SteelConnect EX FlexVNF Basic Configuration Guide

Version 16.1R2

December 2019

Table of Contents

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

1 Configuring Organizations

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

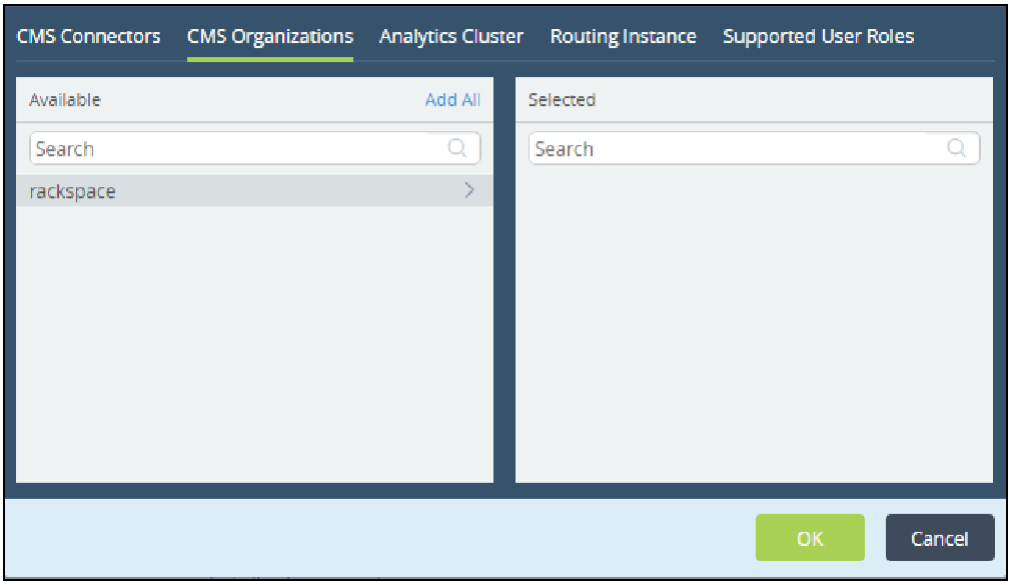
1. In the Director view, go to **Administration** > **Organizations**.
2. Click the Add icon to open the **Add Organization** screen.

Field	Description
Name	Name of the organization. Example: *ServiceProvider*
Description	Information about the organization.

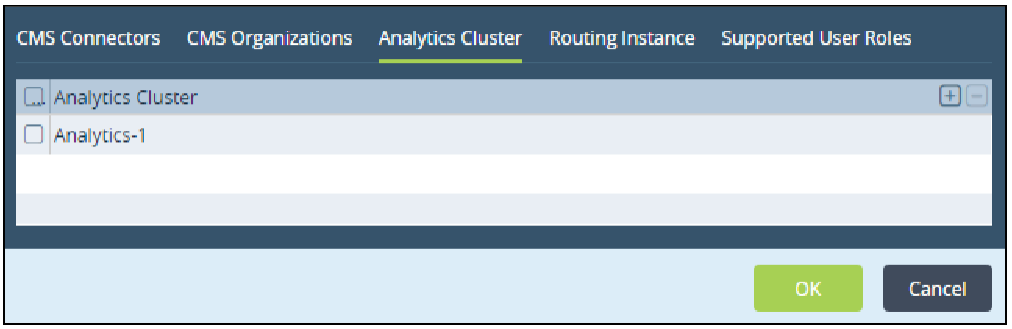
Field	Description
Tags	Tags that help explain the organization.
Global Organization ID	Unique ID for the organization
Organization Label	Label to identify the organization.
Shared Control Plane	Enable or disable sharing of control planes with the parent organization. Organizations with an activated **Shared 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: *ServiceProvider*
Authentication Connector	Authentication connector connects to external servers hosting users who connect with SteelConnect EX Director. The servers can be directory services like *LDAP* and *RADIUS*.

Field	Description
Subscription Plan	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: ▪ *Default NextGen FW NextGen VPN Plan*. Configure next generation firewall and next generation VPN. ▪ *Default NextGen VPN-Plan*. Configure next generation VPN. ▪ *Default Stateful FW NextGen VPN Plan*. Configure stateful firewall and next generation ▪ VPN. *Default-Stateful-FW-Plan*. Configure stateful firewall. Default-ADC-Plan. Choose this option to configure an ADC. ▪ *Default-ADC-SFW-Plan*. Configure an ADC for a stateful firewall. ▪ *Default-All-Services-Plan*. Configure all services (ADC, CGNAT, IPsec, firewall, et al). ▪ *Default-CGNAT-Plan*. Configure CGNAT. ▪ *Default-CGNAT-SFW-Plan*. Configure stateful firewall and CGNAT. ▪ *Default-IPSEC-Plan.* Configure IPsec. ▪ *Default-NextGen-FW-Plan*. Configure next generation firewall. ▪ *Default-NextGenFW-CGNAT-Plan*. Configure next generation firewall and CGNAT. ▪ *Default-SFW-IPSEC-CGNAT-Plan*. Configure stateful firewall IPsec and CGNAT. ▪ *Default-SFW-IPSEC-Plan*. Configure stateful firewall IPsec. ▪ *Default-Stateful-FW-Plan*. Configure stateful firewall. ▪ *Default-DPI-Plan*. 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.

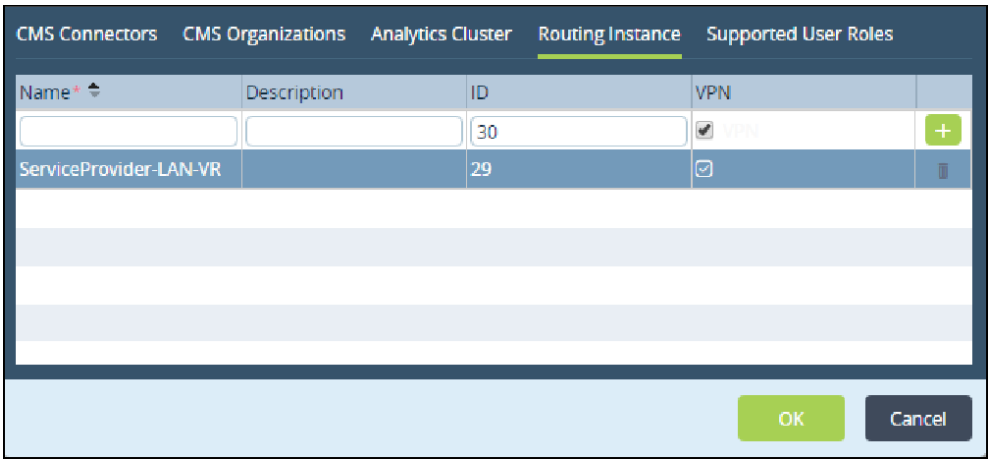


c. Click **Analytics Connectors**.



i. Click the Add icon to add a cluster.
ii. Select a cluster from the list of available clusters.

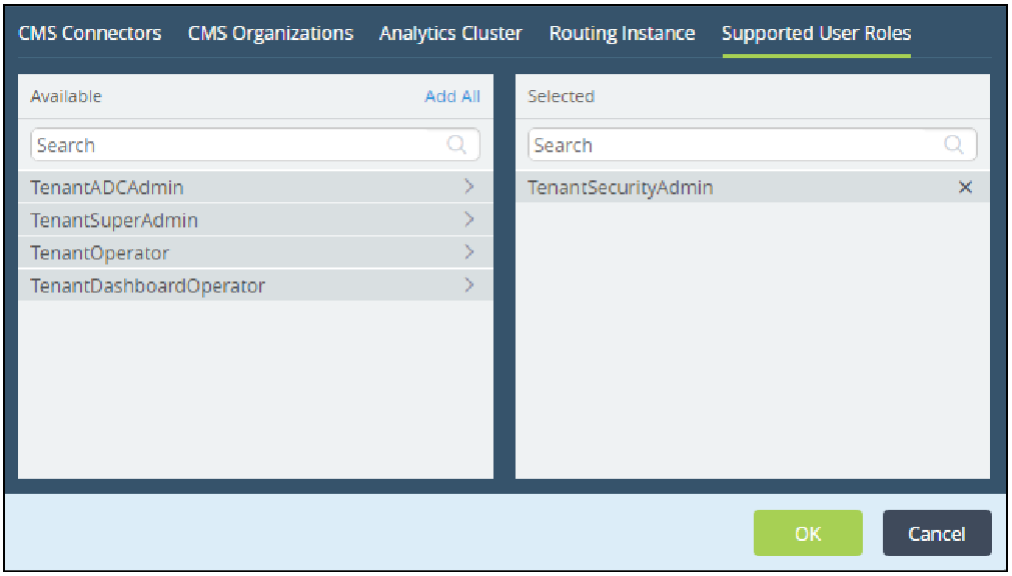
d. Click **Routing Instances** to define virtual routing instances for the organization.



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

i. Click the Add icon.

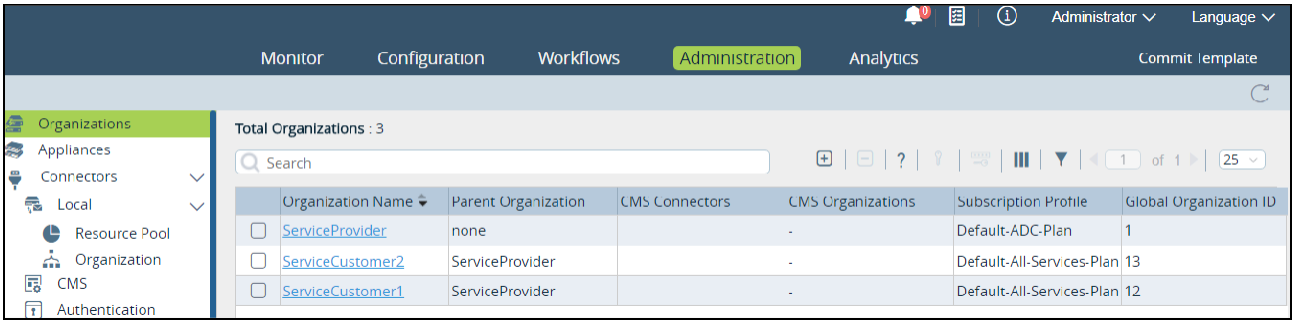
e. Click **Supported User Roles**.



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

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

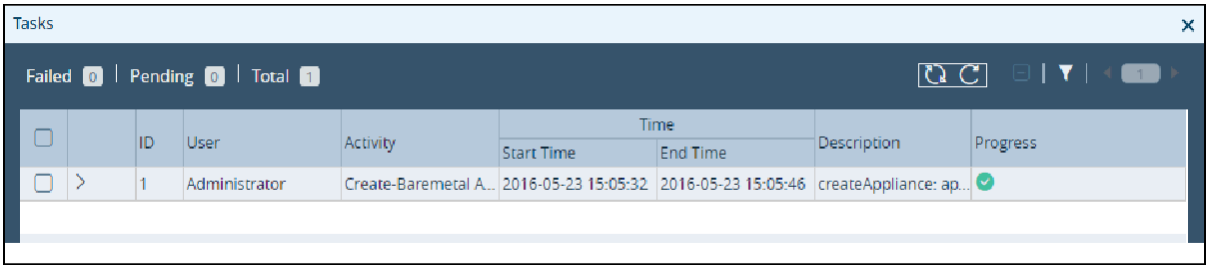
This creates a provider organization. Now, you can create its child organizations.



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.

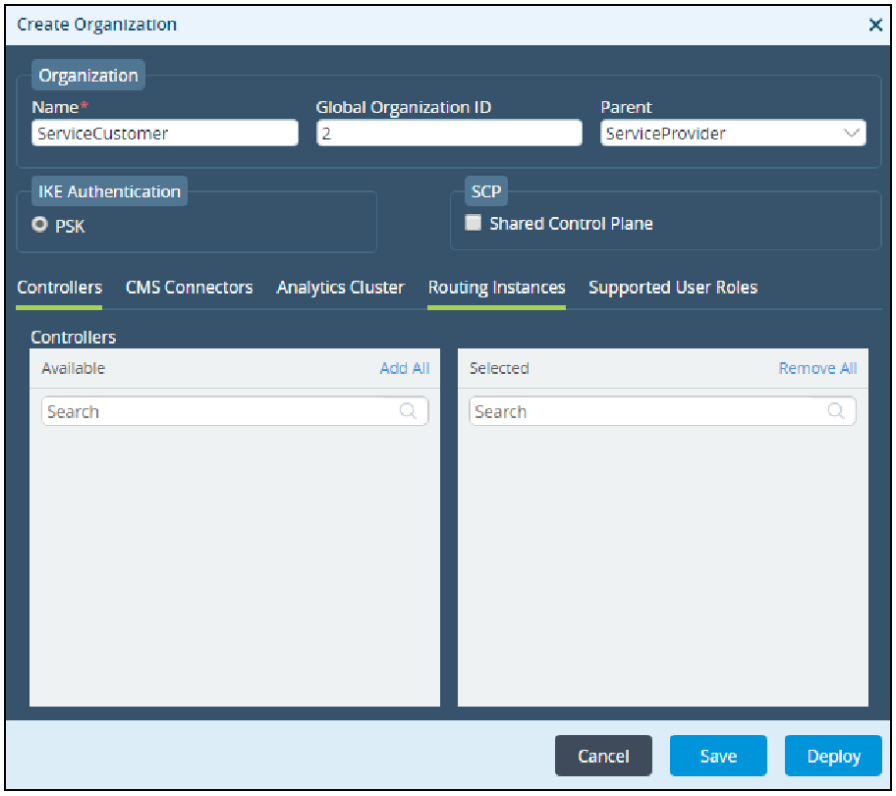


1.2.2 Adding customer organizations

Steps

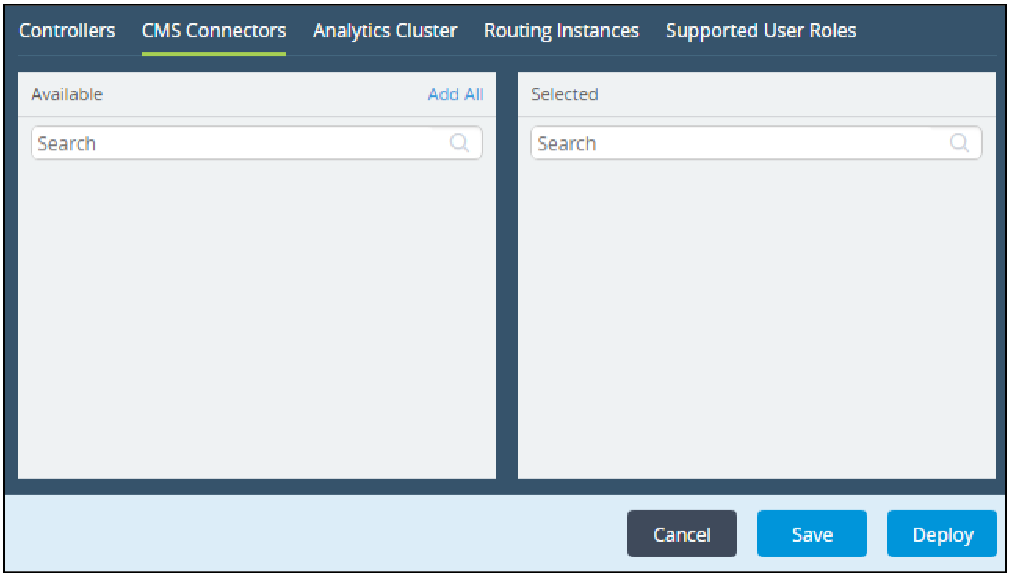
1. In the Director view, go to **Workflows** > **Infrastructure** > **Organizations**.

2. Click the Add icon to onboard an organization.

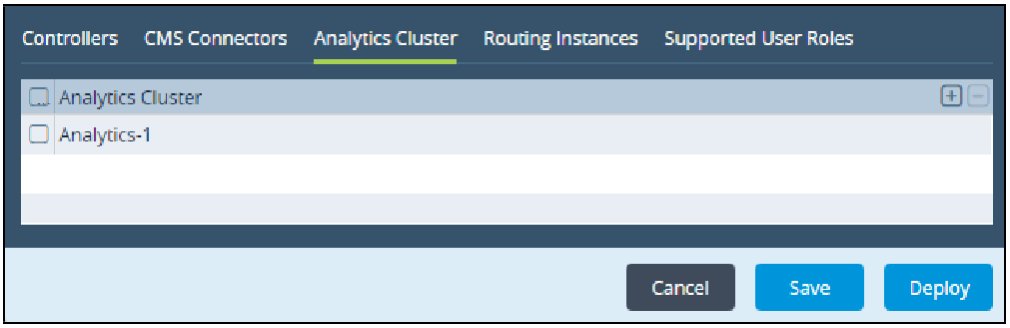


Field	Description
Name	Name of the organization. Example: *ServiceProvider*
Global Organization ID	ID assigned to the organization. The system populates the value automatically with the next available ID. You can change it to a different available value between 1 and 31.
Parent	Parent organization of the organization created.
IKE Authentication	Type of authentication: *PSK*(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.

