs.
- **Recent Events.** Number of events of different categories (critical, major, minor, indeterminate, warnings)
- **Firmware Summary.** Number of CPUs, system version, etc.
- **Provider Health.** Health of the different elements such interfaces, services, etc.
- **Application Activity.** Top applications installed on the system.
- **Services.** Number of services running (SD-WAN, CGNAT, etc.)

3.5 Recent events

Go to **Monitor > Provider Organization > Recent Events**.

This tile provides a summary of all the alarms of customer organizations and system alarms with respect to the associated devices. Alarms include multiple levels—critical, major, minor, indeterminate, and warning. All event alarms can be drilled down to view the alarm details for each category.



Click **Detail** on **Recent Events** to view the information of all the alarms in relation to the associated devices.

The screenshot shows the 'Recent Events' table in the SteelConnect EX FlexVNF interface. The table has columns for Device Name, Organization Name, Alarm Type, Handling State, Severity, Status Change Time, and Alarm Text. The interface includes a navigation menu on the left, a search bar, and a toolbar with buttons like 'Back', 'Column Filter', and 'Refresh'.

| Device Name | Organization Name | Alarm Type | Handling State | Severity | Status Change Time | Alarm Text |
|---|-------------------|-------------------------|----------------|----------|-------------------------|---|
| <input checked="" type="checkbox"/> Controller2 | Provider | sdwan-branch-disconnect | | major | Sat, Jan 27 2018, 05:26 | Branch Site1Branch1 is connected |
| <input type="checkbox"/> Controller1 | Provider | sdwan-branch-disconnect | | major | Sat, Jan 27 2018, 05:26 | Branch Site1Branch1 is connected |
| <input type="checkbox"/> Controller1 | Provider | sdwan-datapath-down | | major | Sat, Jan 27 2018, 05:23 | Datapath from Controller1/MPLS to Site1Branc... |

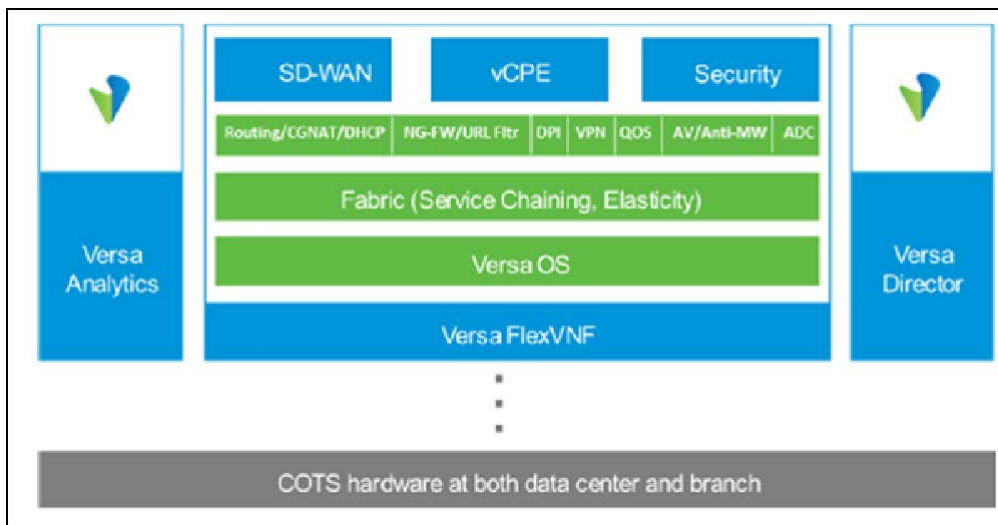
- Click the **Back** button to go back to the tile view of this screen.
- Click the **Column Filter** icon to select the columns to be displayed.

[Return to Top\(see page 0\)](#)

4 Configuring uCPE on SteelConnect EX FlexVNF

4.1 SteelConnect EX uCPE Overview

SteelConnect EX's FlexVNF supports various network services and functions, including Routing, NextGen Firewall, DPI, DDOS, IPS/IDS, Carrier Grade NAT, L4 to L7 ADC, and SD-WAN VPN services. All the services are actioned in a single pass and metadata extracted from one service (such as DPI) is passed along to other services (such as URL filtering), to provide a highly scalable service infrastructure. SteelConnect EX's FlexVNF also supports chaining the services that are running on different nodes, including 3rd party service functions.



This is how the SteelConnect EX FlexVNF uCPE functions:

- **FlexVNF** which implements various Virtual Network Functions (VNFs).
- **SteelConnect EX Director** which serves as a VNF Manager.
- **SteelConnect EX Analytics** which is a big data analytics platform providing Visibility and Control, Prediction, Correlation, Anomaly Detection, and Feedback Loop.

A single SteelConnect EX FlexVNF can contain one or more Service Virtual Machines. An individual SteelConnect EX FlexVNF supports the following modes of service chaining:

- **Vertical Service Chaining Model:** One or more service virtual machines (VM), where all service VMs are performing identical set of services.
- **Horizontal Service Chaining Model:** One or more groups of service virtual machines where each group is performing different sets of services.


Physical Networks Functions (PNFs) and VNFs from third party vendors are supported with both Horizontal Service Chaining mode and Vertical Service Chaining mode.