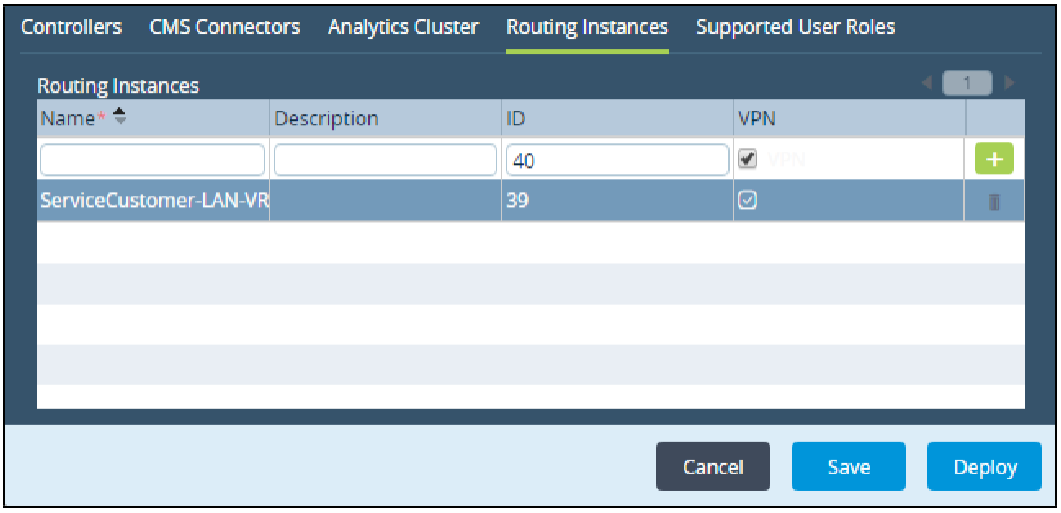


c. Click **Analytics Cluster**.



i. Click the Add icon to add a cluster.
ii. Select a cluster from the list of available clusters.

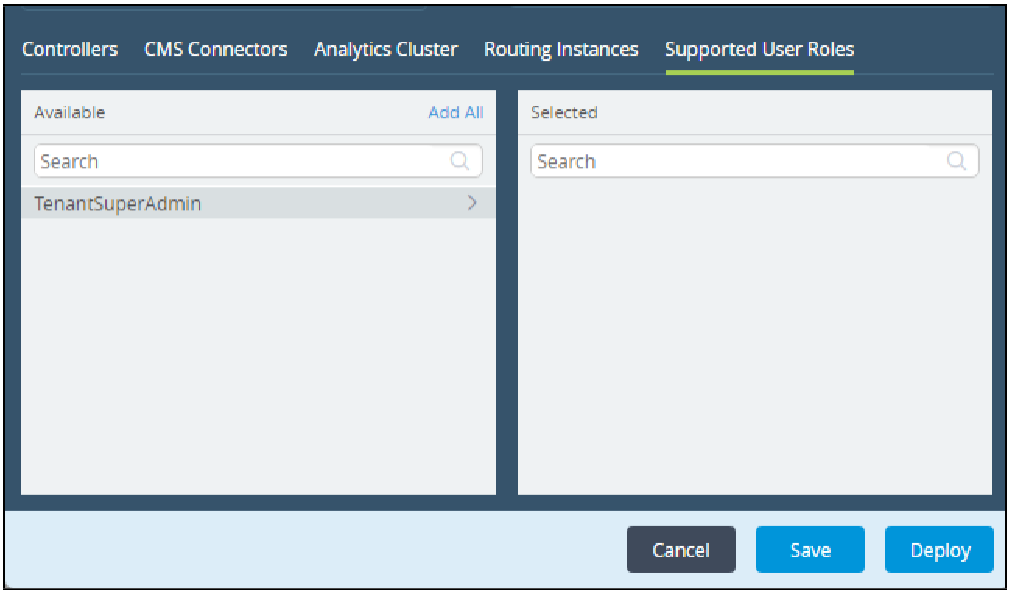
d. Click **Routing Instances** to define virtual routing instances for the organization.



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.

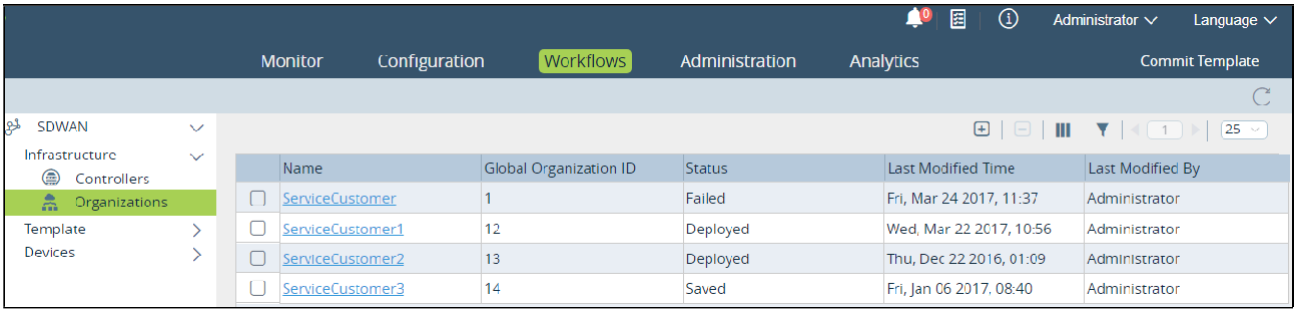
e. Click **Supported User Roles**.



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).



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.M8vbF3jl1pp0;
        sshpublickey laptop {
            "sshrsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCyhCqGWaZmpji
xaKVqjK2Ij4QUaJuiA1T+pSTveaJxrNSiCWzfKibY+
y/QV0a3+0Y4SQ5W9gkyMbL6Mrk1afqnznp5y20gMIbt
ul58aJ/Q09Ygu2qg4ULb7iUgHBzwunk2hViKez06yMD
jbsE3JGvk5chffSbWXWrkObgwcHkn6KPLiYSW0cEbVS
Qa1bbF7GSJhIX6QWR17IWjp7MiD569aYxf6rI/WdjSI
StO1p7mm01Y93sXnYn7hLs+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/;
            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)

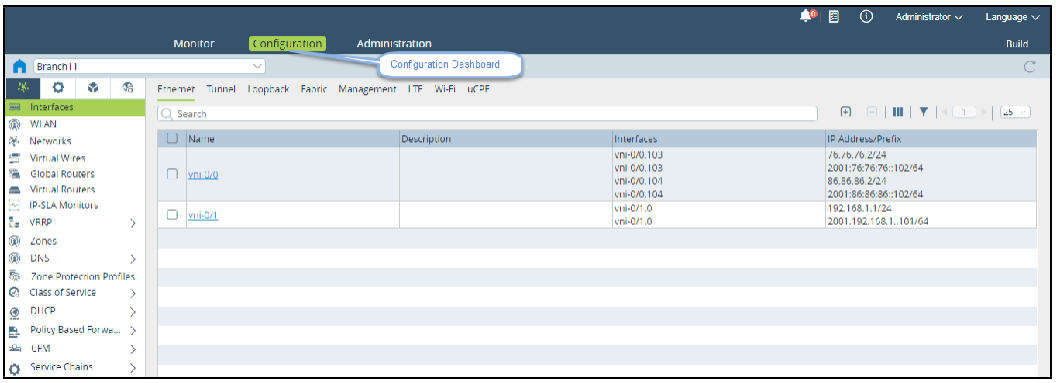
2 Configuring SteelConnect EX FlexVNF appliances

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

2.1 Configuring appliances

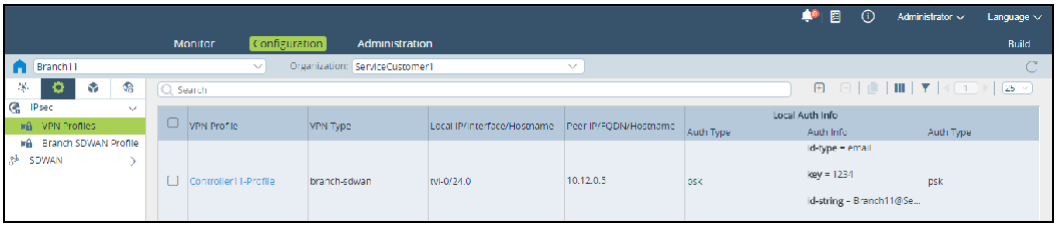
Steps

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 h/as 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 writes.
     - **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.

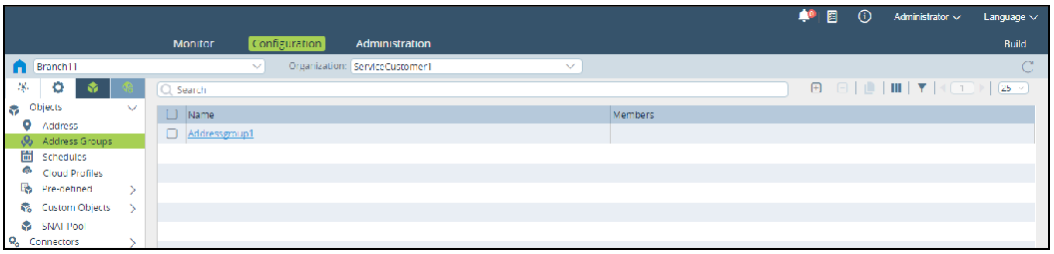


   - **Services**.
     This tab is used to configure services based on the subscription plan:

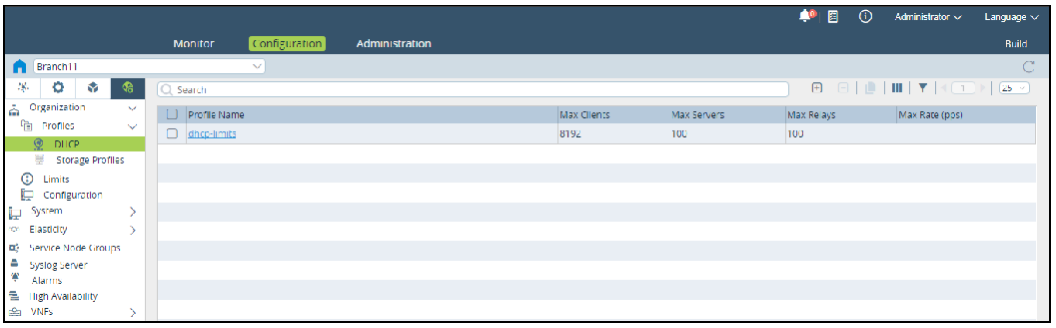
- **IPsec**
- **SDWAN**



- **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**



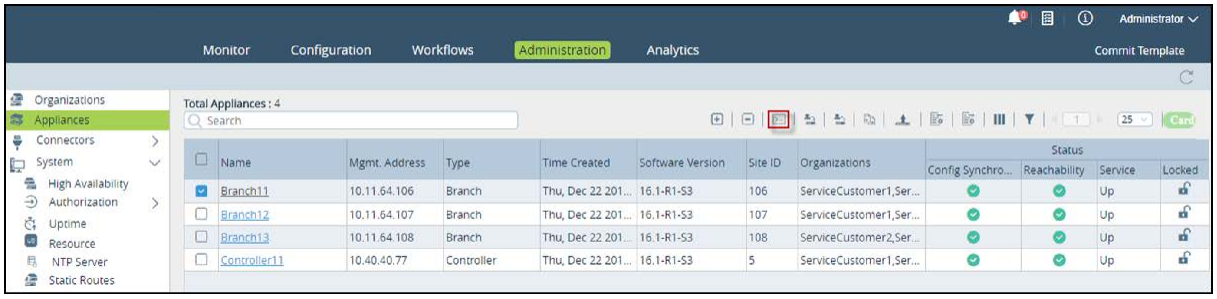
- **Others**.
  This tab is used to configure the following elements:
  - **Organization**
  - **System**
  - **Elasticity**
  - **Server Node Groups**
  - **Syslog Server**
  - **Alarms**
  - **High Availability**



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:

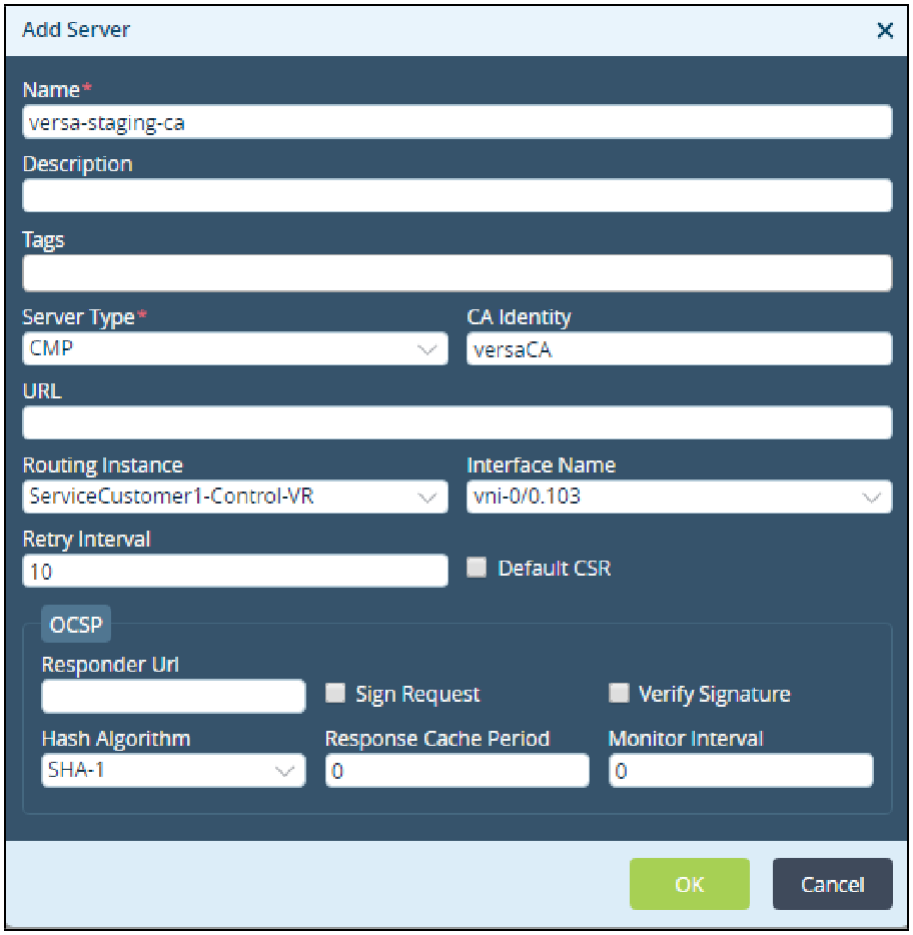
1. Configuring certificate server(see page 19)
2. Configuring certificate request(see page 22)

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.



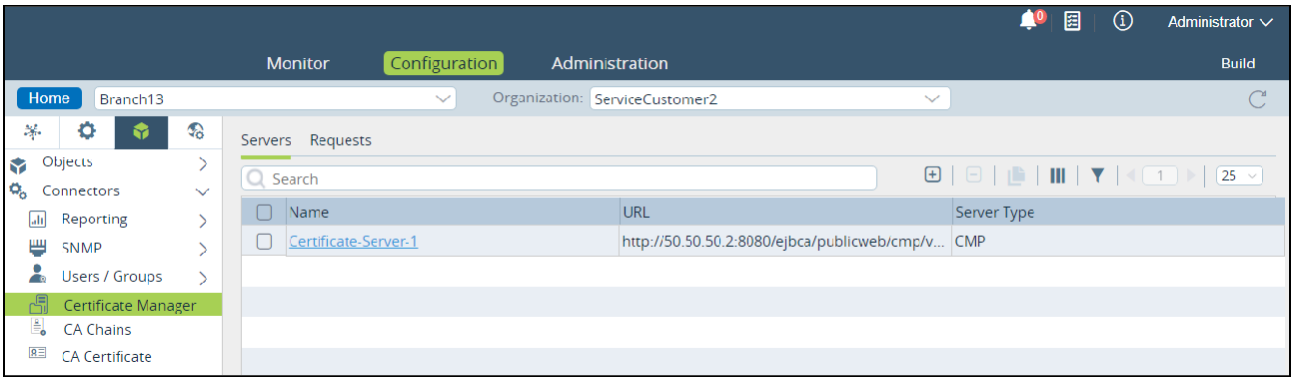
Field	Description
Name	Name of the server.
Description	Description of the server.
Tags	Tags to identify the server.
Server Type	Type of the server. Example: *CMP*
CA Identity	Name of the certificate authority.
URL	URL of the server hosting the certificate authority.
Routing Instance	Routing instance 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.