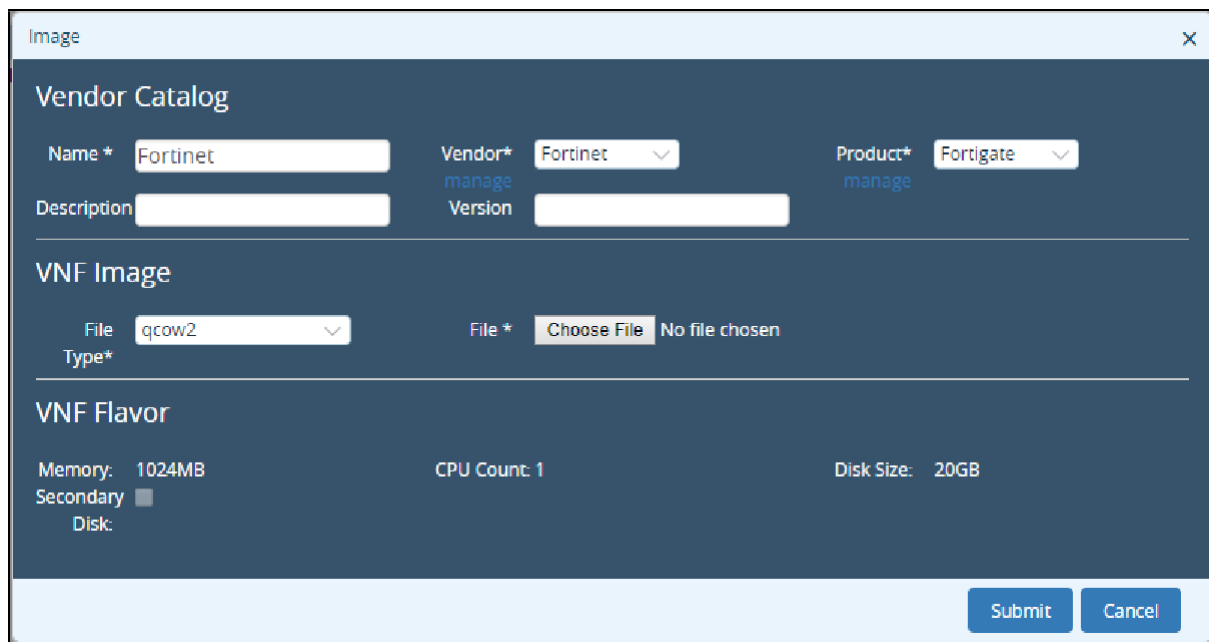
Service chain can be created which straddles multiple branches and hubs. Such a service-chain would contain one SteelConnect EX FlexVNF at each of those branches or hubs. The SteelConnect EX FlexVNF at each of the branches or hubs could be configured for horizontal or vertical modes of service chaining.

4.2 Configuring uCPE on SteelConnect EX FlexVNF

4.2.1 Creating a VendorCatalog

To create a third party VNF to the SteelConnect EX FlexVNF's vendor catalog, perform the following steps:

1. In the Director view, go to **Administration > Inventory > Vendor Catalog** and click the  Add icon to create a new vendor catalog. This opens the Image window.



| Field | Description |
|-------------|---|
| Name | Name of the new uCPE that you are adding to the SteelConnect EX FlexVNF. |
| Description | Brief description of the interface and its purpose. |
| Vendor | Vendor that is supported on SteelConnect EX FlexVNF: <ul style="list-style-type: none"> • <i>Fortinet</i> • <i>Riverbed</i> • <i>Secui</i> |
| Version | uCPE version for the selected vendor. |
| Product | Vendor's product/model. |
| File Type | VNF image file type. Currently, only qcow2 version is supported on the SteelConnect EX FlexVNF. |
| File | qcow2 file name. |

2. Click **manage** under **Vendor** to create a new vendor.

Vendor and Product

Manage Vendors

| | |
|-----------|--|
| ABC | |
| AXC | |
| SDSDS | |
| AAA | |
| AST | |
| Fortinet | |
| Riverbed | |
| Secui | |
| Palo-Alto | |
| Microsoft | |
| Linux | |
| Replify | |

Create New Vendor

Vendor Name *

3. Enter the vendor name and click **Create** to create a product for the vendor.

Vendor and Product

Manage Products

No records

Create Product for Vendor BASF

Product Name *

Details

Service Function *

VNF Flavor

Memory * (MB)

Disk Size * (GB)

Secondary Disk ☐

CPU Count *

| Field | Description |
|------------------|--|
| Product Name | Name of the product. |
| Service Function | Type of product: <ul style="list-style-type: none"> • <i>Firewall</i> • <i>NextGenFirewall</i> • <i>WANOptimizer</i> • <i>Others</i> |
| Memory (MB) | Memory capacity of the product. |
| Disk Space (GB0) | Disk space occupied by the product. |
| CPU Count | |
| Secondary Disk | Indicates whether an additional disk is required. |

- Click **OK**.
- Click **manage** under **Product** to create a product.