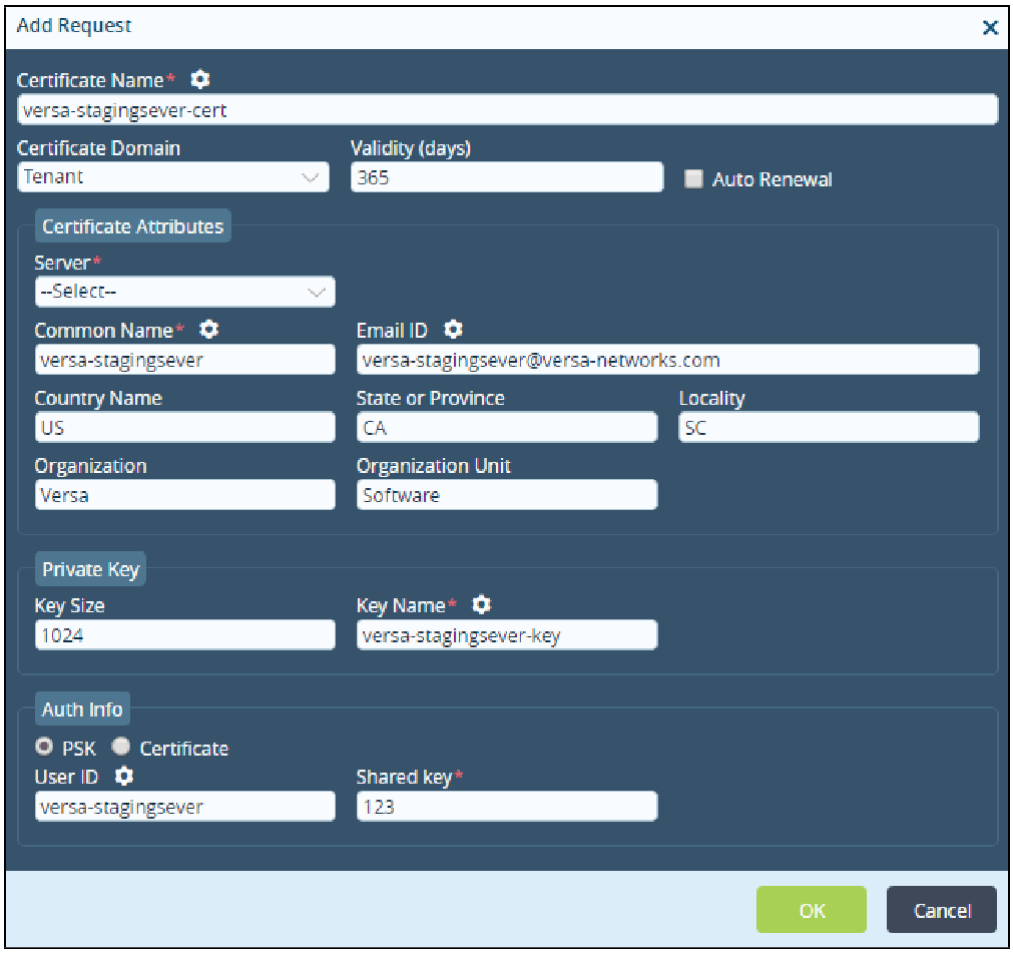
- To delete an existing server, select the check box corresponding to the server and click the Delete icon on the top right corner.
- To filter the configuration screen table information, click on the top right corner.

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.

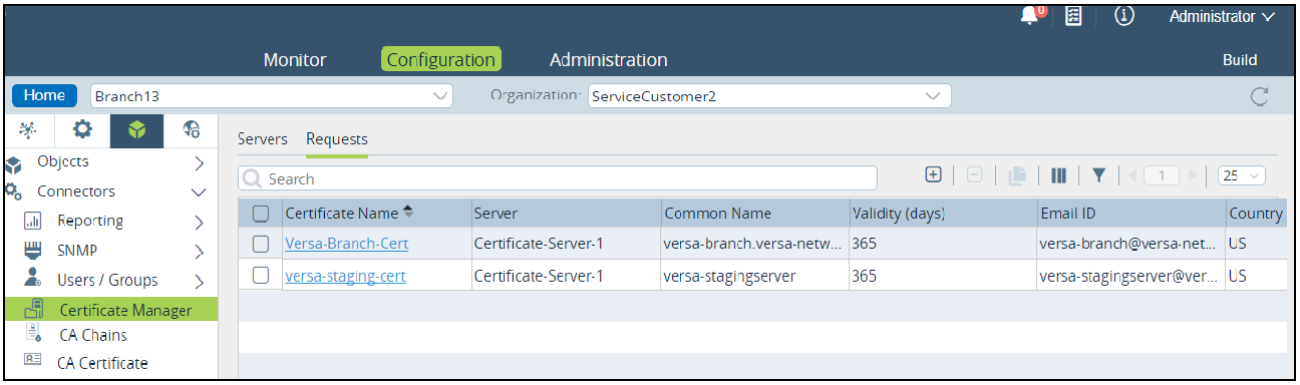


Field	Description
Certificate Name	Name of the branch certificate.
Certificate Domain	Domain of the certificate.
Validity	Number of days for which this certificate is valid.
Auto Renewal	Enable or disable the renewal of the certificate.
Server	Name of the server.

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: • *PSK(PreSharedKey)* • *Certificate*
User ID Shared Key	Applicable when *PSK* is the authentication mode. • *UserID* • *SharedKey*. Password should be identical to the shared key of the server.
• Certificate Name • CA Chain • Certificate Domain	Applicable when *Certificate* is the authentication mode. • *CertificateName*. Name of the certificate. • *CAChain*. Name of the certificate chain. • *CertificateDomain*.

4. Click **OK**.

This configures a certificate.

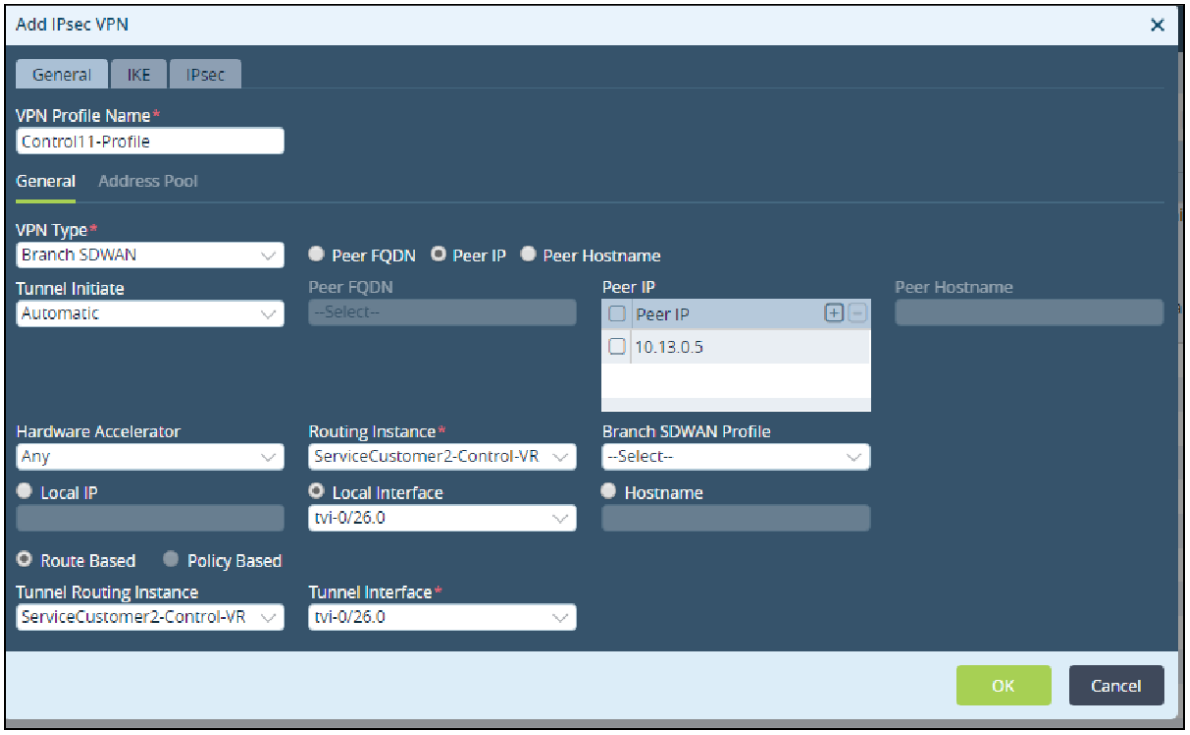


2.4 Applying configured certificates

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

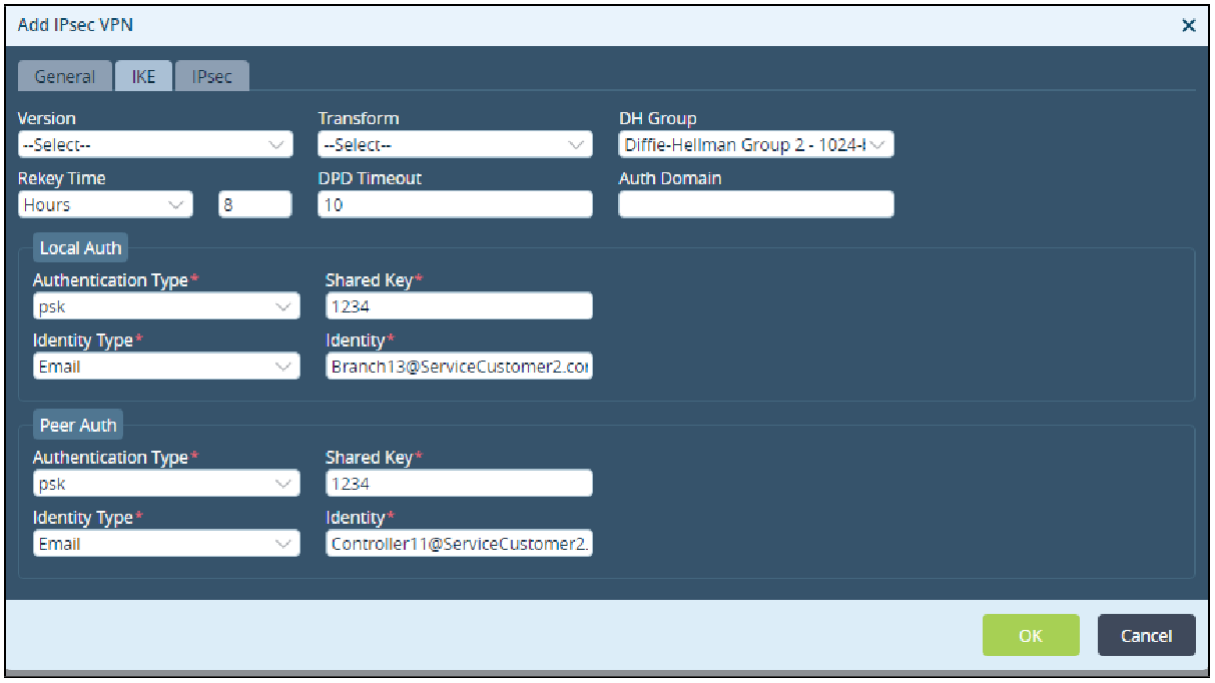
Steps

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.



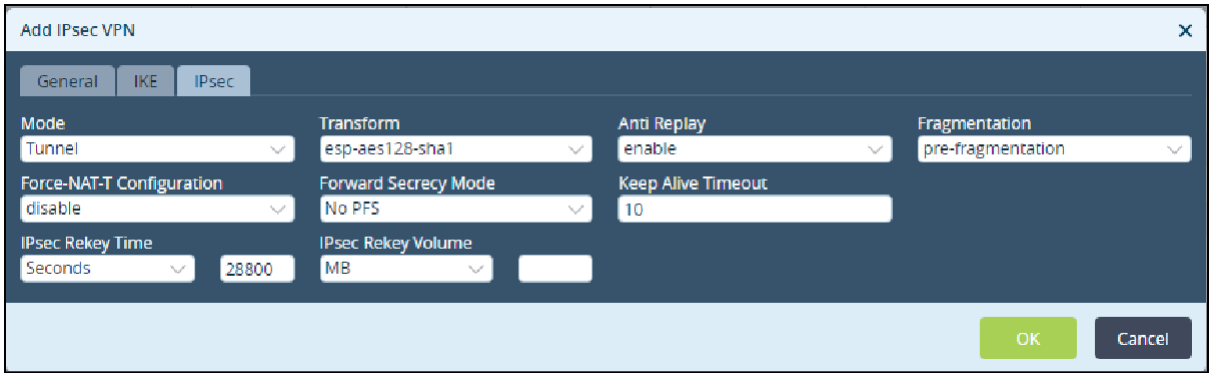
Field	Description
VPN Profile Name	Name of the VPN profile.
VPN Type	Type of VPN.
Tunnel Initiate	Mode to initiate the child SA creation. For rule-based VPN, a tunnel can be initiated only when traffic is seen for that rule. • *Traffic* • *Automatic*
• Peer FQDN • Peer IP • Peer Hostname	Type of identification to be used for the peer identity.
Routing Instance	Routing instance to be used.
Branch SDWAN Profile	Type of branch profile.
• 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.

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



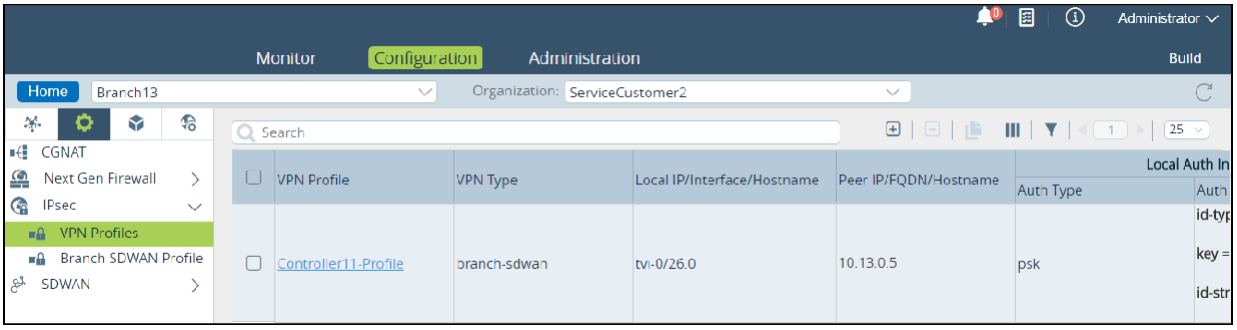
Field	Description
Rekey Time	Time duration in which another key is generated.
Local Auth	
Authentication Type	Mode of authentication: • *PSK*(Pre Shared Key) • *Certificate*
Shared Key	Key for access. (Applicable when *PSK* is selected)
Identity Type	Type of identity proof to be given: • *Email* • *FQDN* (Applicable when *PSK* is selected)
Identity	Email ID. (Applicable when **Identity Type** is *Email*)

5. In the **IPSec** tab, enter the required information. Refer to Configuring IPsec profiles in the *SteelConnect EX SD-WAN Configuration Guide*.



6. Click **OK**.

This completes applying the certificate information for the VPN.



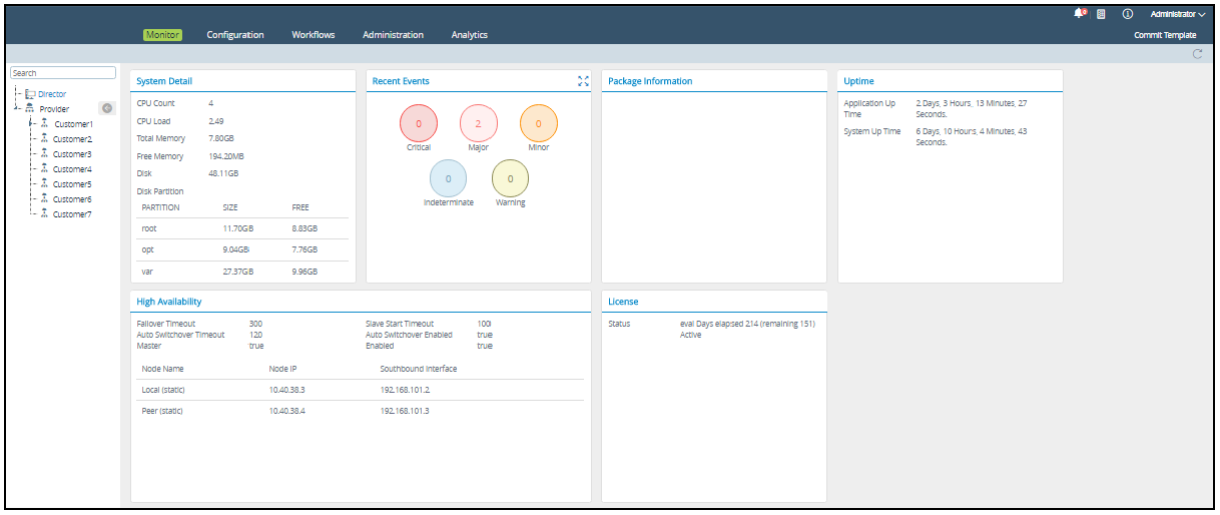
2.5 Alarm management

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.

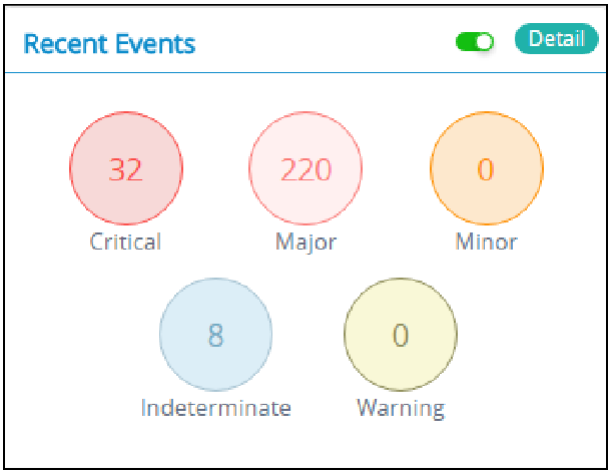


The screen displays the following sections:

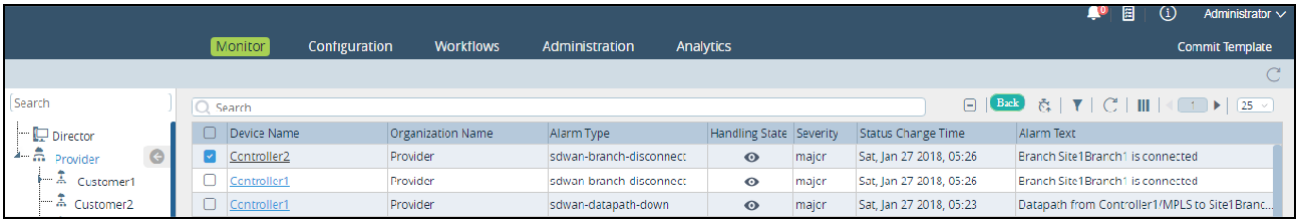
- **Asset Inventory**. Number of tenants, directors, SDWAN controllers, vCPEs.
- **Recent Events**. Number of events of different categories (critical, major, minor, indeterminate, warnings)
- **Firmware Summary**. Number of CPUs, system version, etc.
- **Provider Health**. Health of the different elements 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.