Vendor and Product

Manage Products

Fortigate

Create Product for Vendor Fortinet

Product Name * FortiConnect

Details

Service Function * Firewall

VNF Flavor

Memory * (MB) 50

Disk Size * (GB) 2

Secondary Disk ☐

CPU Count * 6

Create

Ok

| Field | Description |
|--------------|----------------------|
| Product Name | Name of the product. |

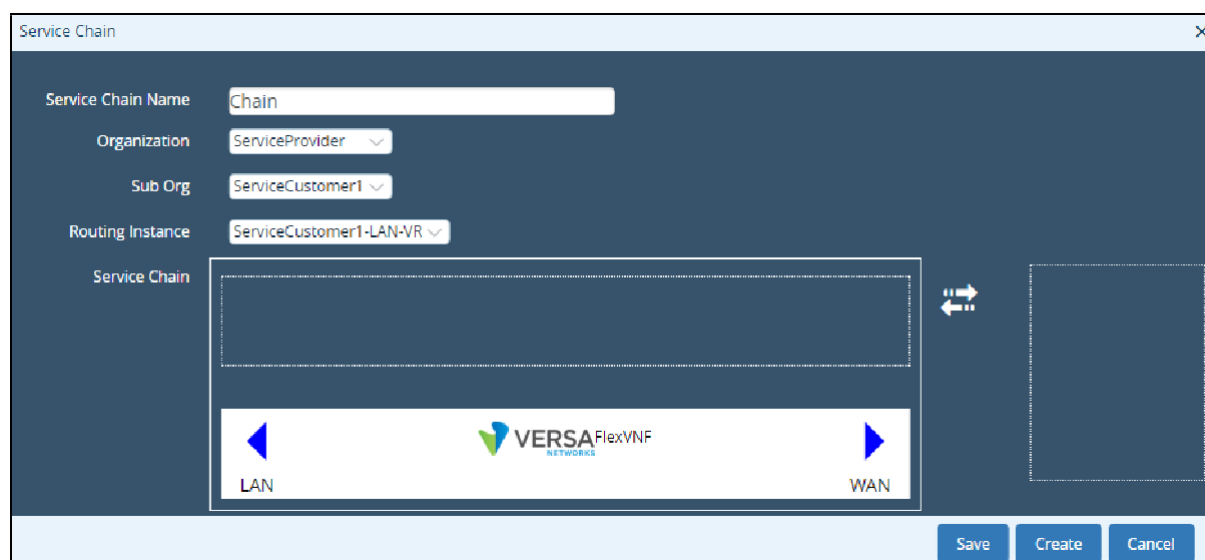
| Field | Description |
|------------------|--|
| Service Function | Type of product: <ul style="list-style-type: none"> • <i>Firewall</i> • <i>NextGenFirewall</i> • <i>WANOptimizer</i> • <i>Others</i> |
| Memory (MB) | Memory capacity of the product. |
| Disk Space (GB0) | Disk space occupied by the product. |
| CPU Count | |
| Secondary Disk | Indicates whether an additional disk is required. |

6. Click **OK**.
7. Click **Submit** to create a new vendor catalog.

4.2.2 Creating a Service Chain Template

To configure the SteelConnect EX FlexVNF service chaining, perform the following steps:

1. In the Director view, go to **Administration > Inventory > Vendor Catalog** and click the  Add icon to create a new vendor catalog. This opens the Image window.



| Field | Description |
|--------------------|---|
| Service Chain Name | Name for this service chain. |
| Organization | Organization to which this service chain belongs. |

| Field | Description |
|------------------|---|
| Routing Instance | Routing instance used for this service chain instance. |
| Service Chain | Select the VNF from the list and drag and drop it to the SteelConnect EX FlexVNF box. This chains the third-party VNF with the SteelConnect EX FlexVNF. |


- Click the uCPE service chained with the SteelConnect EX FlexVNF to modify the guest VNF's (uCPE) configuration. This opens the VNF Attributes window.

| Field | Description |
|---------------------|--|
| Memory | CPU memory limit for the select guest VNF. |
| Secondary Disk Size | Secondary disk size of the guest VNF. |
| Auxiliary Interface | Guest VNF as an auxiliary interface. |
| Service Chain | Layer on which the service chain is configured: <ul style="list-style-type: none"> • Layer2 • Layer3 |
| User Data | User data about the guest VNF for reference. |

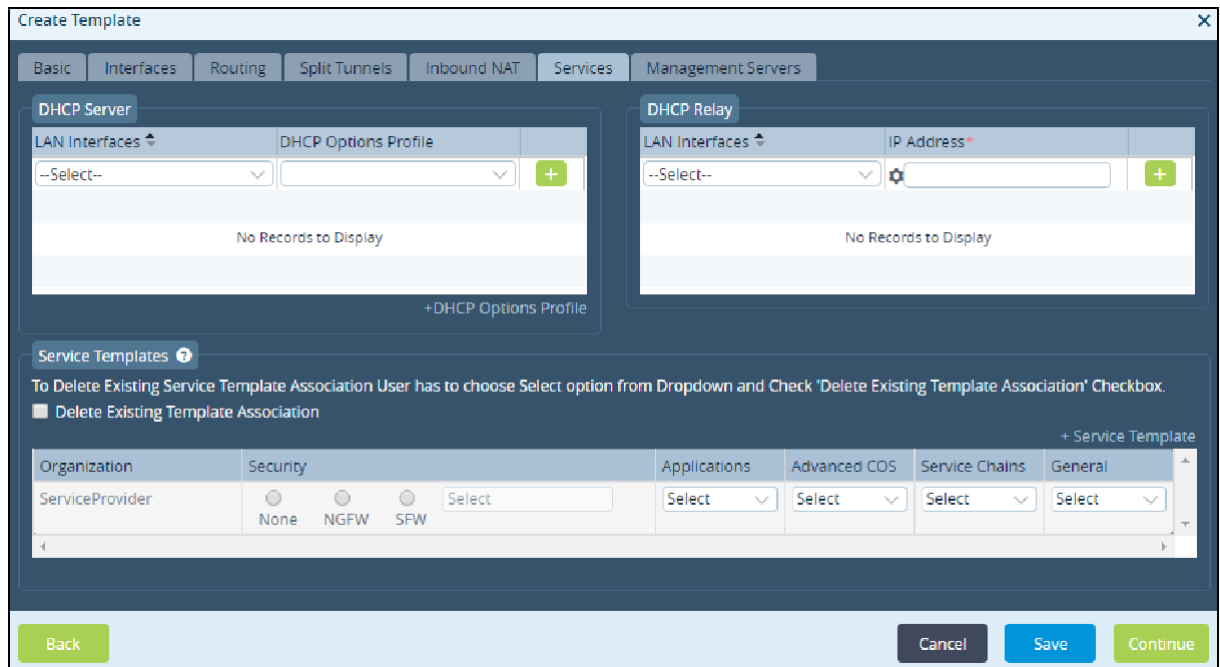
- Click **Save** to update the guest VNFs configuration.
- Click **Save & Deploy** to commit the service chaining of the 3rd party VNFs on the SteelConnect EX FlexVNF.