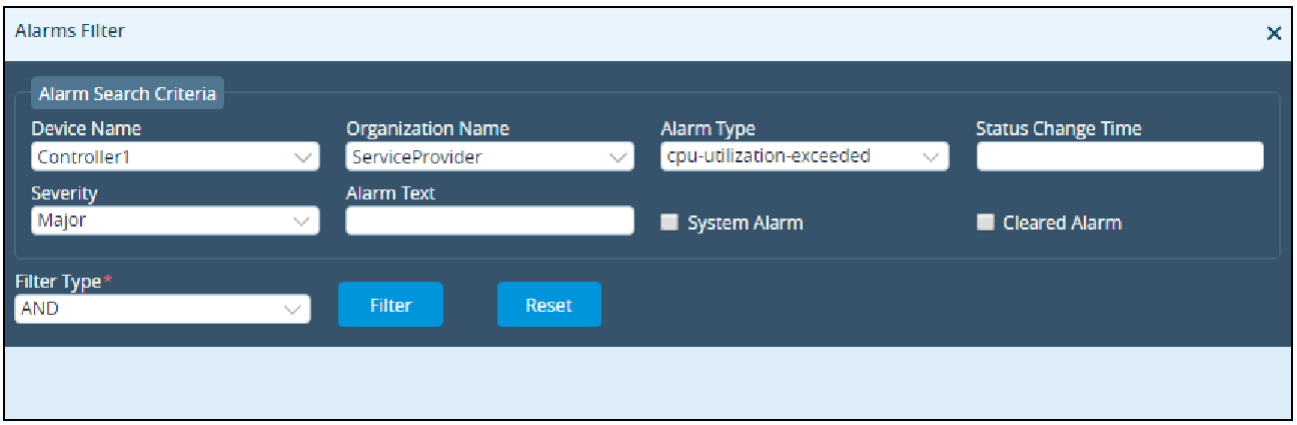


Click the Detail Detail button on **Recent Events** to view the information of all the alarms in relation to the associated devices.

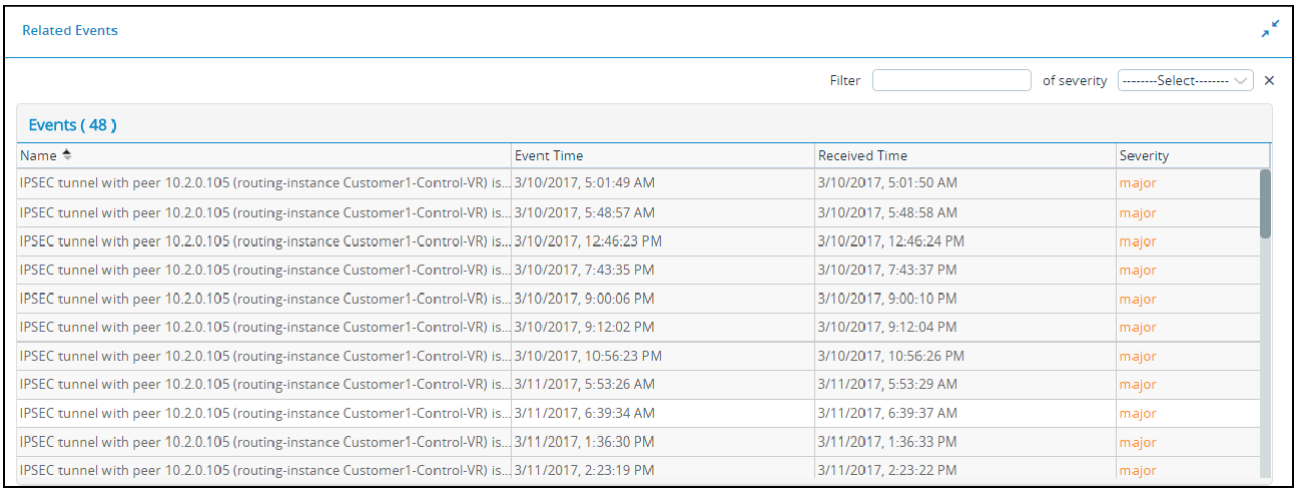


Click Back to go back to the tile view of this screen.
Click **Column Filter** to select the columns to be displayed.

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



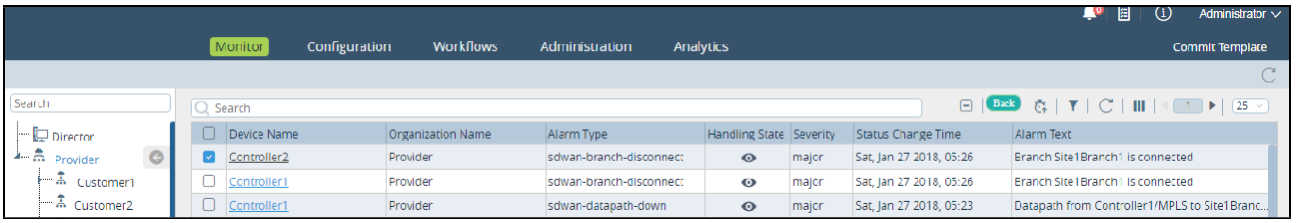
Click on a device to view its alarm (raised and cleared) history.



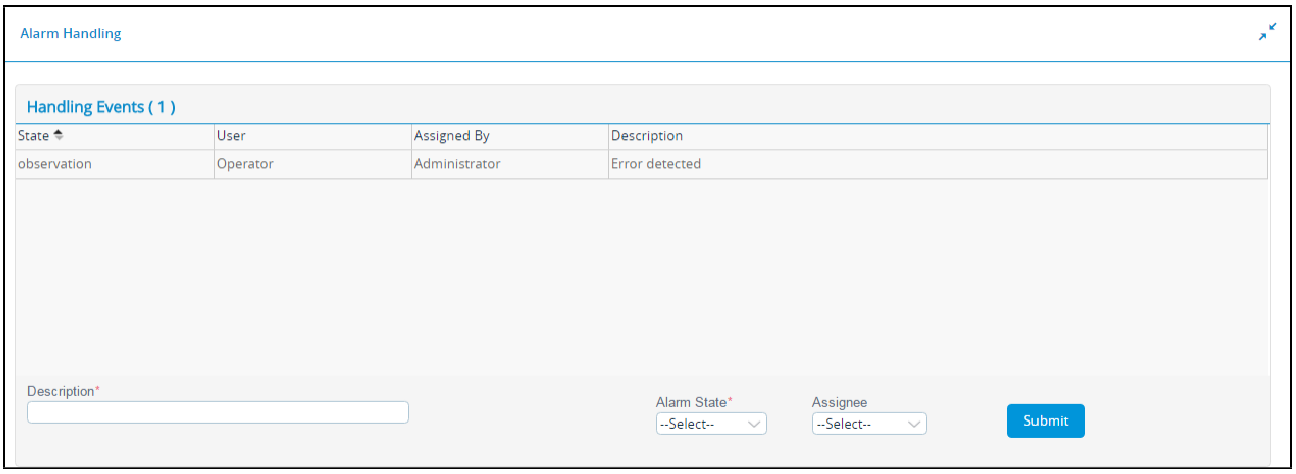
You can filter events per severity level.

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.



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



> 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

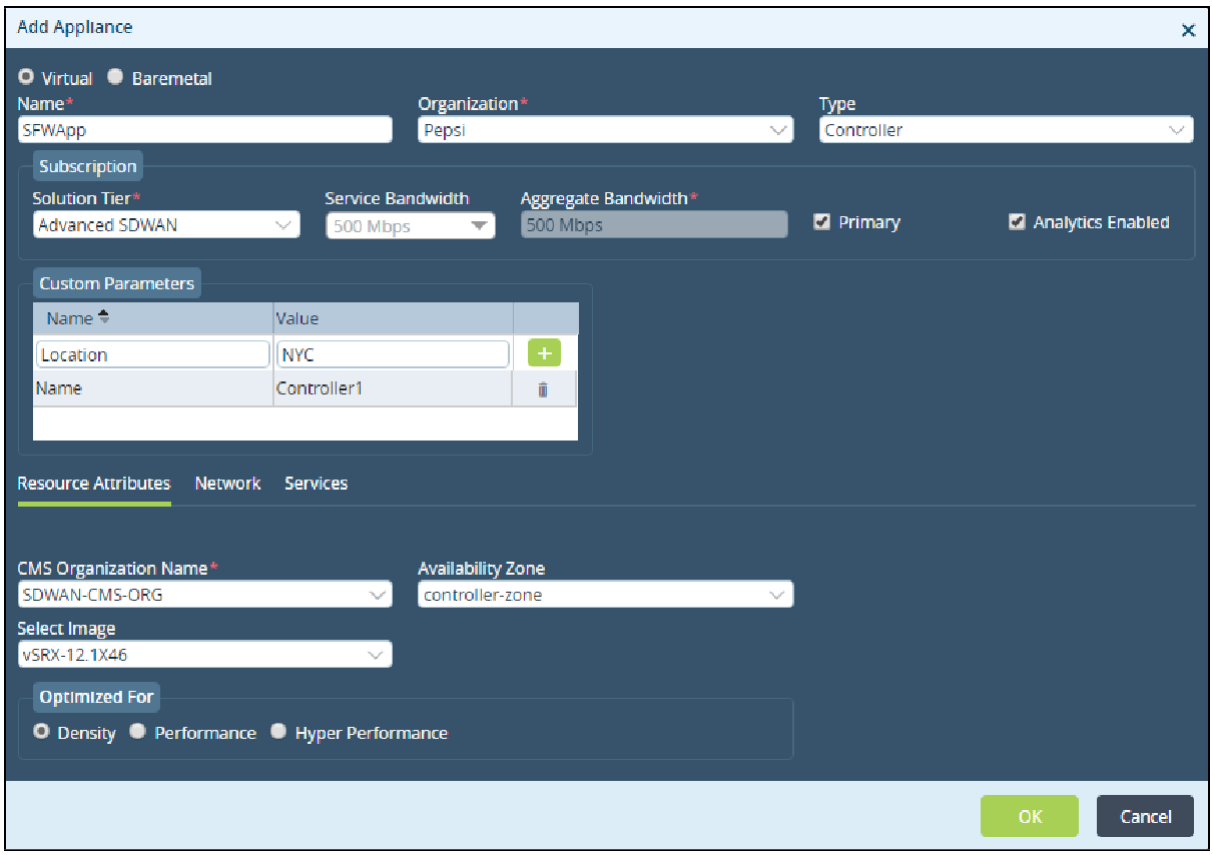
1. Enter the event description.
2. Select the **Alarm State**. The values are:
   - *Acknowledge*
   - *Close*
   - *Investigation*
   - *None*
   - *Observation*
3. Select the **Assignee**.
4. Click **Submit**.

3 Creating FlexVNF appliances

After configuring FlexVNF on vCloud Director, the next step is to create an appliance. This makes the appliance available on the network.

Steps

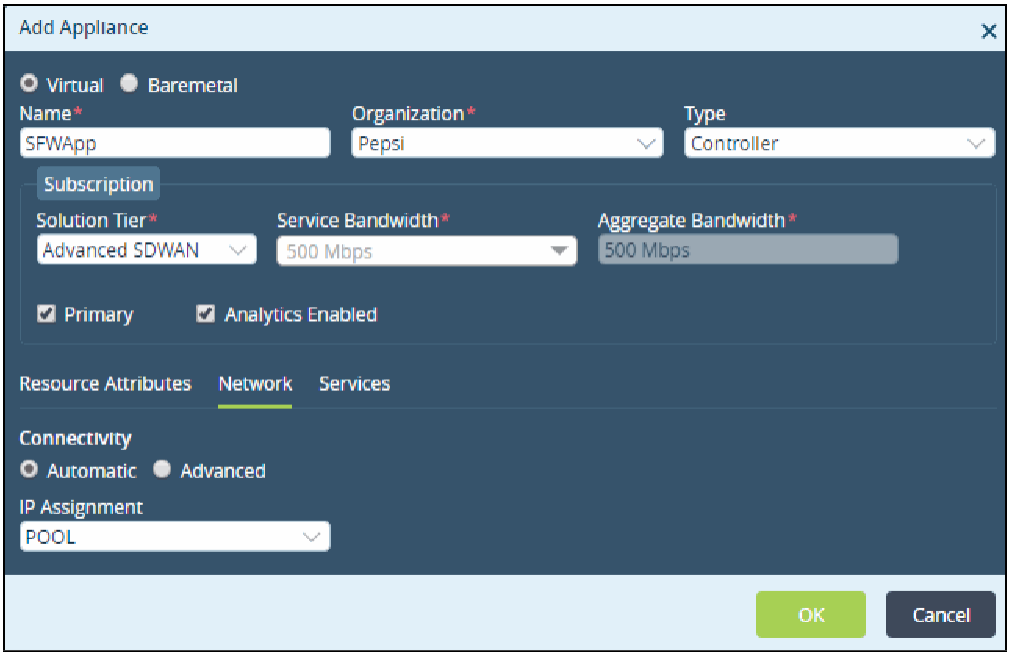
1. In the Director view, go to **Administration** > **Appliances**.
2. Click the Add icon to open the **Add Appliance** screen.



Field	Description
• Virtual • Baremetal	Type of underlying platform.
Name	Name of the SteelConnect EX FlexVNF. Example: *SFWApp*
Organization	Name of the organization. Example: *Pepsi*

Field	Description
Type	Appliance type: ▪ *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.
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	▪ **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.

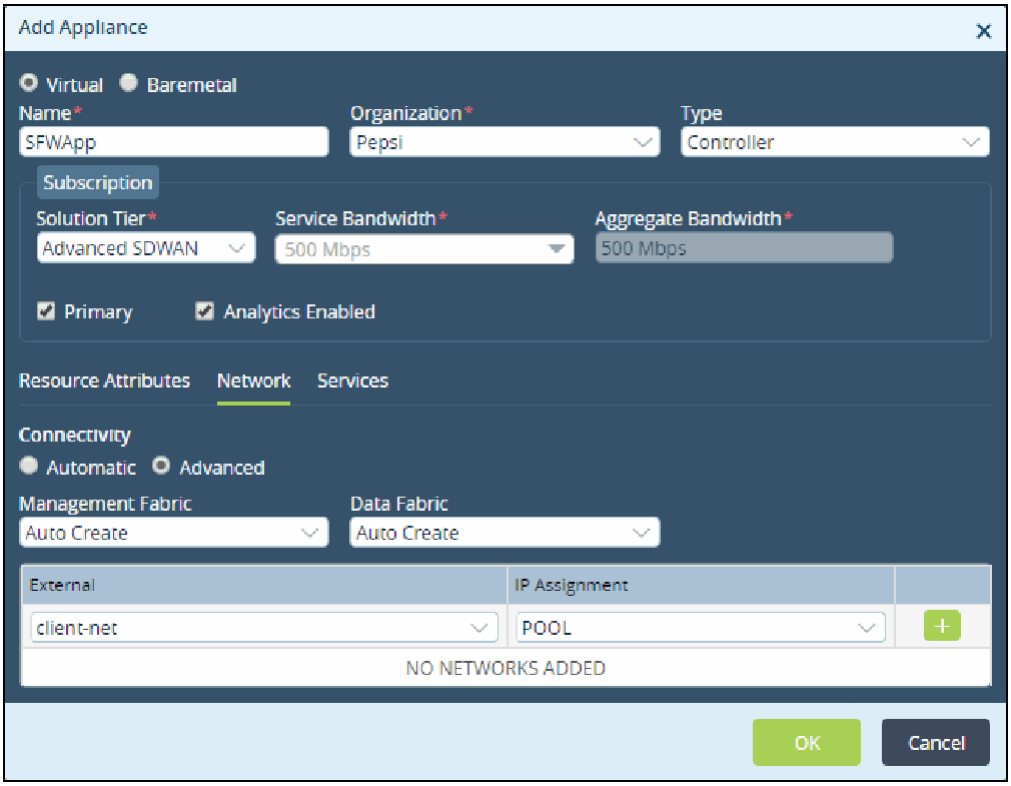
a. Click the **Network** tab.



Field	Description
Connectivity	▪ 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: ▪ *POOL* • *DHCP* • *NONE*

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

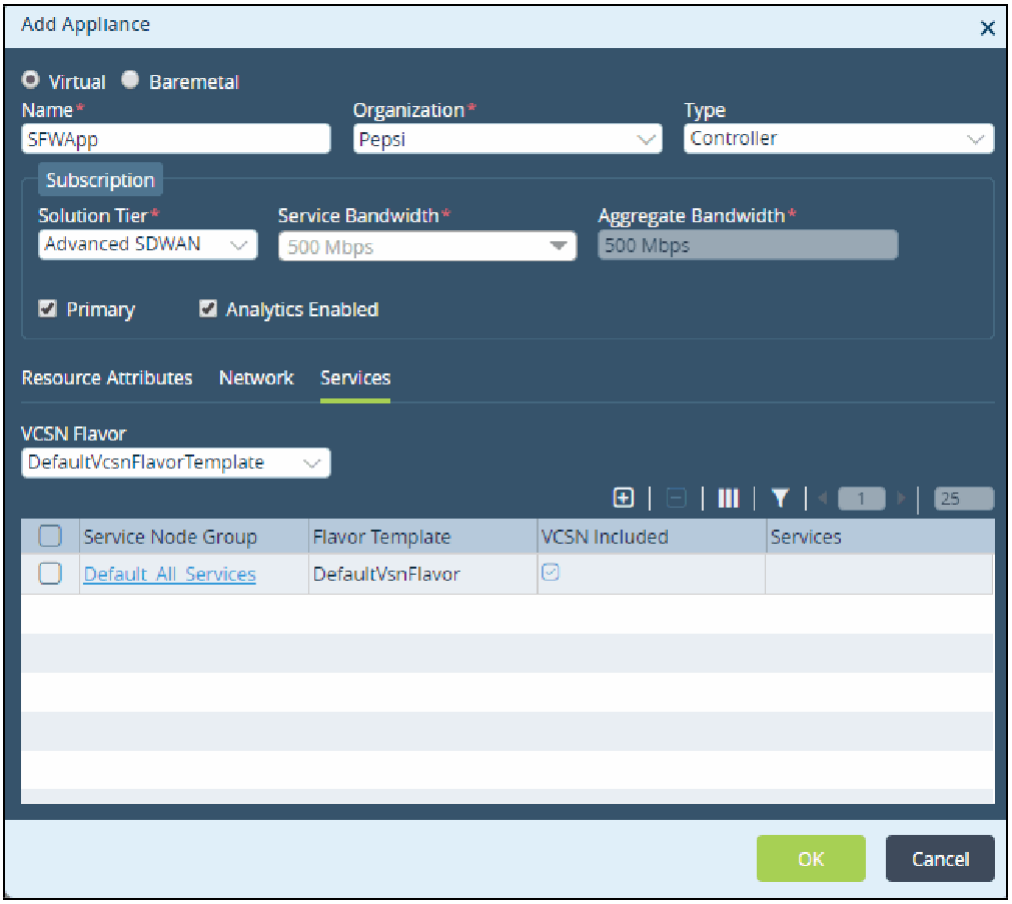
i. In the **Advanced** option, manually add multiple external networks to connect the appliance by selecting the **External** network entity and related **IP Assignment** method.



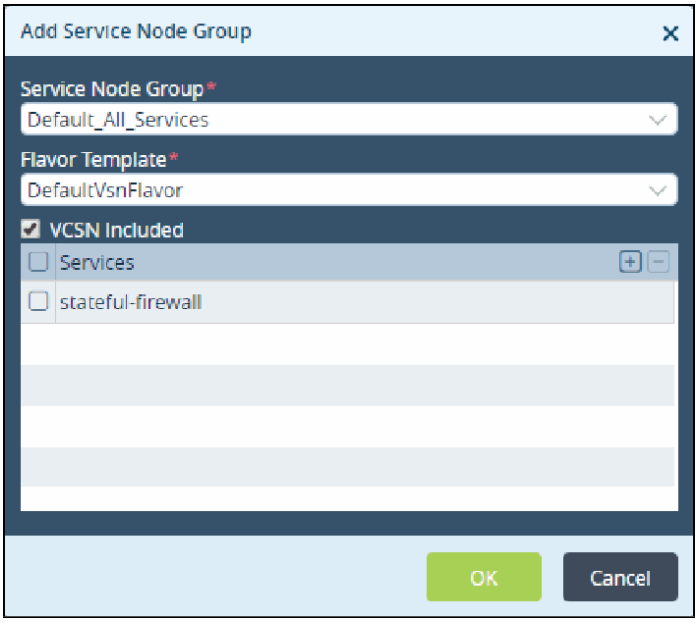
Field	Description
Management Fabric	Internal network.
Data Fabric	External network.
External	Name of the external network.
IP Assignment	Method of IP address allocation: ▪ *POOL* • *DHCP* • *NONE*

ii. Click the + Add icon. Repeat this step to add multiple external networks.

b. Click the **Services** tab.



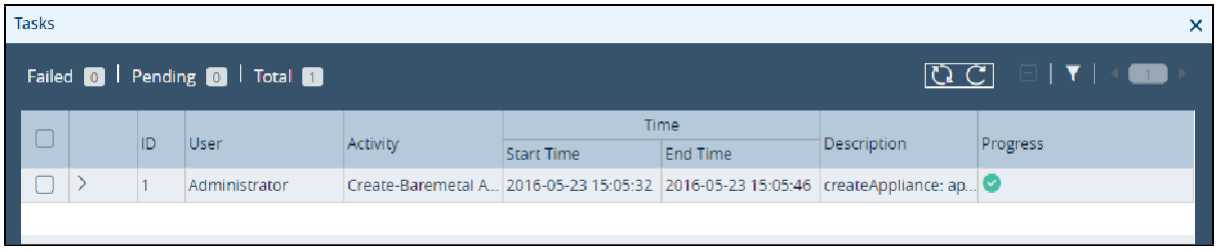
i. Click the Add icon to add a service node group.



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.



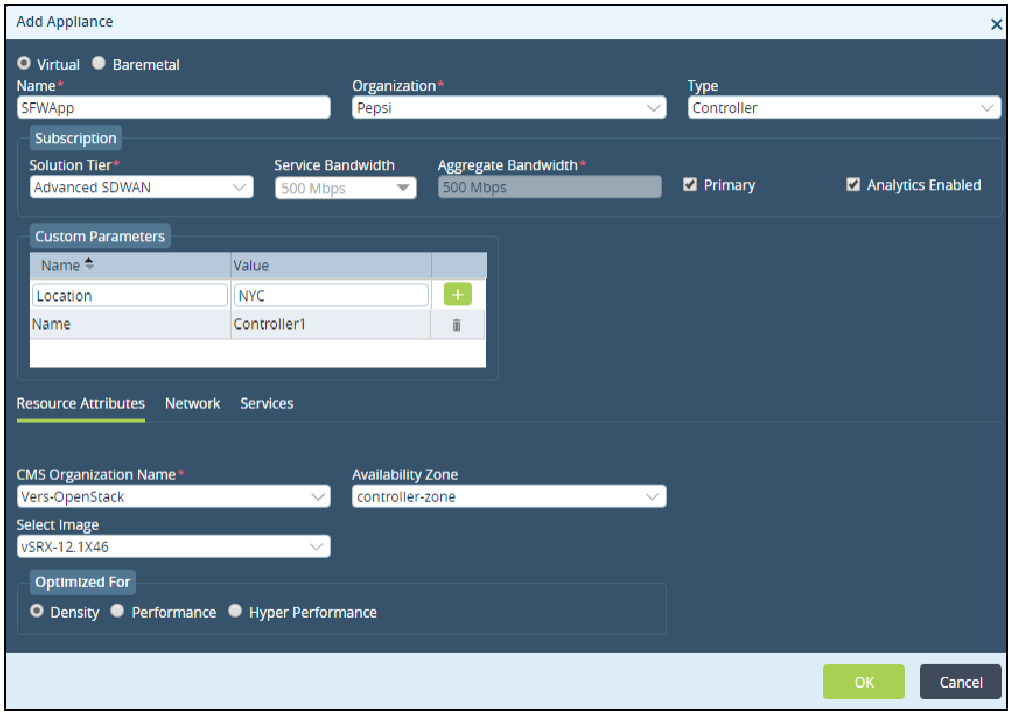
3. Click the Tasks icon on the top right menu to view the activity details.

Appliances can be also configured using the CLI.

3.1 Creating FlexVNF appliances on OpenStack

Steps

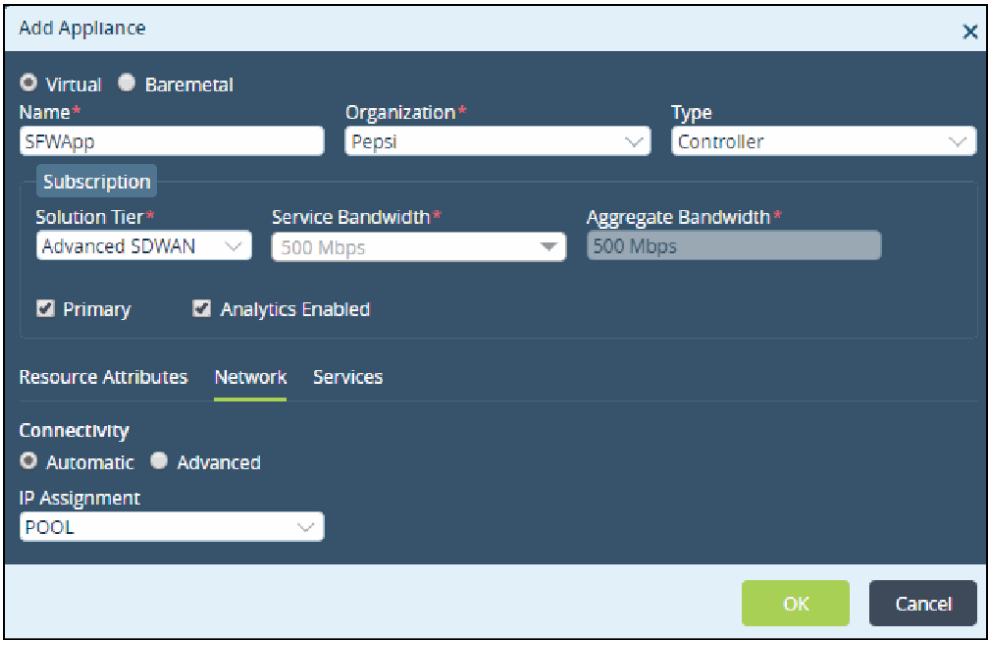
1. In the Director view, go to **Administration** > **Appliances**.
2. Click the Add icon to open the **Add Appliance** screen.



Field	Description
• Virtual • Baremetal	Type of underlying platform.
Name	Name of the SteelConnect EX FlexVNF. Example: *SFWApp*
Organization	Name of the organization. Example: *Pepsi*
Type	Appliance type: ▪ *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	▪ **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.

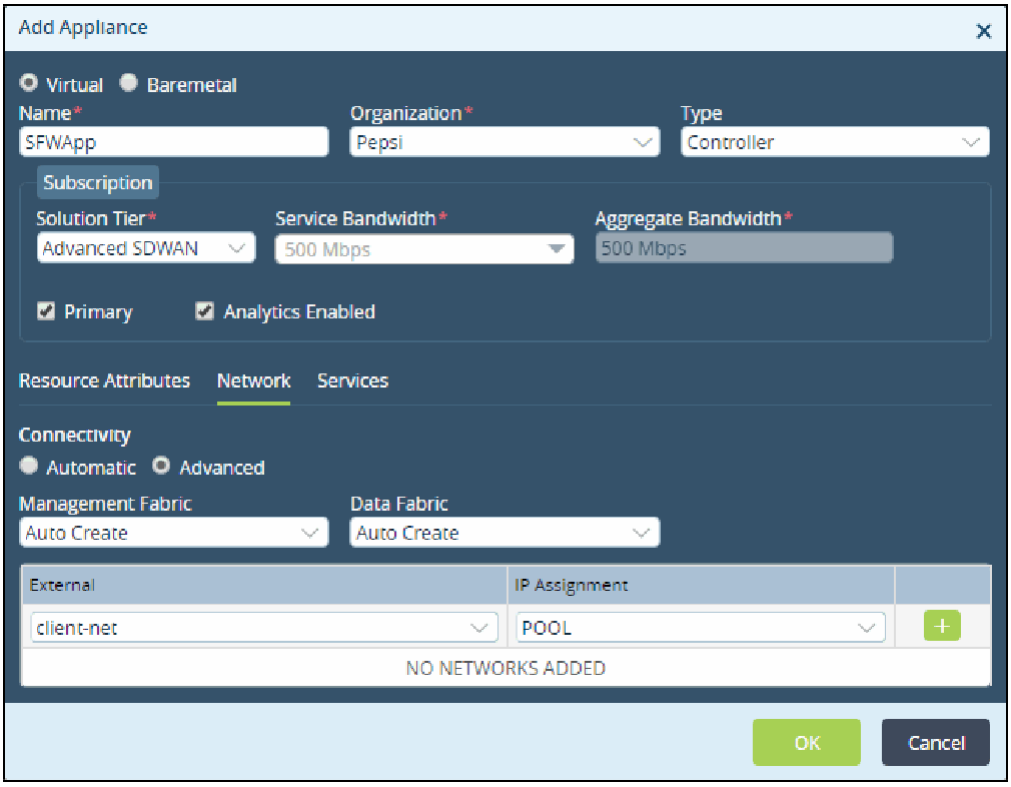
a. Click the **Network** tab.



Field	Description
Connectivity	▪ **Automatic**. connects the FlexVNF appliance to all the networks existing on vCloud Director. • **Advanced**
IP Assignment	Mode of allocating IP addresses: ▪ *POOL* • *DHCP* • *NONE*

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.

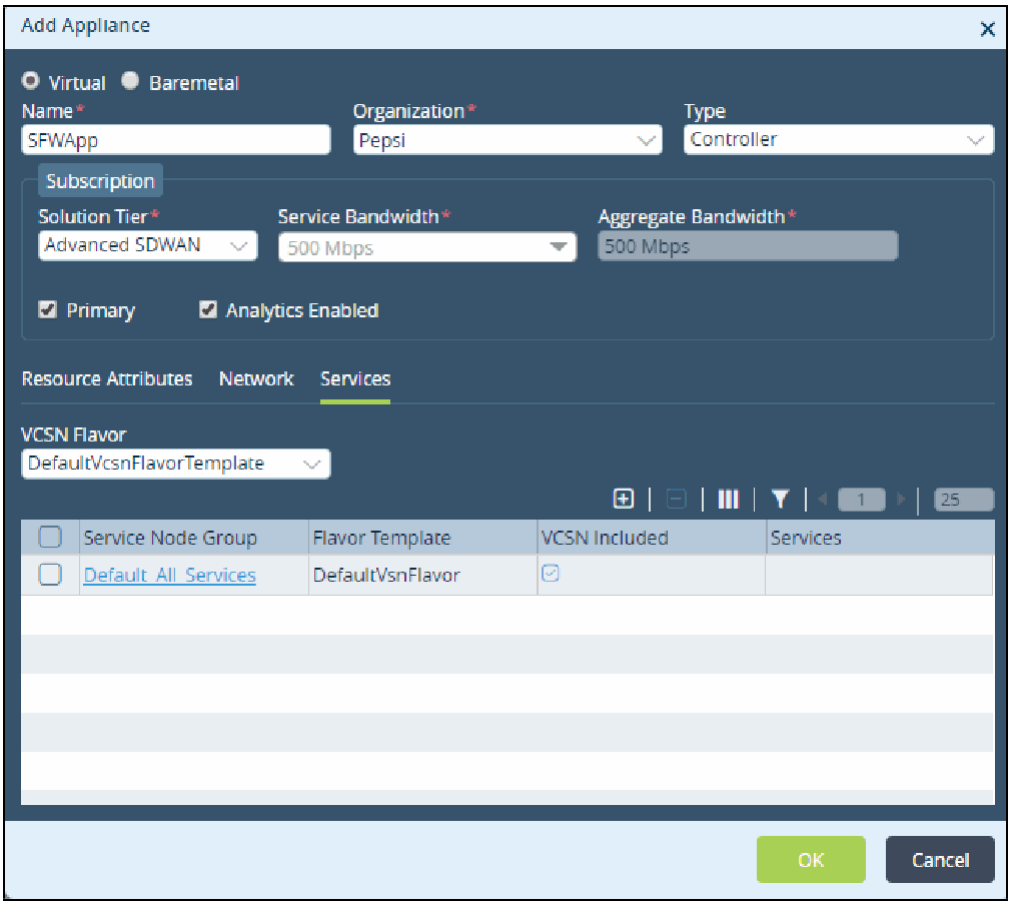


Field	Description
Management Fabric	Internal network.
Data Fabric	External network.
External	Name of the external network.

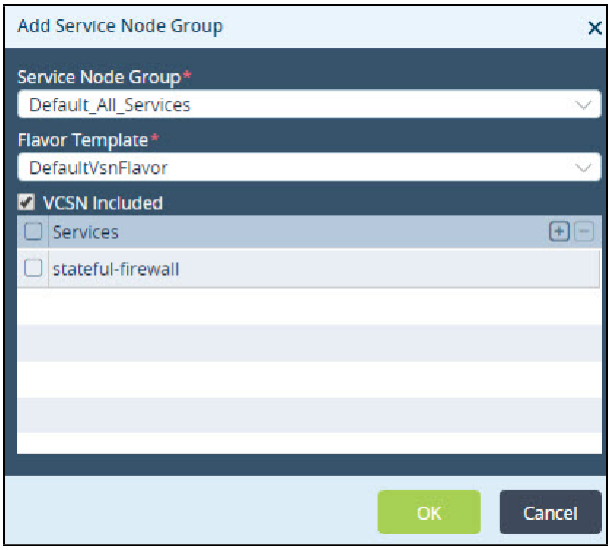
Field	Description
IP Assignment	Method of IP address allocation: ▪ *POOL* • *DHCP* • *NONE*

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.