4.2.3 Associating Service-Chaining Template with the Device Template

To chain a network service with the SteelConnect EX FlexVNF, perform the following steps:

1. Go to **Workflows > Template > Templates** and click the  Add icon to deploy a uCPE on SteelConnect EX FlexVNF.

This opens the Create Template window.




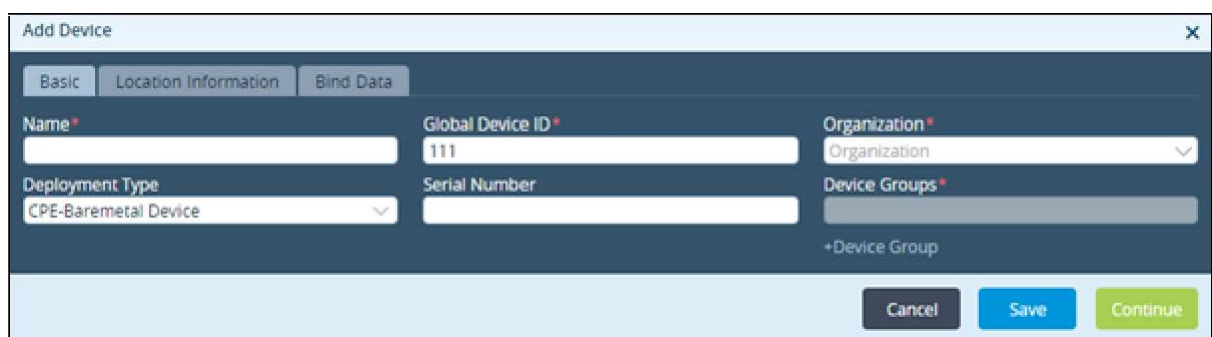
The 'Create Template' window is shown with the 'Management Servers' tab selected. It contains sections for 'DHCP Server', 'DHCP Relay', and 'Service Templates'. The 'Service Templates' section includes a table with columns for Organization, Security, Applications, Advanced COS, Service Chains, and General. The 'Security' column has radio buttons for 'None', 'NGFW', and 'SFW'. The 'Applications' column has a 'Select' dropdown. The 'Advanced COS' column has a 'Select' dropdown. The 'Service Chains' column has a 'Select' dropdown. The 'General' column has a 'Select' dropdown. At the bottom, there are 'Back', 'Cancel', 'Save', and 'Continue' buttons.

2. Enter the necessary details in the **Services** tab.
3. Click **Save** to complete the service chaining configuration.
4. Click **Continue** to create/recreate and deploy the template with the service chain template.

4.2.4 Adding Devices to the Device Template

To add devices to the device template, perform the following steps:

1. Go to **Workflows > Devices > Devices** and click the  Add icon to add a device to the device template. This opens the Add Device window.



The 'Add Device' window is shown with the 'Basic' tab selected. It contains fields for 'Name', 'Global Device ID', 'Organization', 'Deployment Type', 'Serial Number', and 'Device Groups'. The 'Deployment Type' dropdown is set to 'CPE-Baremetal Device'. The 'Global Device ID' field contains '111'. The 'Organization' dropdown is set to 'Organization'. The 'Device Groups' field is empty. At the bottom, there are 'Cancel', 'Save', and 'Continue' buttons.

- a. In **Basic**, specify a device name, associate an organization to the device, and add the device to a device group.
- b. In **Local Information**, specify your address and geographical co-ordinates.

- c. In **Bind Data**, specify the bind data.