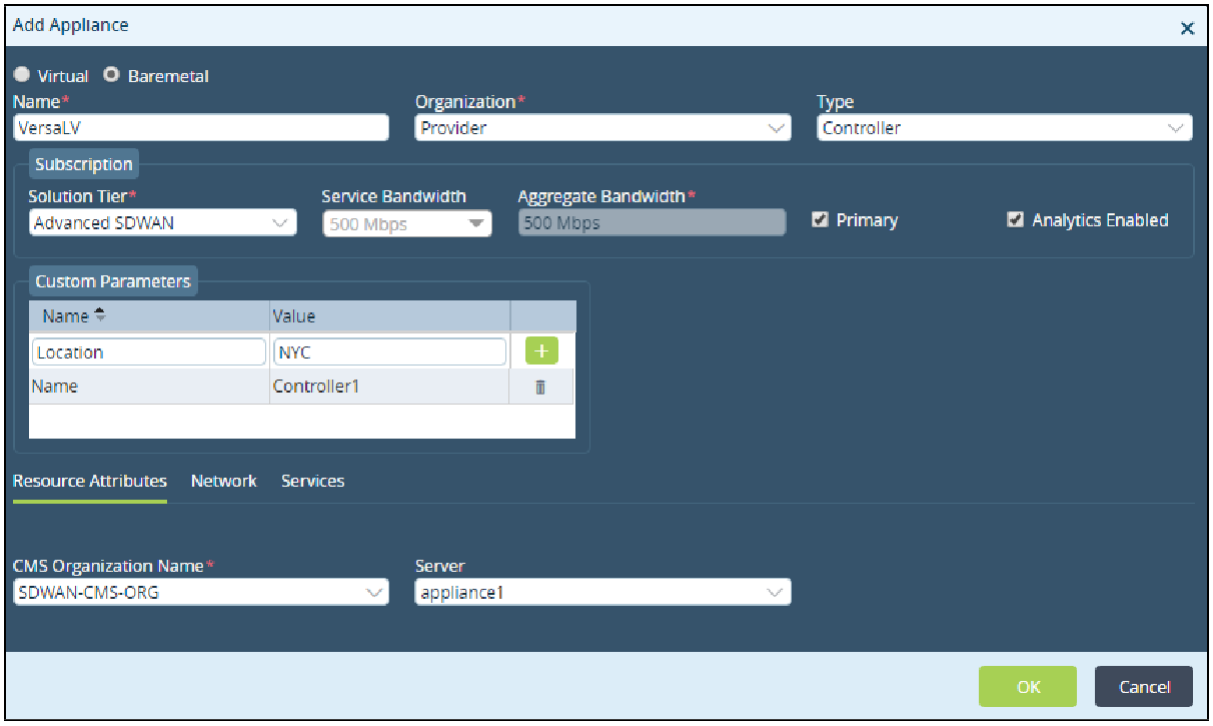
This creates an appliance on OpenStack.

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

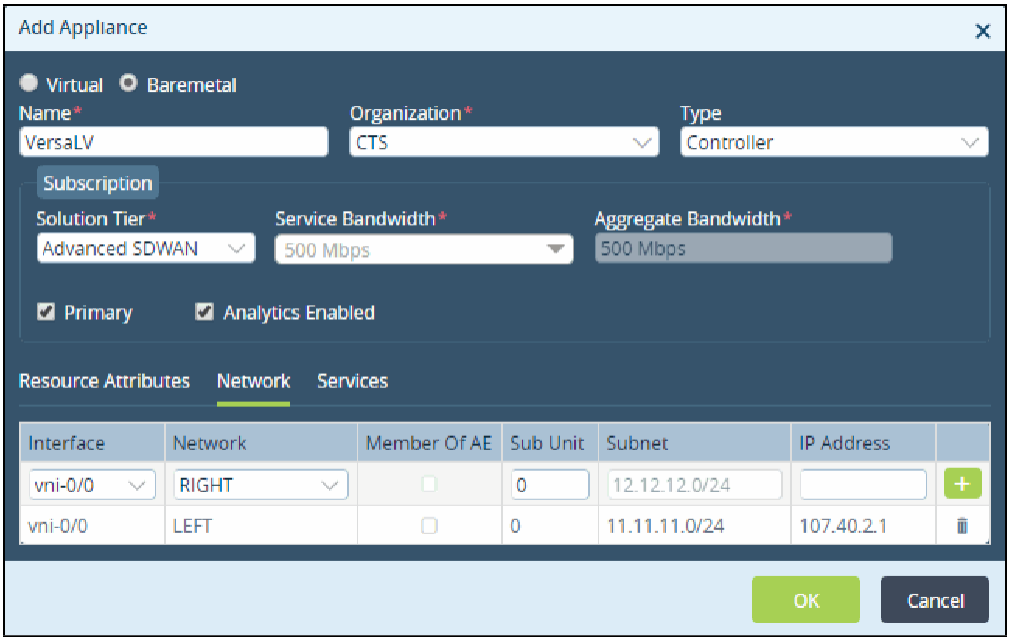
1. In the Director view, go to **Administration** > **Appliances**.
2. Click the Add icon. The Add Appliance screen displays.



Field	Description
Virtual Baremetal	Type of underlying platform.
Name	Name of the SteelConnect EX FlexVNF. Example: *SFWApp*
Organization	Name of the organization. Example: *Pepsi*
Type	Appliance type: ▪ *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	▪ **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.

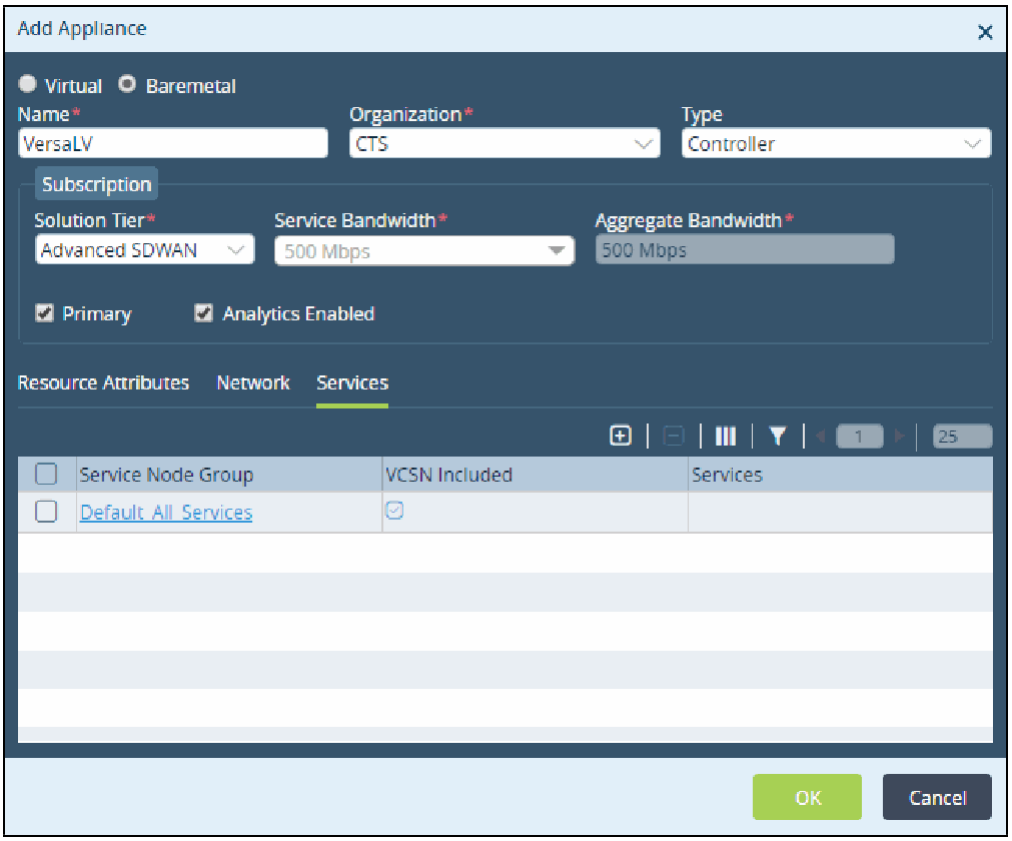
a. Click the **Network** tab. This displays the networks, if any, associated with the organization. The network information automatically derives from the host interfaces.



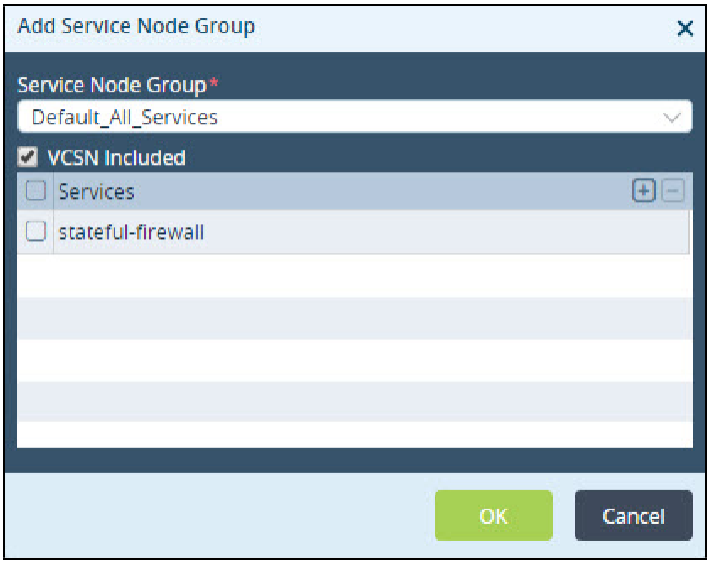
Field	Description
Interface	Interface to be used.
Network	Network to be used.
Sub Unit	Sub Unit.
IP Address	IP address of the network.

i. Click the Add icon. Repeat the steps to add multiple 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.

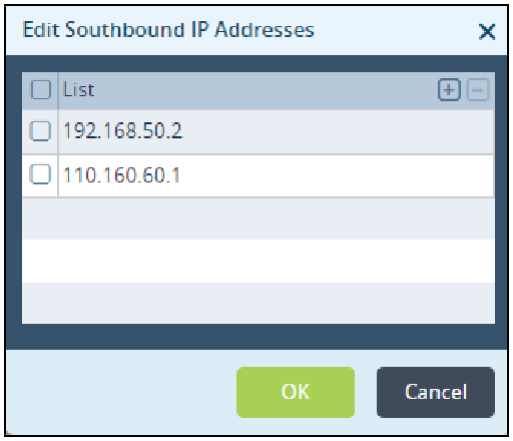
This creates an appliance on bare metal. This completes creating an appliance on OpenStack, vCloud Director, and bare metal.

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.

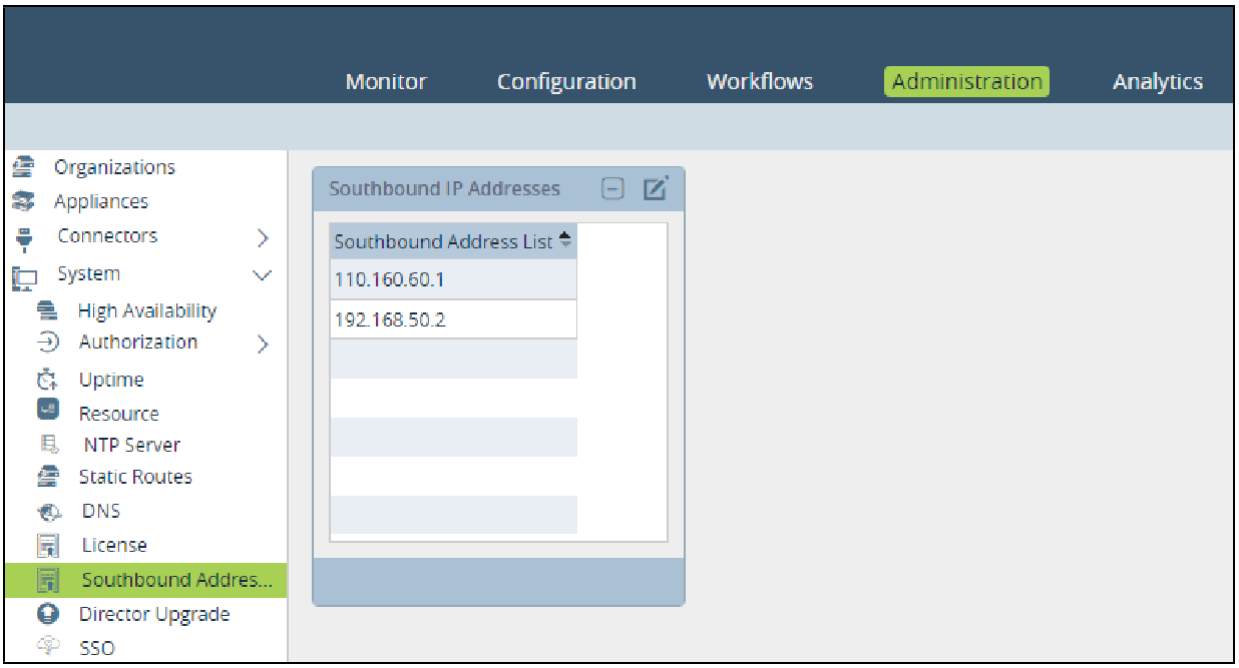
Steps

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.

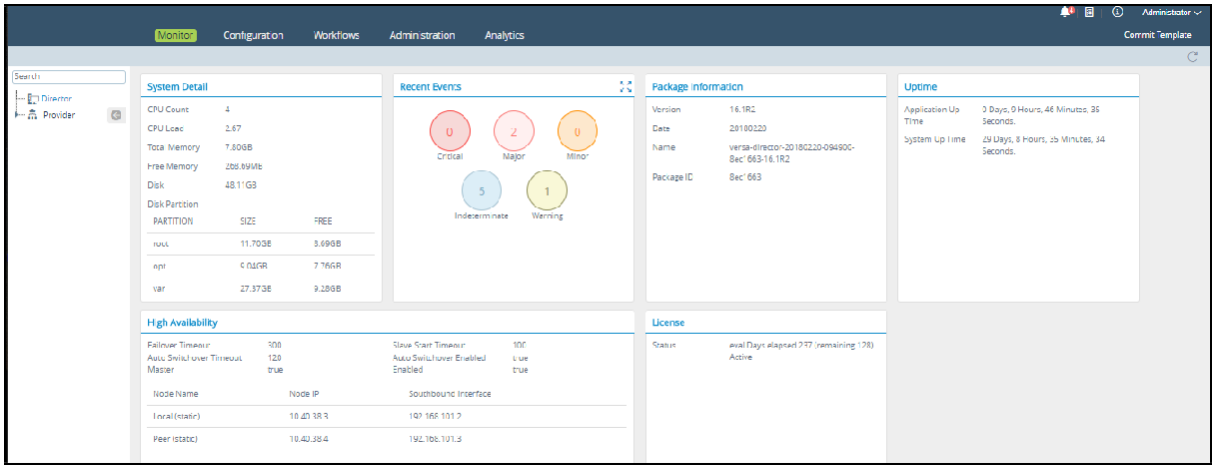


3.4 Alarm management

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

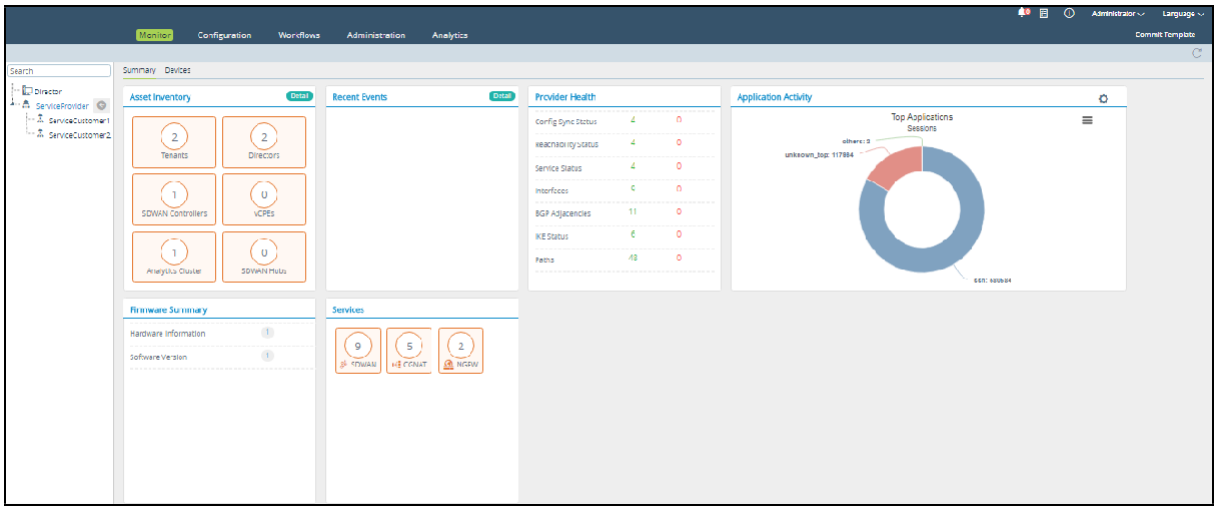
1. In the Director view, go to **Monitor**.



This screen displays the following sections at the Director level:

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

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

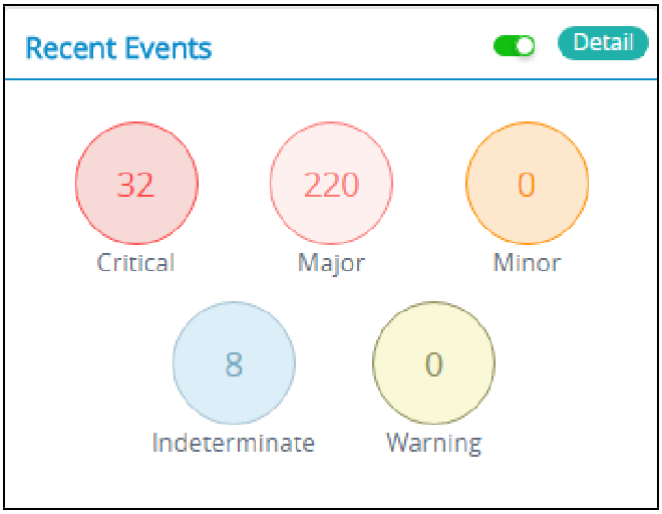


The screen displays the following sections:

- **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.)