Add Device - UCPE-1

Basic Location Information **Bind Data**

User Input Auto-Generated

Post Staging Template - uCPE-Replify-FG

| Serial | Device Name | Interfaces with Mask | | Default Gateway |
|----------------|-------------|-------------------------|--------------------------|--------------------------------|
| | | LAN_IPv4__staticaddress | MPLS_IPv4__staticaddress | MPLS-Transport-VR_IPv4__vrHopA |
| LR201703008556 | UCPE-1 | 192.168.1.1/24 | 192.168.10.1/24 | 192.168.10.2 |

Service Template Variable Template : uCPE-Replify-FG Device Group : DG-Replify-FG

Service Templates : Replify-FG

User Input Auto-Generated Clone Clear

| <input type="checkbox"/> | Serial | Device Name | DHCP | |
|--------------------------|----------------|-------------|---|---|
| | | | uCPe-MgmtIntf_Pool_Range_Begin_IP_apRa... | uCPe-MgmtIntf_Pool_Range_End_IP_apRa... |
| <input type="checkbox"/> | LR201703008556 | UCPE-1 | 172.25.1.10 | 172.25.1.100 |

{\${v_ucPE-MgmtIntf_Pool_Range_Begin_IP_apRangeB...}egin}

Validate Template

Back Cancel Save Redeploy

2. Click **Save** to onboard the device to the Device Template.

4.2.5 Onboarding the device through Zero Touch Provisioning (ZTP)

1. Bring up the device using ZTP. Refer to [URL Based Zero Touch Provisioning](#).
2. Reboot the device. After the device is up, the controller sends the post-staging notification to SteelConnect EX Director.
3. SteelConnect EX Director copies the qcow2 file to the respective device and triggers the command to start the VNF.

Before copying the file, Versa Director checks if the same qcow2 file exists in the device (in the directory `/home/versa/images`), in which case it does not overwrite the existing file.

4.2.6 Verifying the uCPE Configuration

To verify the creation of the uCPE in the SteelConnect EX FlexVNF, perform the following steps:

1. In the Director view, go to **Administration > Appliances** to view the list of appliances configured on the SteelConnect EX FlexVNF. The dashboard will now have a new entry for the uCPE added in the previous section.



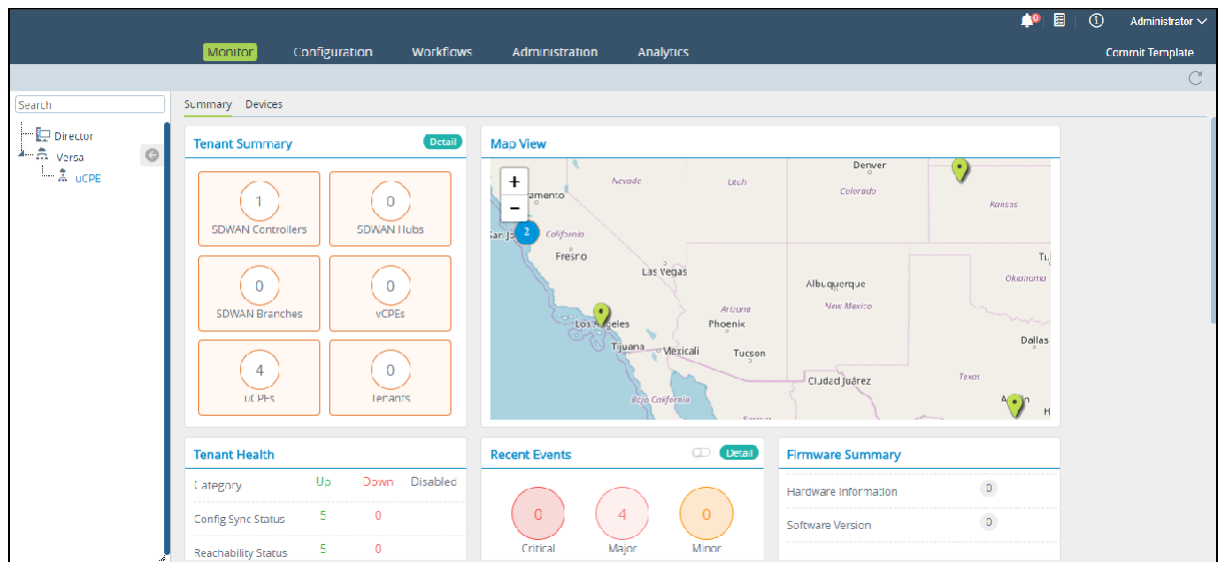
The screenshot shows the 'Administration' tab in the SteelConnect EX FlexVNF interface. The left sidebar lists various management areas, with 'Appliances' selected. The main panel displays a table of appliances with columns for Name, Mgmt. Address, Type, Service Start, Software Version, Site ID, Organizations, and Status. There are 5 total appliances listed.

| Name | Mgmt. Address | Type | Service Start | Software Version | Site ID | Organizations | Status |
|-------------|---------------|------------|------------------|------------------|---------|---------------|--------|
| Controller1 | 10.40.12.64 | Controller | Tue, Jun 19 2... | 16.1-R2-S2.3 | 1 | uCPE,Versa | Up |
| UCPE-1 | 10.1.192.101 | uCPE | Tue, Jun 19 2... | 16.1-R2-S2.3 | 101 | uCPE | Up |
| UCPE-2 | 10.1.192.102 | uCPE | Tue, Jun 19 2... | 16.1-R2-S2.3 | 102 | uCPE | Up |
| UCPE-3 | 10.1.192.103 | uCPE | Tue, Jun 19 2... | 16.1-R2-S2.3 | 103 | uCPE | Up |
| UCPE-4 | 10.1.192.104 | uCPE | Wed, Jun 27 2... | 16.1-R2-S2.3 | 104 | uCPE | Up |

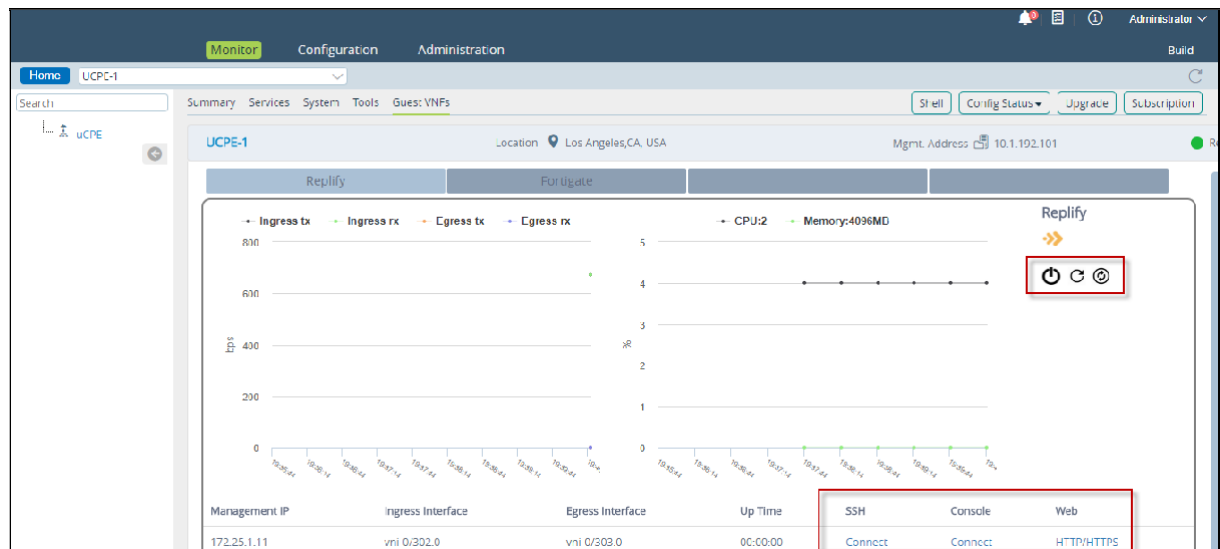
4.2.7 Monitoring uCPE

To monitor the uCPE's on the SteelConnect EX FlexVNF, perform the following steps:

1. Go to **Monitor > Org > Devices > uCPE** to view the uCPEs statistics.



2. Select the **Guest VNFs** tab in the dashboard to view the details of the onboarded uCPE.



The dashboard displays these two graphs:

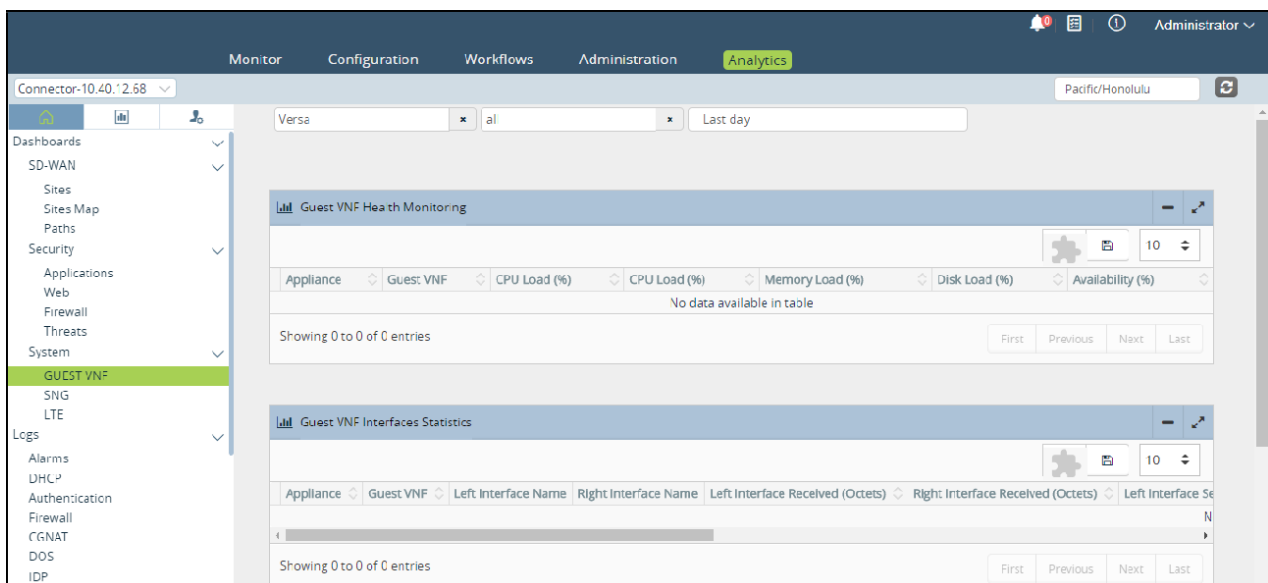
- CPU/Memory graph over a 30 second interval.
- Ingress/Egress tx/rx statistics over a 30 second interval.

3. Use this dashboard to **Shutdown**, **Reset**, and **Reboot** the uCPE.

You can also use this dashboard to connect to third party VNFs using **SSH**, **Console**, or **HTTP**.

4.3 Viewing the uCPE on SteelConnect EX Analytics

Go to **Analytics > Dashboard > System > Guest VNF** to check the various uCPEs (Guest VNF) details on the SteelConnect EX Analytics.