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.

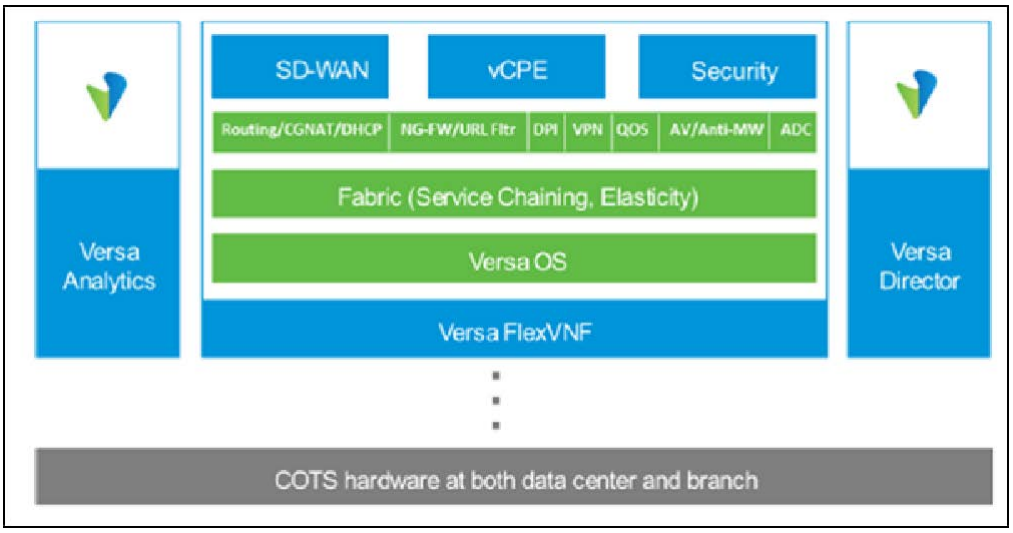
- Click the Back Back button to go back to the tile view of this screen.
- Click the **Column Filter** icon to select the columns to be displayed.

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 Directo**r which serves as a VNF Manager.
- **SteelConnect EX Analytic**s 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.

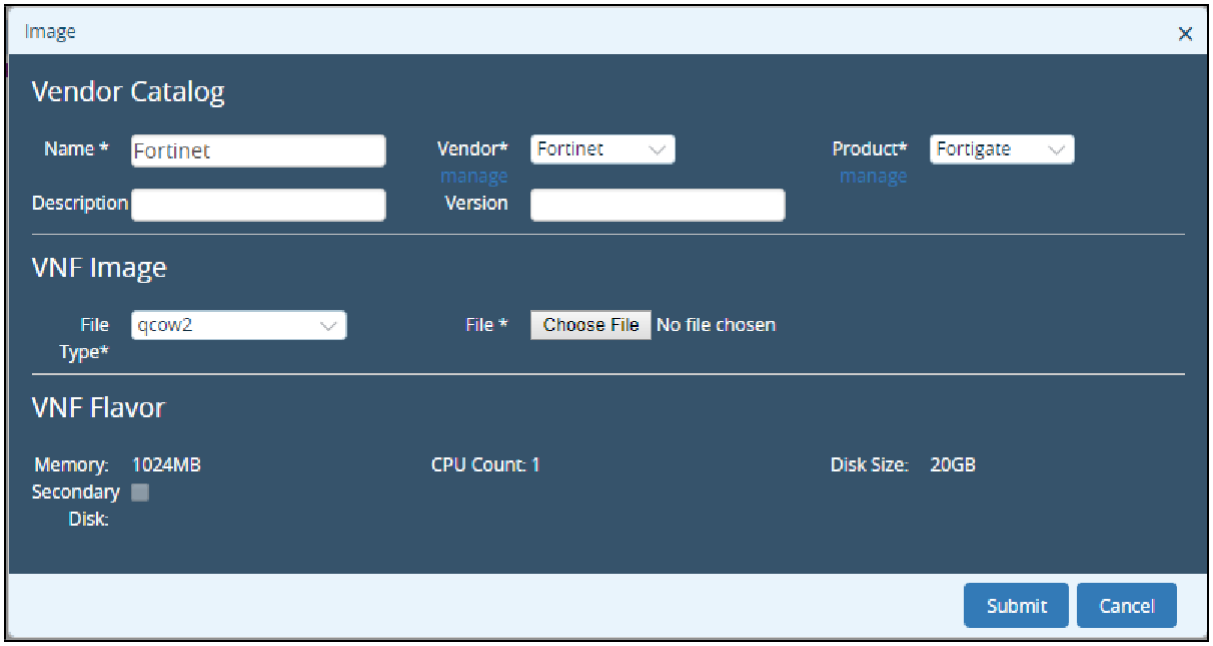
Service chain can be created which straddles multiple branches and hubs. Such a service-chain would contain one SteelConnect EX FlexVNF at each of those branches or hubs. The SteelConnect EX FlexVNF at each of the branches or hubs could be configured for horizontal or vertical modes of service chaining.

4.2 Configuring uCPE on SteelConnect EX FlexVNF

4.2.1 Creating a Vendor Catalog

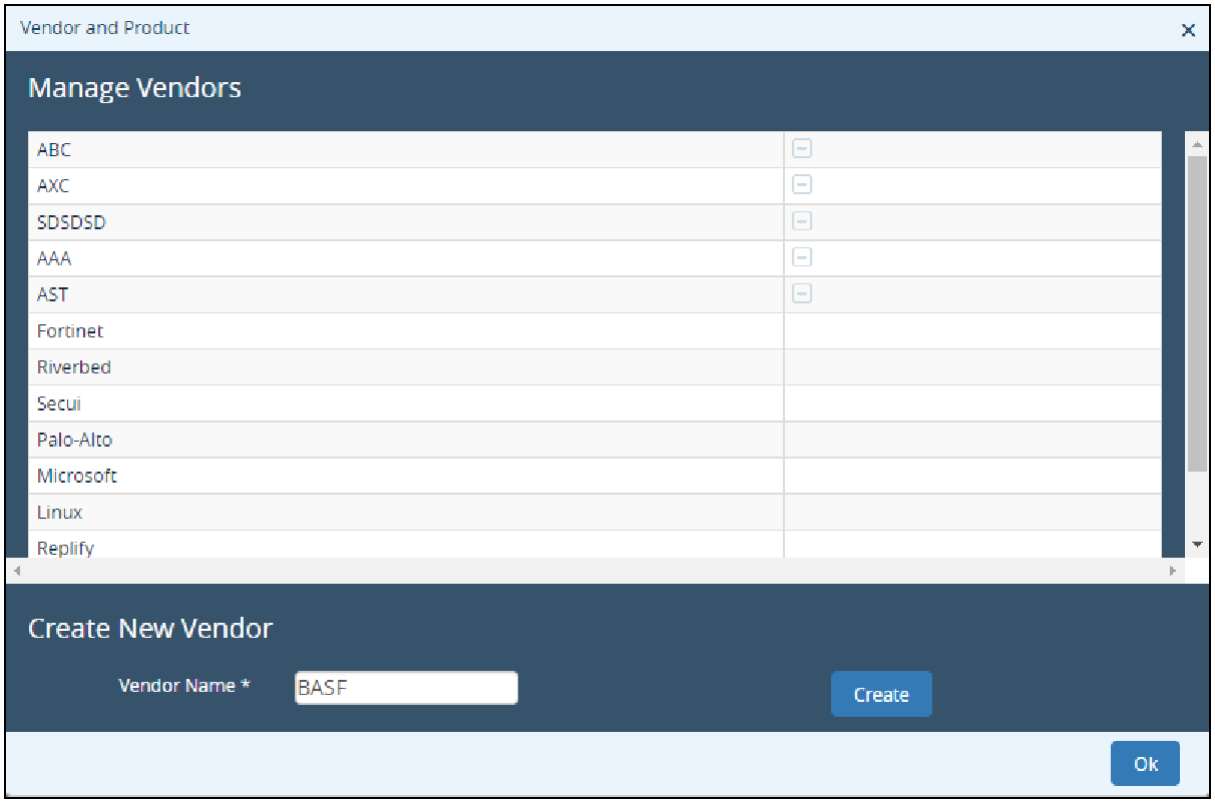
To create a third party VNF to the SteelConnect EX FlexVNF's vendor catalog, perform the following steps:

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.

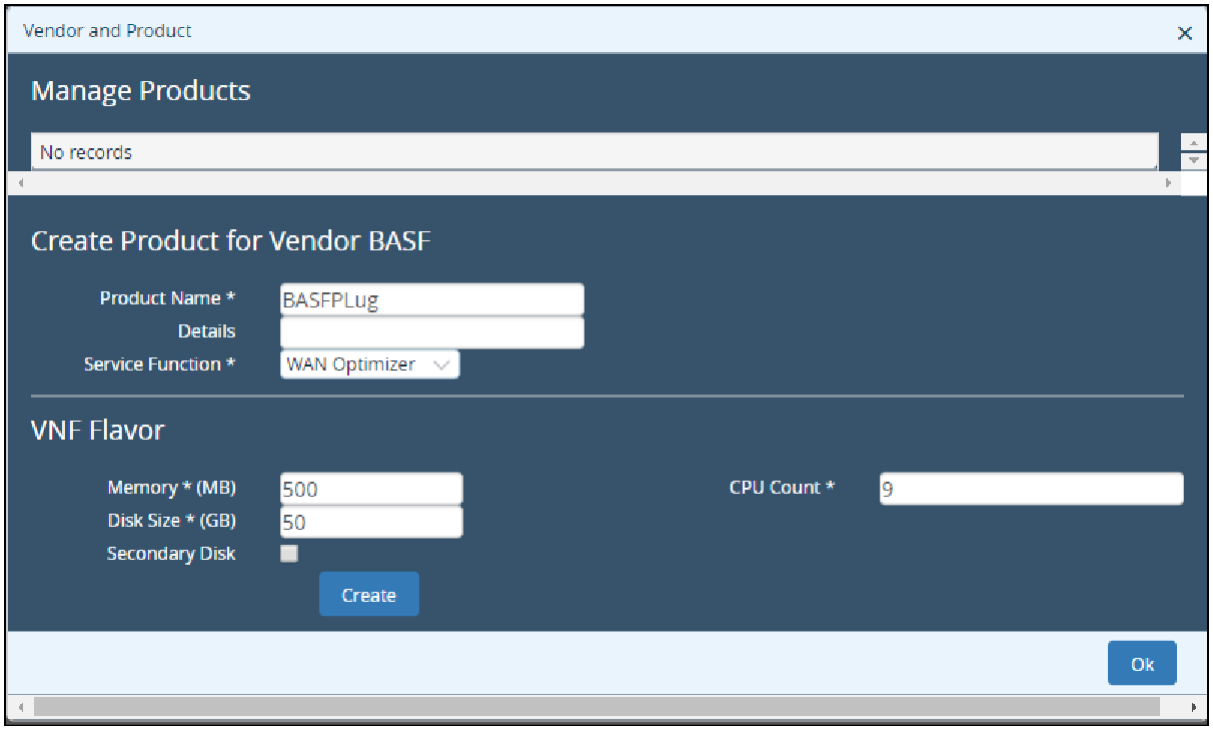


Field	Description
Name	Name of the new uCPE that you are adding to the SteelConnect EX FlexVNF.
Description	Brief description of the interface and its purpose.
Vendor	Vendor that is supported on SteelConnect EX FlexVNF: • *Fortinet* • *Riverbed* • *Secui*
Version	uCPE version for the selected vendor.
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.

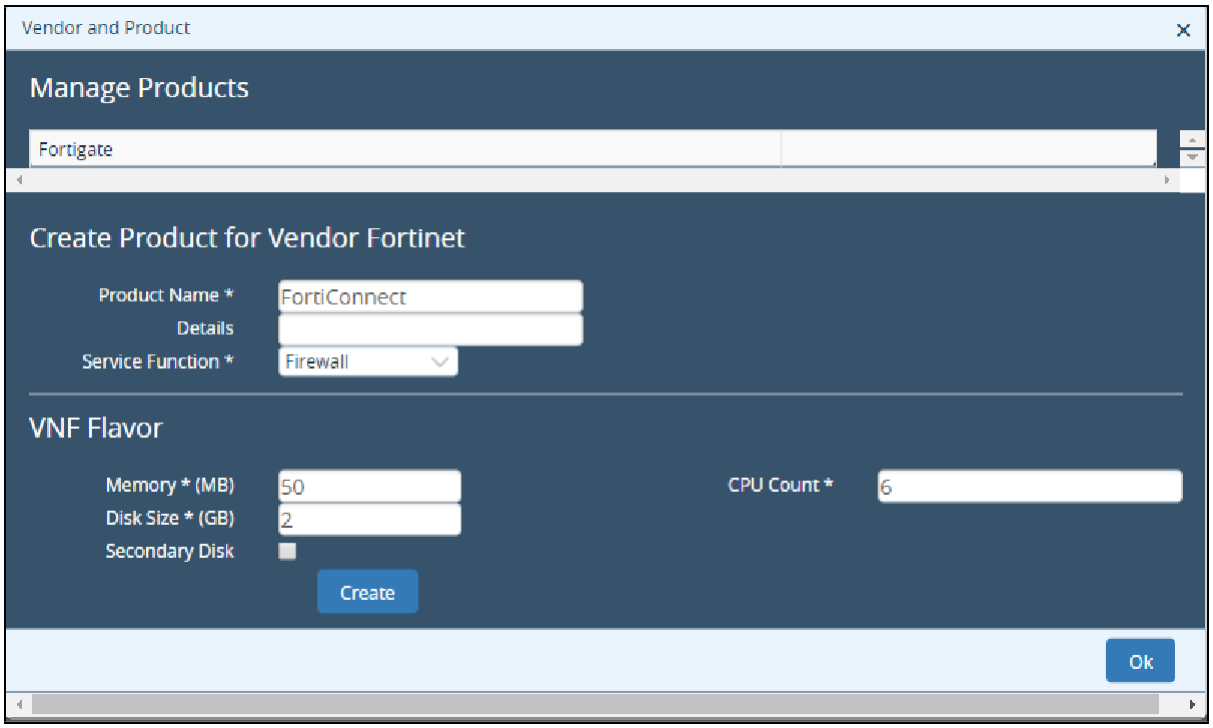


3. Enter the vendor name and click **Create** to create a product for the vendor.



Field	Description
Product Name	Name of the product.
Service Function	Type of product: • *Firewall* • *NextGenFirewall* • *WANOptimizer* • *Others*
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.

4. Click **OK**.
5. Click **manage** under **Product** to create a product.



Field	Description
Product Name	Name of the product.

Field	Description
Service Function	Type of product: • *Firewall* • *NextGenFirewall* • *WANOptimizer* • *Others*
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

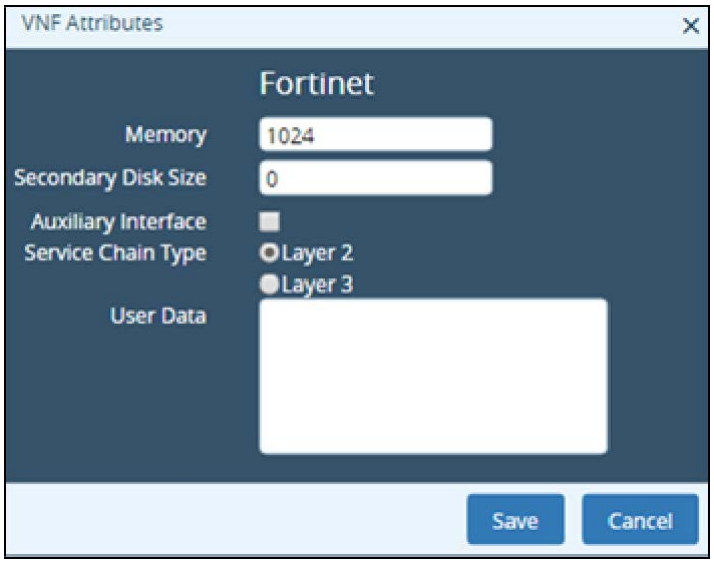
To configure the SteelConnect EX FlexVNF service chaining, perform the following steps:

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.