Installing hypervisor packages

1. Run the following CLI command to install the hypervisor packages. This creates the OVS-bridges and interfaces from vni-0/300 to vni-0/307.

```
request system hypervisor enable no-confirm
```

This will stop the service and install the hypervisor packages. This needs to be done before pushing the uCPE-service chain template. If the packages are not installed before the template push, the starting of guest-vnf will not go through and the task will fail.

2. Check the virsh version after installation.

```
sudo virsh version
```

This displays the following:

```
Compiled against library: libvirt 4.0.0
Using library: libvirt 4.0.0
Using API: QEMU 4.0.0
Running hypervisor: QEMU 2.0.0
```

3. Check the uCPE-interface creation and mapping.

```
admin@Branch-UCPE-MT-cli> show interfaces brief
```

This will show the newly created interfaces as vni-0/300 to vni-0/307.

```
admin@Branch-UCPE-MT-cli> show interfaces brief|grep UCPE
```

This displays the interface mapping of the uCPE interfaces to the OVS-Switch.

```
admin@Branch-UCPE-MT-cli>
admin@Branch-UCPE-MT-cli> show interfaces statistics | grep UCPE
vni-0/300      1      Provider-Control-VR  UCPE-MGMT1  0      0      0      0      0      0      0      0      0      0
vni-0/300.0    1      Provider-Control-VR  UCPE-MGMT1  0      0      0      0      0      0      0      0      0      0
vni-0/301      1      Provider-Control-VR  UCPE-MGMT2  0      0      0      0      0      0      0      0      0      0
vni-0/301.0    1      Provider-Control-VR  UCPE-MGMT2  0      0      0      0      0      0      0      0      0      0
vni-0/302      2      Customer2-LAN1-VR    UCPE-PORT1  0      0      0      0      0      1      0      42      0      320
vni-0/302.0    2      Customer2-LAN1-VR    UCPE-PORT1  0      0      0      0      0      1      0      42      0      320
vni-0/303      2      Customer2-LAN1-VR    UCPE-PORT2  0      0      0      0      0      1      0      42      0      320
vni-0/303.0    2      Customer2-LAN1-VR    UCPE-PORT2  0      0      0      0      0      1      0      42      0      320
vni-0/304      0      global              UCPE-PORT3  0      0      0      0      0      0      0      0      0      0
vni-0/305      0      global              UCPE-PORT4  0      0      0      0      0      0      0      0      0      0
vni-0/306      0      global              UCPE-PORT5  0      0      0      0      0      0      0      0      0      0
vni-0/307      0      global              UCPE-PORT6  0      0      0      0      0      0      0      0      0      0
vni-0/307.0    0      global              UCPE-PORT6  0      0      0      0      0      0      0      0      0      0
[ok][2018-05-09 18:53:11]
admin@Branch-UCPE-MT-cli>
```

- show guest-vnfs virtual-machines info brief/detail. This displays the status of the VNFs running in the device.

```
admin@Branch-UCPE-MT-cli>
admin@Branch-UCPE-MT-cli> show guest-vnfs virtual-machines info detail

Virtual Machine      Adtran
State                running
Uptime               1w0d03h
Creation Timestamp   2018-04-24 10:32:42.383208
Management IP        172.25.1.5
Management MAC       52:54:00:00:01:01
Number of CPUs       2
Memory               2048
VNC Port             5901
Management Interface vni-0/300.0
Auxiliary Interface  n/a
Left Interface        vni-0/302.0
Right Interface       vni-0/303.0
Primary-volume
  Disk Path           /home/versa/images/adtran.qcow2
  Disk format         qcow2
Secondary Volume
  Disk Path           n/a
  Disk format         n/a

[ok][2018-05-09 18:55:55]
admin@Branch-UCPE-MT-cli>
```

4.3.1 Troubleshooting uCPE

Versa-virtmgr failed to start.

Try to start the service individually.

```
sudo initctl start versa-virtmgr
```

Versa-virtmgr also depends on the services versa-virtlogd and versa-virtlockd. Check the status of these services in the vsh status output. If this fails to come up, start the services manually.

```
sudo service virtlogd start
sudo service virtlockdstart
```

Try starting the versa-virtmgrservice.

4.3.2 Alarms generation for uCPE

Alarms are generated for the management reachability of the VNFs running provided the health-monitor is enabled in the configuration of the virtual machines. These alarms are generated when the management interface is not reachable.

```
cli> show alarms last-n 205 | grep virtmgr
```

The following output appears:

```
virtmgr    guestVnfDown    2018-05-02T15:45:42-0 Provider: Guest VNF Adtran is down. Management
interface probe failure
virtmgr    guestVnfUp      2018-05-02T15:47:12-0 Provider: Guest VNF Adtran is up. Management interface
probe success
```

Alarms are generated for the data-path reachability between SteelConnect EX VNF and the third-party VNF. Monitoring is triggered only if bypass-on-fail is generated under the org-level service-chain-instance.

```
cli> show alarms last-n 200 | grep sfc
```

The following output appears:

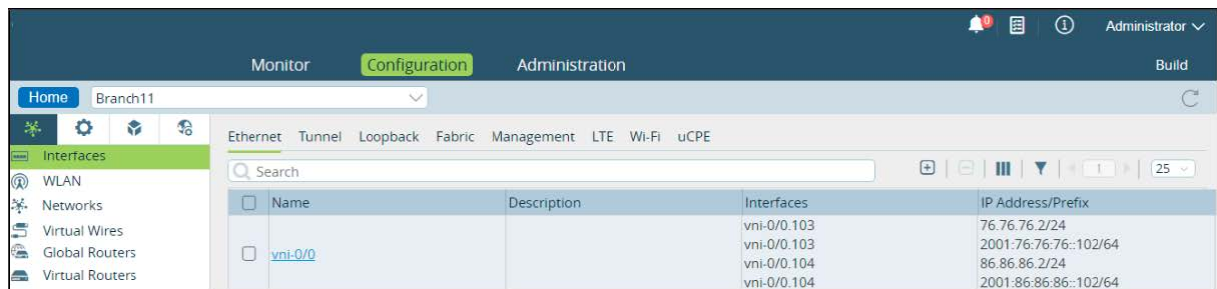
```
sfc      sngDown      2018-04-23T17:25:58-0 Customer2: Service Node Group Fortios-FromLAN-SNG is down.
Health monitor failure
sfc      sngUp        2018-04-20T15:34:31-0 Customer2: Service Node Group Fortios-FromLAN-SNG is up.
Health monitor success
```

[Return to Top](#)(see page 0)

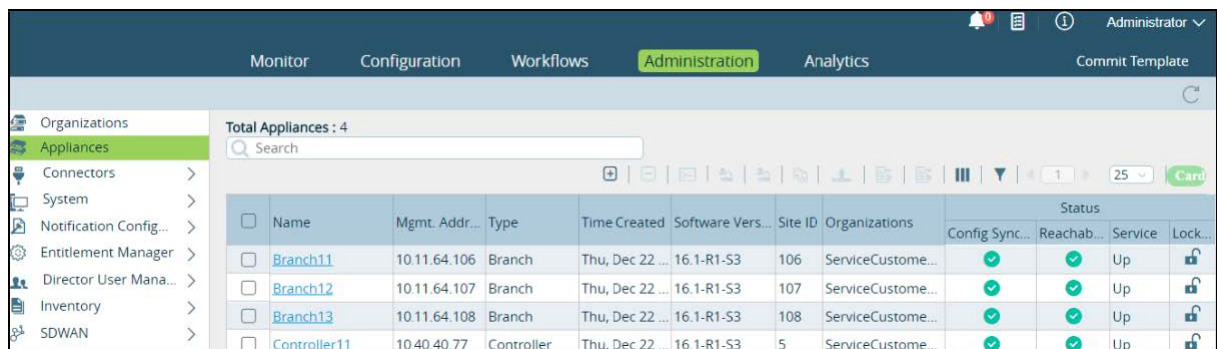
5 Verify SteelConnect EX FlexVNF Operation







To verify the operation of a FlexVNF device:


1. Log in to Director
2. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Devices > Devices in the left menu bar.
 3. Select an Organization in the left menu bar.
 4. Select a device in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Interfaces in the left menu bar. The main pane lists all FlexVNF devices. Select a tab in the main pane to list the different types of interfaces configured on the device.



5. Click Home to return to Director view.
6. Select Administration in the top menu bar.
7. Select Appliances in the left menu bar.
8. Select a FlexVNF device in the main pane by clicking the checkbox to the left of the device name. The following fields provide status information about the device's status.



| Field | Description |
|---------------------|---|
| Config Synchronized | <p>Status of configuration synchronization between device and Director:</p> <ul style="list-style-type: none"> •  Checkmark—Configurations on FlexVNF device and Director are synchronized with each other. This is the normal operational status. •  X—Configuration on FlexVNF device is not synchronized with configuration on Director. Check the connectivity between the FlexVNF device and the Director node. • Unknown—Configuration has not been synchronized with Director. This is the initial state. This state occurs for one of the following reasons: <ul style="list-style-type: none"> - FlexVNF device has just come up and has not yet synchronized with the Director node. - FlexVNF device and Director have not attempted to synchronize. - Director node is unable to connect to the FlexVNF device. • Locked—Configuration is administratively locked and FlexVNF device cannot synchronize with Director. • Error—Error occurred during configuration synchronization status check. |
| Reachability | <p>Status of the connection between SteelConnect EX Director and the appliance.</p> <ul style="list-style-type: none"> •  Checkmark—Appliance is reachable from SteelConnect EX Director. •  X—Director node cannot reach the FlexVNF device. Check the connectivity between the FlexVNF device and the Director node. • Unknown—Director node cannot determine the FlexVNF device's reachability status. This can occur when the FlexVNF device has just come up and has not yet connected to the Director node. |
| Service | <p>Status of FlexVNF services on the FlexVNF device:</p> <ul style="list-style-type: none"> • Up—FlexVNF services are active and functioning properly. • Failed—FlexVNF services are inactive. • Degraded—One or more FlexVNF services are no longer running. • Unknown—FlexVNF service status is unknown. • This can occur when the FlexVNF device has just come up and has not yet connected to the Director node, and it can occur when the Director node is unable to connect to the FlexVNF device. |
| Locked | <p>Status of an administrative configuration lock:</p> <ul style="list-style-type: none"> •  Locked icon—FlexVNF configuration is administratively locked and cannot be modified. •  Unlocked icon—FlexVNF configuration is administratively unlocked and can be modified. |

- Click the  Appliance CLI icon in the task menu bar to open the CLI.
- Log in with the username admin and the password versa123.
- Check the FlexVNF system status. The command output shows the software modules that are running on the device.

```
admin@FlexVNF:~$ show system status
```