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



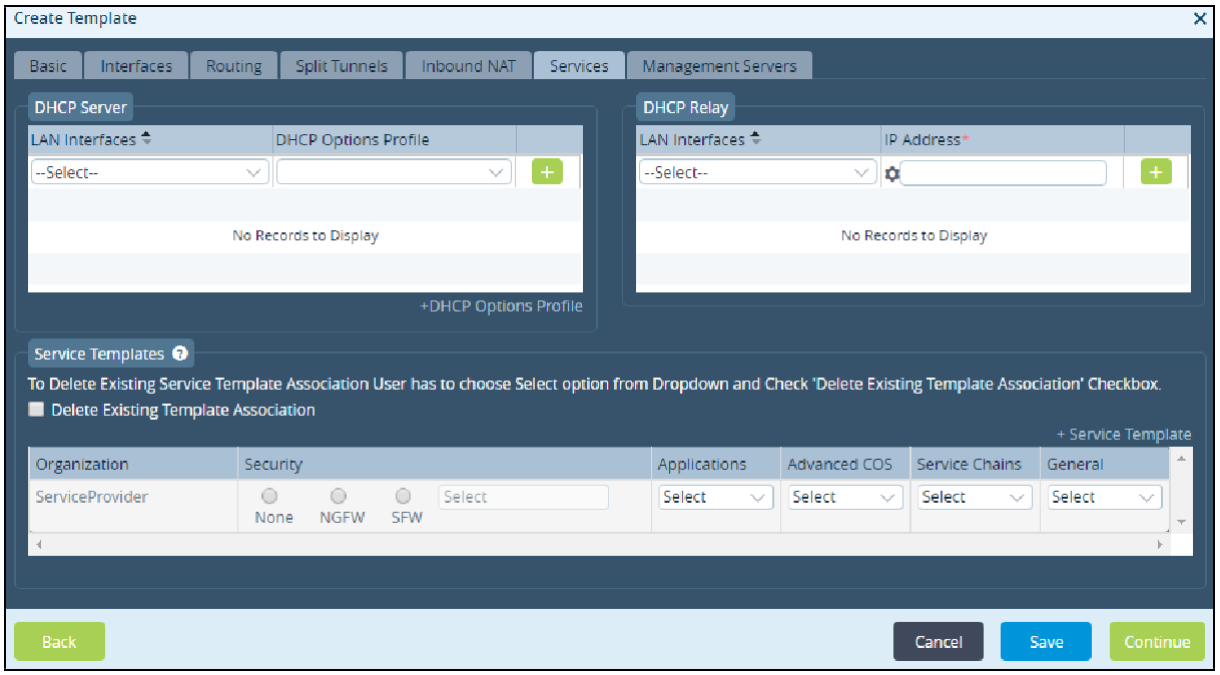
Field	Description
Memory	CPU memory limit for the select guest VNF.
Secondary Disk Size	Secondary disk size of the guest VNF.
Auxiliary Interface	Guest VNF as an auxiliary interface.
Service Chain	Layer on which the service chain is configured: • *Layer2* • *Layer3*
User Data	User data about the guest VNF for reference.

3. Click **Save** to update the guest VNFs configuration.
4. 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.

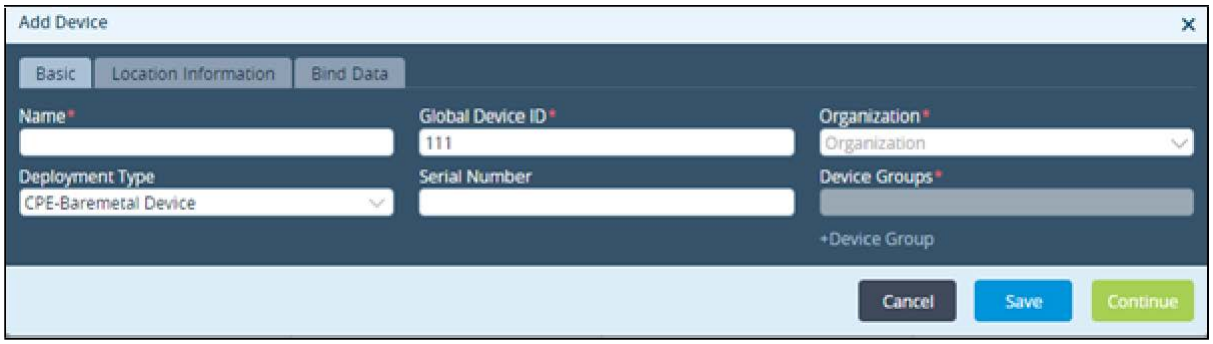


2. Enter the necessary details in the **Services** tab.
3. Click **Save** to complete the service chaining configuration.
4. Click **Continue** to create/recreate and deploy the template with the service chain template.

4.2.4 Adding Devices to the Device Template

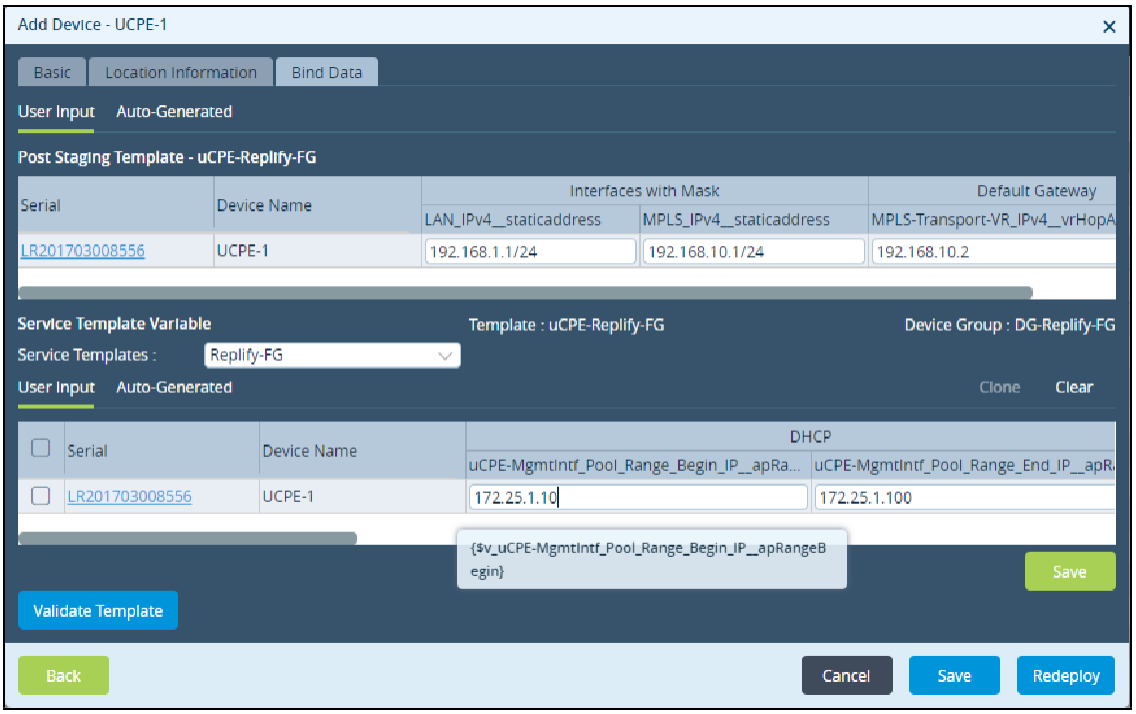
To add devices to the device template, perform the following steps:

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.



   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.



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

4.2.5 Onboarding the device through Zero Touch Provisioning (ZTP)

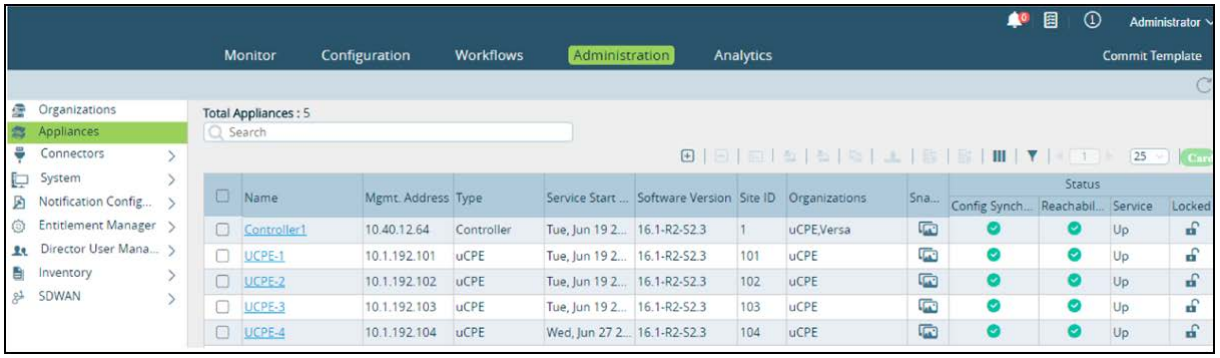
1. Bring up the device using ZTP. Refer to *URL Based Zero Touch Provisioning.*
2. Reboot the device. After the device is up, the controller sends the post-staging notification to SteelConnect EX Director.
3. SteelConnect EX Director copies the qcow2 file to the respective device and triggers the command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

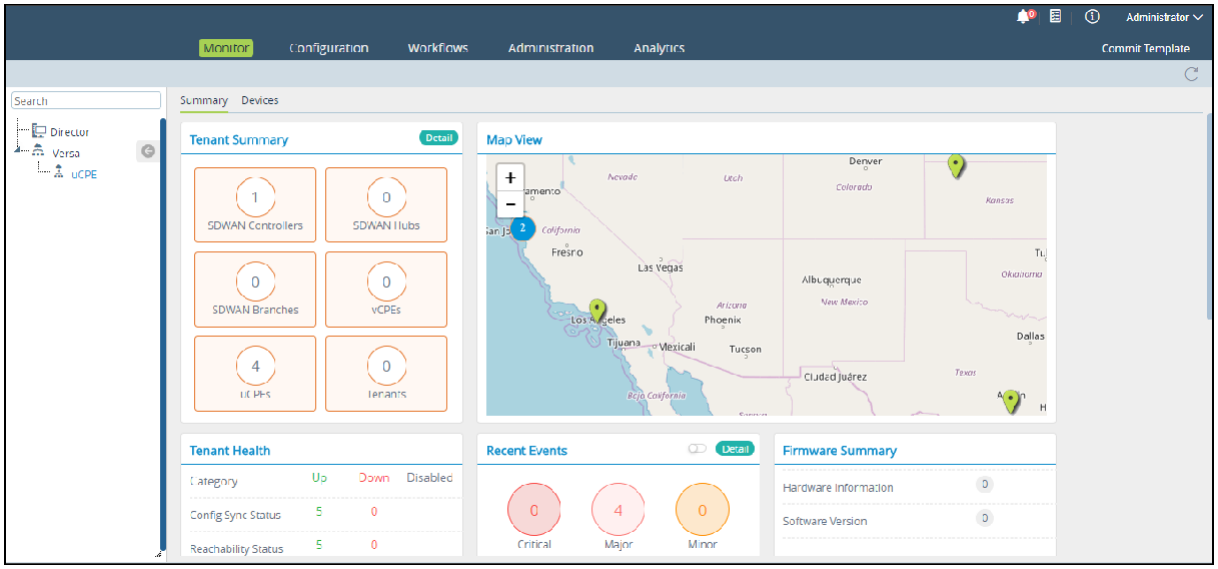
1. In the Director view, go to **Administration** > **Appliances** to view the list of appliances configured on the SteelConnect EX FlexVNF. The dashboard will now have a new entry for the uCPE added in the previous section.



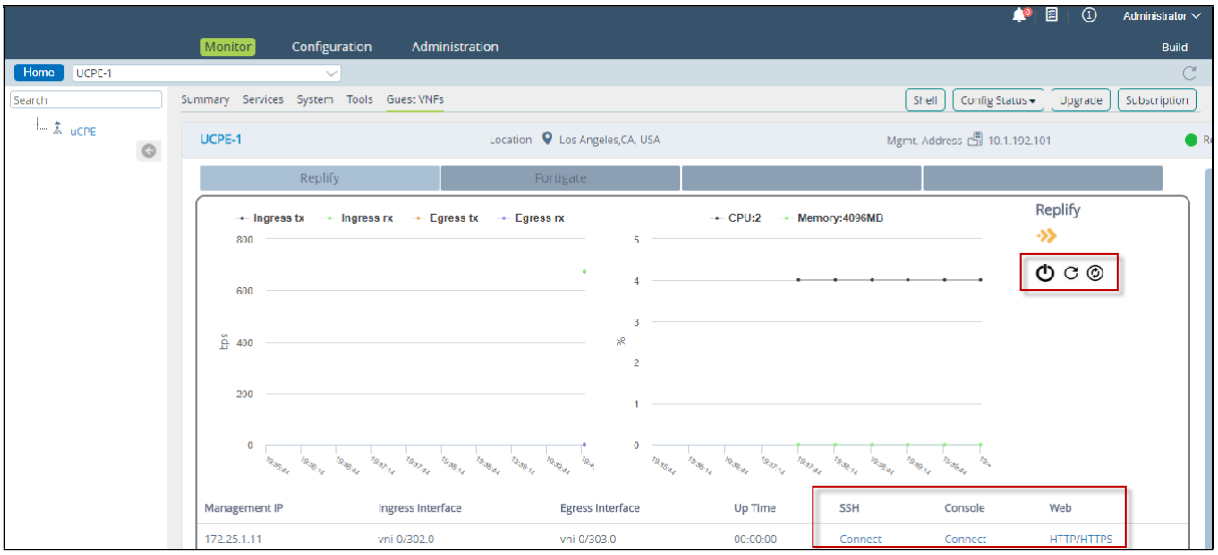
4.2.7 Monitoring uCPE

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:

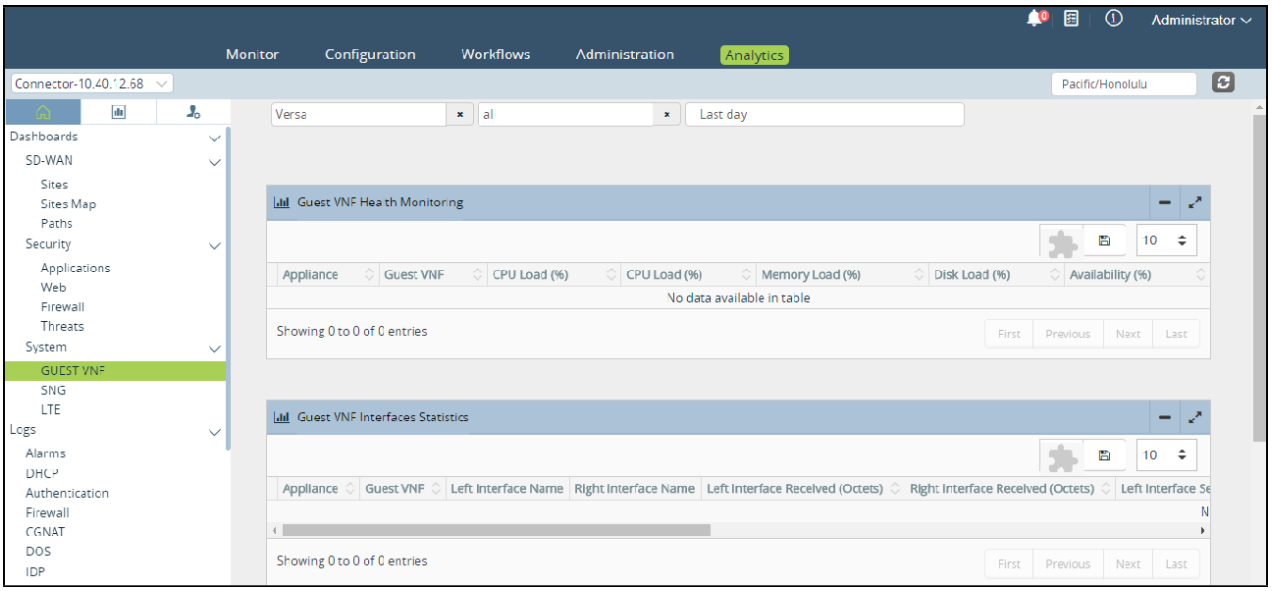
- CPU/Memory graph over a 30 second interval.
- Ingress/Egress tx/rx statistics over a 30 second interval.

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
vni-0/300.0   1       Provider-Control-VR   UCPE-MGMT1  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
vni-0/301.0   1       Provider-Control-VR   UCPE-MGMT2  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                             UCPE-PORT3  0        0    0      0      0      0        0    0      0      0
vni-0/305     0                             UCPE-PORT4  0        0    0      0      0      0        0    0      0      0
vni-0/306     0                             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>
```

4. 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 virtlockd start
```

Try starting the `versa-virtmgr` service.

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
```

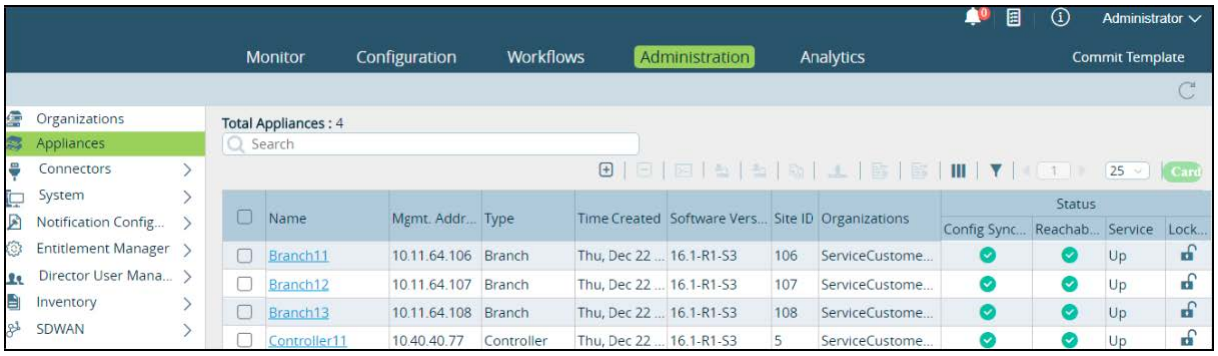
Return to Top(see page 0)

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	Status of configuration synchronization between device and Director: • 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: - 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	Status of the connection between SteelConnect EX Director and the appliance. • 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	Status of FlexVNF services on the FlexVNF device: • 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	Status of an administrative configuration lock: • Locked icon—FlexVNF configuration is administratively locked and cannot be modified. • Unlocked icon—FlexVNF configuration is administratively unlocked and can be modified.

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

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